Mendelova univerzita v Brně
Provozně ekonomická fakulta

Potenciálne finančné straty podniku spôsobené nedostatočne zabezpečenou podnikovou sieťou

Bakalárska práca

Vedúci práce:
Ing. Jiří Balej

Martin Janšto

Brno 2015

Čestné prehlásenie

Prehlasujem, že som tuto prácu: **Potenciálne finančné straty podniku spôsobené nedostatočne zabezpečenou podnikovou sieťou** vypracoval samostatne a všetky použité pramene a informácie sú uvedené v zozname použitej literatúry. Súhlasím, aby moja práca bola zverejnená v súlade s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v súlade s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Som si vedomý, že sa na moju prácu vzťahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavretie licenčnej zmluvy a použitie tejto práce ako školského diela podľa § 60 odst. 1 Autorského zákona.

Ďalej sa zaväzujem, že pred spísaním licenčnej zmluvy o využití diela inou osobou (subjektom) si vyžiadam písomné stanovisko univerzity o tom, že predmetná licenčná zmluva nie je v rozpore s oprávnenými záujmami univerzity, a zaväzujem sa uhradiť prípadný príspevok na úhradu nákladov spojených so vznikom diela, a to až do ich skutočnej výšky.

V Brne dňa 31. decembra 2015 _____

Abstract

Janšto, M. Potential financial losses due to vulnerabilities of corporate computer network. Bachelor thesis. Brno: Mendel University, 2015.

Thesis deals with design and realization of the vulnerability testing of the corporate network from both outer and inner environment of the company. Thesis contains the risk analysis and proposed adequate security measures. Financial cost of implementation of the security measures are compared with the business impact analysis. The main goal of the thesis is to show the importance of information security expenditures in the company.

Keywords

Penetration testing, vulnerabilities, risk analysis, information security.

Abstrakt

Janšto, M. Potenciálne finančné straty podniku spôsobené nedostatočne zabezpečenou podnikovou sieťou. Bakalárska práca. Brno: Mendelova univerzita v Brně, 2015.

Práca sa zaoberá návrhom a realizáciou testovania zraniteľností podnikovej siete z vonkajšieho a vnútorného prostredia podniku. Súčasťou práce je analýza rizík a následne navrhnuté adekvátne bezpečnostné opatrenia. Finančné náklady na implementáciu opatrení sú v práci porovnávané s analýzou dopadov na podnikanie. Cieľom práce je poukázať na dôležitosť a oprávnenosť výdavkov spojených s informačnou bezpečnosťou v podniku.

Kľúčové slová

Penetračné testovanie, zraniteľnosti, analýza rizík, informačná bezpečnosť.

Obsah

1 Úvod 11

2 Prehľad legislatívnych predpisov 12

2.1 Pripravovaný zákon o informačnej bezpečnosti ... 12

2.2 Zákon č. 351/2011 Z. z. elektronických komunikáciách ... 12

2.3 Zákon č. 136/2014 Z. z. o ochrane osobných údajov ... 12

2.4 Zákon č. 45/2011 Z. z. o kritickej infraštruktúre ... 13

2.5 Zákon 275/2006 Z. z. o informačných systémoch verejnej správy ... 13

3 Testovanie zraniteľností podnikovej siete 14

3.1 Penetračné testovanie ... 14

3.1.1 Nástroje používané pri penetračnom testovaní ... 14

3.2 Skúmanie zraniteľností podniku z vnútorného prostredia ... 15

4 Systém riadenia informačnej bezpečnosti 16

4.1 Politika informačnej bezpečnosti ... 16

4.2 Bezpečnostné smernice ... 17

4.3 Klasifikácia aktív ... 17

4.4 Analýza rizík ... 20

4.5 Bezpečnostné opatrenia na zníženie miery rizika ... 21

4.6 Havarijné plány a plány obnovy ... 21

4.7 Efektívny systém riadenia informačnej bezpečnosti ... 22

4.8 Analýza dopadov na podnikanie ... 23

5 Praktická časť 25

5.1 Test zraniteľností vonkajšieho prostredia ... 25

5.1.1 Doména podniku ... 25

5.1.2 DNS záznamy domény ... 25

5.1.3 Subdomény domény firmaabc.sk ... 26

5.1.4 Zraniteľnosti webovej stránky www.firmaabc.sk ... 27

5.1.5 Služby na verejnej IP adrese podniku ... 28

5.1.6 Zistené zraniteľnosti z vonkajšieho prostredia 30
5.2 Informačná bezpečnosť z vnútorného prostredia podniku 30
5.2.1 Popis podniku 30
5.2.2 Okolie podniku 30
5.2.3 Fyzická bezpečnosť podnikových priestorov 31
5.2.4 Stav systému riadenia informačnej bezpečnosti a dokumentácie 31
5.3 Identifikácia aktív podniku 32
5.4 Analýza rizík kritických aktív 32
5.4.1 Diskové pole a aplikačný server 33
5.4.2 Aplikácia AbcSecure 33
5.4.3 Sieťová infraštruktúra 34
5.4.4 Osobné údaje 35
5.5 Zraniteľnosti kritických aktív 35
5.5.1 Diskové pole a aplikačný server 35
5.5.2 Aplikácia AbcSecure 36
5.5.1 Sieťová infraštruktúra 37
5.5.2 Osobné údaje 38
5.6 Navrhnuté bezpečnostné opatrenia 39
5.7 Analýza dopadu na podnikanie 41
5.7.1 Ohrozenie prevádzky aplikácie AbcSecure 41
5.7.2 Strata, únik alebo krádež osobných a iných citlivých údajov 42

6 Záver 44

7 Literatúra 45

1 Úvod

Postupujúca informatizácia každodenných činností vytvorila potrebu chrániť dôležité informácie, ktoré sú spracúvané a uchovávané v rozsiahlych informačných systémoch. Získanie citlivých informácií je cieľom útočníkov, ktorí s údajmi obchodujú. Nezriedka informácie končia u konkurencie alebo sú využívané pri páchaní trestnej činnosti.

Význam informačnej bezpečnosti narastá a spolu s ňou i množstvo vynaložených prostriedkov na ochranu aktív spoločnosti. Narušenie informačnej bezpečnosti môže pre spoločnosť stratu jej mena a s ním spojenej dôveryhodnosti, konkurenčných výhod, ale i nemalých finančných prostriedkov, prípadne jej likvidáciu.

Informačná bezpečnosť je široký pojem zahŕňajúci veľké množstvo oblastí, ktoré spolu s pokrokom vo svete informačno-komunikačných technológii neustále rastie a mení sa.

Úroveň informačnej bezpečnosti je priamo závislá od množstva efektívne vynaložených prostriedkov na implementáciu bezpečnostných opatrení, avšak veľakrát stačí prijať opatrenia, ktorými sa bezpečnostné riziko zníži na prijateľnú úroveň a zároveň nevyžadujú vysoké finančné investície.

Práca je rozdelená na štyri časti. Prvou časťou je prehľad platnej legislatívy týkajúcej sa informačnej bezpečnosti v Slovenskej republike. V druhej časti sú vysvetlené základné termíny, nástroje a postupy používané v praktickej časti práce. Ďalšou časťou je popis zavádzania systému riadenia informačnej bezpečnosti a dokumentácia súvisiaca s informačnou bezpečnosťou podniku. Súčasťou tejto časti práce je i návrh postupu v praktickej časti pri klasifikácii aktív podniku, analýze rizík a dopadov na podnikanie a návrhu bezpečnostných opatrení. Obsahom praktickej časti práce je samotné zrealizovanie navrhnutého postup a porovnanie finančných nákladov na odstránenie zraniteľností s finančnými nákladmi v prípade zneužitia zistených zraniteľností. Cieľom práce je poukázať na dôležitosť zavedenia systému riadenia informačnej bezpečnosti v podniku a zároveň dokázať, že úroveň informačnej bezpečnosti v podniku je možné zvýšiť i bez nutnosti vysokých investícií do implementácie rozsiahlych softvérových riešení.

2 Prehľad legislatívnych predpisov

Súčasný právny poriadok Slovenskej republiky obsahuje viacero právnych predpisov týkajúcich sa informačnej bezpečnosti. Pokrývajú špecifické oblasti informačnej bezpečnosti, ale právny predpis, ktorý by pokrýval informačnú bezpečnosť celého digitálneho priestoru Slovenskej republiky, v súčasnosti neexistuje. Dôsledkom je nekonzistencia používanej terminológie, nejednoznačnosť kompetencií štátnych orgánov a zmätok v povinnostiach dotknutých organizácií.

2.1 Pripravovaný zákon o informačnej bezpečnosti

V súčasnosti bol schválený len zámer zákona dňa 25. februára 2010. Zákon by mal upravovať ochranu celého digitálneho priestoru Slovenskej republiky. Za prípravu nového zákona o informačnej bezpečnosti je zodpovedné Ministerstvo financií Slovenskej republiky. Hlavným cieľom tohto zákona bude zjednotenie terminológie, štruktúry dokumentácií, zákonných povinností povinných osôb a zdôraznenie dôležitosti informačnej bezpečnosti v Slovenskej republike.

2.2 Zákon č. 351/2011 Z. z. elektronických komunikáciách

Zákon považuje internet a počítačové siete za elektronické komunikačné siete. Orgánmi štátnej správy v tejto oblasti sú Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky a Telekomunikačný úrad Slovenskej republiky. Pod ich kompetencie z oblasti informačnej bezpečnosti spadá kontrola a regulácia fyzickej bezpečnosti sietí, dodržiavania technických noriem a podmienok odpočúvania elektronickej komunikácie a ochrana údajov spojených s prevádzkou elektronických komunikačných sietí.

Zákon sa vzťahuje len na služby elektronických komunikačných sietí, nie na prenášaný obsah služieb. Prevádzkovateľ a jeho povinnosti podľa § 64 sa vzťahujú na subjekty, ktoré poskytujú služby elektronických komunikačných sietí.

2.3 Zákon č. 136/2014 Z. z. o ochrane osobných údajov

Legislatívne predpisy v oblasti ochrany osobných údajov boli v Slovenskej republike viackrát menené kvôli nejednoznačnosti a prílišnej prísnosti v oblasti opatrení a sankcií v porovnaní s ostatnými štátmi EÚ. Úrad na ochranu osobných údajov je orgánom štátnej správy, ktorý tento zákon interpretuje, je kontrolným orgánom a má právo udeľovať sankcie.

Osobné údaje sú také údaje, za pomoci ich kombinácie je možné jednoznačne identifikovať osobu. V zákone sa osobné údaje delia na dve kategórie. Osobitné, ktoré sú taxatívne vymenované v § 13 zákona a patrí medzi ne napríklad jedinečný identifikátor – rodné číslo. Obyčajné osobné údaje sú všetky osobné údaje, ktoré nie sú osobitné.

Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ informačného systému, ktorý ich spracúva. Osobné údaje musí chrániť pred poškodením, stratou, zničením, porušením integrity, neoprávneným prístupom, neoprávneným zverejňovaním, zneužitím alebo nedovoleným typom zhromažďovania.

Prevádzkovateľ informačného systému osobných údajov je povinný mať vypracovaný bezpečnostný projekt informačného systému, ak v informačnom systéme spracúva osobitné kategórie osobných údajov alebo informačný systém slúži na zabezpečenie verejného záujmu.

Bezpečnostný projekt vymedzí rozsah potrebných opatrení na elimináciu hrozieb a rizík ohrozujúcich informačný systém z hľadiska bezpečnosti spracúvania osobných údajov.

Technické, personálne a organizačné bezpečnostné opatrenia, ktoré sú subjekty spracúvajúce osobné údaje povinné prijať, sú podrobne uvedené vo vyhláške Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013. Rozsah opatrení záleží od miery citlivosti osobných údajov, podmienkam a rizikám ich spracúvania.

Doplňujúca vyhláška č. 117/2014 kladie ešte väčší dôraz na kontrolné činnosti, postupy pri haváriách, poruchách a iných mimoriadnych udalostiach a zdôrazňuje taktiež preventívne opatrenia na zníženie ich pravdepodobnosti. Zdokumentovaná musí byť i efektívna obnova do predchádzajúceho stavu.

2.4 Zákon č. 45/2011 Z. z. o kritickej infraštruktúre

Zákon zavádza pojem – kritická infraštruktúra – infraštruktúra, bez ktorej by spoločnosť nemohla fungovať. Jej prvkom je služba alebo inžinierska stavba, ktorej zničenie alebo znefunkčnenie by malo závažné dôsledky na celú infraštruktúru.

Prevádzkovateľ kritickej infraštruktúry je povinný modernizovať jej prvky, zaviesť bezpečnostný plán a vypracovať bezpečnostný projekt. Nad celou kritickou infraštruktúrou má dohľad Vláda SR a Ministerstvo vnútra SR.

2.5 Zákon 275/2006 Z. z. o informačných systémoch verejnej správy

Zákon sa vzťahuje na informačné systémy verejnej správy. Ich prevádzkovateľom stanovuje povinnosť zabezpečiť bezpečnú a nepretržitú prevádzku, súlad so štandardmi informačných systémov verejnej správy, ktoré sú pravidelne aktualizované Ministerstvom financií SR. Predpokladom plnenia štandardov informačných systémov verejnej správy je implementácia systému manažmentu informačnej bezpečnosti. Štandardy síce vychádzajú z noriem ISO/IEC 27002:2005, ale nie sú s nimi plne kompatibilné. Tento zákon dopĺňa najmä Výnos o štandardoch pre ISVS č. 55/2014 Z. z. a jeho neskoršie novely. Popisujú okrem požiadaviek na štruktúry uchovávaných dát, architektúru i požiadavky na bezpečnostné mechanizmy informačných systémov verejnej správy.

3 Testovanie zraniteľností podnikovej siete

Testovanie zraniteľností môže prebiehať rôznymi spôsobmi. V našej práci si popíšeme jeden z často používaných procesov testovania zraniteľností počítačovej siete firmy. Odporúča sa rozdelenie testovania na dve časti, z vonkajšieho prostredia a z vnútorného prostredia firmy. Prvým krokom bude otestovanie vonkajšieho rozhrania spoločnosti penetračným testovaním.

3.1 Penetračné testovanie

Penetračné testovanie je súhrn činností, ktoré simulujú reálny útok útočníka. Osoba, ktorá testovanie vykonáva, sa nazýva etický *hacker*. Penetračné testovanie sa delí na tri typy podľa množstva informácií, ktoré sú známe osobe vykonávajúcej penetračné testovanie:

- **black box** – test, pred ktorým etický *hacker* nepozná žiadne bližšie informácie o sieťovej infraštruktúre, počte skúmaných zariadení, rozmiestnení prvkov, k dispozícii od testovaného subjektu nedostal žiadnu dokumentáciu a celý scenár testovania si vytvára sám. O testovaní zraniteľností siete vie väčšinou iba bezpečnostný manažér, prípadne štatutárny orgán subjektu.
- **white box** – je testovanie vopred známej infraštruktúry, etický *hacker* má prístup ku všetkým dokumentáciám, systémom a v prípade podrobného testovania i k zdrojovým kódom informačných systémov. O testovaní bezpečnosti vie i systémový administrátor, prípadne všetci zamestnanci subjektu.
- **gray box** – test, pred ktorým etický *hacker* pozná iba niektoré časti infraštruktúry. Táto znalosť je vhodná najmä pri potrebe dôkladnejšieho testovania zraniteľností z vonkajšieho prostredia podnikovej infraštruktúry.

Pred samostatným testovaním je potrebné so zástupcom podniku zmluvne zabezpečiť jeho súhlas a súhlas vlastníka siete s rozsahom testovania zraniteľností, spôsobom testovania, napr. vylákanie dôležitých citlivých informácií od zamestnancov – tzv. *sociálne inžinierstvo* alebo či je možné testovaním dočasne obmedziť funkčnosť služieb. Obvyklým testovaním zraniteľností by však firme nemali byť spôsobené žiadne škody.

V našej práci použijeme pre testovanie zraniteľností vonkajšieho rozhrania typ testovania „black box“, okrem názvu firmy nám teda nebudú k dispozícii žiadne iné údaje. Týmto spôsobom otestujeme najznámejšie zraniteľnosti z pohľadu náhodného útočníka, ktorý nemá o sieti firmy iné ako verejne dostupné informácie.

3.1.1 Nástroje používané pri penetračnom testovaní

Testovanie zraniteľností počítačovej siete z vonkajšieho prostredia pozostáva zo zberu voľne dostupných informácií, prieskumu a identifikácie vonkajšieho rozhrania siete podniku a poskytovaných služieb a zisťovanie zraniteľností aplikácii po-

skytujúcich tieto služby. V praktickej časti práce budeme používať nasledujúce nástroje:

- **Internetový prehliadač** – na prehliadanie zdrojového kódu webových stránok a hľadanie voľne dostupných informácií o podniku.
- **Dig** – príkaz operačného systému Linux, slúži na zisťovanie informácií prekladu doménových mien na IP adresy a späť.
- **Host** – príkaz operačného systému Linux, ktorý slúži na preklad IP adresy na doménové meno a späť.
- **Knockpy** – skener v programovacom jazyku Python, slúži na nájdenie subdomén zadanej domény jednoduchým spôsobom vyberania názvov zo slovníka.
- **Ping** – príkaz operačného systému Linux, ktorý slúži na jednoduché otestovanie dostupnosti zariadenia cez sieť zaslaním ICMP ECHO_REQUEST paketu.
- **Nmap** – zadarmo dostupný program pre prieskum siete a bezpečnostný audit. Môže byť použitý na zisťovanie dostupnosti systému cez sieť, ktoré služby tento systém poskytuje, aké sú verzie aplikácii poskytujúcich tieto služby a aký operačný systém beží na danom zariadení.
- **WPScan** – program, ktorý slúži ako skener zraniteľností redakčného systému WordPress (Pritchett, 2013).

3.2 Skúmanie zraniteľností podniku z vnútorného prostredia

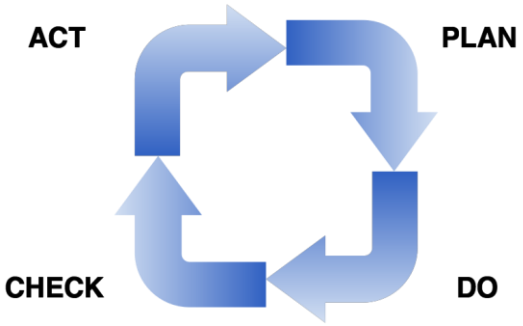
Testovanie zraniteľností počítačovej siete znamená i overenie celkovej úrovne systému riadenia informačnej bezpečnosti v podniku. Po identifikácii zraniteľností počítačovej siete z vonkajšieho prostredia obvykle pokračujeme kontrolou predpisov a dokumentov riadenia informačnej bezpečnosti, skúmaním jednotlivých procesov a ochrany informácii v podniku.

Osobnými pohovormi so zamestnancami je do istej miery možné zistiť úroveň povedomia informačnej bezpečnosti alebo i pracovné návyky negatívne ovplyvňujúce úroveň informačnej bezpečnosti. V prípade veľkej spoločnosti sa kvôli zjednodušeniu pohovor vykonáva len so zástupcami jednotlivých oddelení.

4 Systém riadenia informačnej bezpečnosti

Požiadavky na informačnú bezpečnosť vyplývajúce zo zákonov stručne zmienených v prehľade legislatívnych predpisov sa týkajú predovšetkým informačných systémov spracúvajúcich osobné údaje alebo informačných systémov verejnej správy. Požadovaný rozsah bezpečnostných opatrení v súkromnej sfére nie je až na tie, týkajúce sa osobných údajov a prípadne poskytovanie služieb v oblasti elektronických komunikácii, striktne vyžadovaný legislatívou. Ak v podniku chceme docieliť, aby sa úplne a správne údaje dostali do rúk len tomu, kto ich potrebuje a kto je k prístupu k nim oprávnený, je dôležité v podniku zaviesť systém riadenia informačnej bezpečnosti.

ISMS (*Information Security Management System*) je časť celkového systému riadenia organizácie, založená na prístupe k rizikám činností, ktorá je zameraná na ustanovenie, zavedenie, prevádzku, monitorovanie, preskúmanie, údržbu a zlepšovanie bezpečnosti informácií (ISO/IEC 27001:2013). ISMS je definovaný normami *ISO/IEC 17799:2005* a *ISO/IEC 27001:2013*. Podľa normy *ISO/IEC 27001:2013* sa na zavádzanie systému riadenia informačnej bezpečnosti nahliada ako na projekt a využíva sa *Demingov cyklus PDCA*, kde celý projekt spočíva v opakovaní štyroch krokov: plán (*plan*), implementácia (*do*), sledovanie (*check*) a rozhodovanie (*act*).



Obr. 1 Demingov cyklus

Prístup k riadeniu informačnej bezpečnosti je nutné prispôsobovať i veľkosti konkrétnej organizácie a jej charakteru, či zamerania. Pri malých firmách do 20 zamestnancov nie je zväčša potrebné zamestnávať na plný úväzok bezpečnostného experta, pri väčších firmách vzniká potreba bezpečnostného experta alebo dokonca celého oddelenia, ktoré je nezávislé od IT oddelenia podniku.

Stručne popíšeme dokumentáciu súvisiacu s riadením informačnej bezpečnosti, ktorá bude cieľom nášho skúmania zraniteľností podnikovej siete z vnútorného prostredia podniku.

4.1 Politika informačnej bezpečnosti

Základným dokumentom informačnej bezpečnosti v podniku je politika informačnej bezpečnosti. Tento dokument by mal byť prijímaný v súčinnosti

s manažmentom podniku a mal by zahŕňať prehlásenie organizácie, že vytvorí dostatočné personálne, materiálne, organizačné a právne podmienky pre ochranu informácií a s nimi súvisiacich aktív, zavedie mechanizmy vyhodnocovania závažnosti a monitorovania bezpečnostných incidentov (Olejár, 2015).

Organizácia by v politike informačnej bezpečnosti mala určiť kľúčové osoby, ich zodpovednosti za úroveň informačnej bezpečnosti v organizácií a prípadnú možnosť ich postihu v prípade porušenia ich povinností.

4.2 Bezpečnostné smernice

Ďalším dokumentom, ktorý je pre podnik povinný zo Zákona č. 136/2014 Z. z. o ochrane osobných údajov najmä z dôvodu spracúvania osobných údajov, sú bezpečnostné smernice. Bezpečnostné smernice by mali poskytovať odpovede na konkrétne otázky (Olejár, 2015):

- opatrenia fyzickej bezpečnosti (elektronický zabezpečovací systém, zamykanie objektu, strážna služba, obmedzenie fyzického priestoru – napr. serverovej miestnosti a iné),
- pravidlá používania počítačovej siete,
- pravidlá získavania, spracúvania a likvidácie informácií,
- postupy v prípade bezpečnostných incidentov,
- bezpečnú likvidáciu nefunkčných a nepoužívaných médií a zariadení,
- rozsah pravidelného auditu informačnej bezpečnosti,
- analýzu rizík a prijaté bezpečnostné opatrenia na zníženie úrovne rizík.

Bezpečnostné smernice by mali byť prístupné každému zamestnancovi. V malých firmách sú väčšinou sprístupnené na zdieľaných dátových úložiskách, platia pre všetkých rovnako s vyčlenením špecifických rolí informačnej bezpečnosti. V malom kolektíve firmy nie sú potrebné hromadné školenia zamestnancov, väčšinou postačí vstupné školenie zamestnanca a následné usmernenia.

Väčšie firmy by však už mali zavádzať systém pravidelných školení informačnej bezpečnosti, pravidelné testovanie zamestnancov a vytváranie špecializovaných smerníc v závislosti na citlivosti a charaktere práce jednotlivých oddelení.

4.3 Klasifikácia aktív

Aktíva pre podnik predstavujú všetko, čo má pre organizáciu hodnotu, je nimi všetok hmotný a nehmotný majetok. V rámci systému riadenia informačnej bezpečnosti aktíva rozdeľujeme na:

- **informačné aktíva** – sú nimi informácie, ktoré spoločnosť spracúva, uchováva, napr. osobné údaje, citlivé údaje o klientoch,
- **služby** – služby, ktoré spoločnosť poskytuje svojimi informačnými systémami, napr. webhosting, server elektronickej pošty,
- **softvérové aktíva** – napr. operačné systémy, kancelárske programy, aplikačný softvér,

- **hardvérové aktíva** – napr. počítače, servery, sieťové prvky.

Predpokladom k analýze rizík je klasifikácia informačných aktív. Jednotlivým informačným aktívam prideľujeme postupne číselné hodnoty zo zvolených stupníc požiadaviek na dôvernosť, integritu, dostupnosť a kritický čas obnovy. Zvolené stupnice nie sú pevne zákonom alebo normami dané. Mali by sa zostavovať na mieru podľa charakteru organizácie.

Dôvernosť (C) aktíva predpokladá, že informácie sa dostanú len do rúk oprávnených subjektov. V praktickej časti zvolíme nasledujúcu stupnicu:

Tab. 1 Hodnoty C a dôvernosť aktíva

Hodnota C	Názov	Popis
1	verejné	aktíva s verejným prístupom
2	interné	aktíva, ku ktorým majú prístup len zamestnanci podniku
4	citlivé	aktíva, ku ktorým má prístup len úzky okruh zamestnancov, prístup je riadený a možno ho napr. dočasne obmedziť
8	mimoriadne citlivé	aktíva, ku ktorým majú prístup len zamestnanci, ktorí boli špeciálne preškolení, vyžadujú špeciálne zaobchádzanie.

Integrita (I) aktíva znamená, že aktíva zostanú po celú dobu neporušené a odolné náhodným alebo neautorizovaným vplyvom. Stupnica, ktorú použijeme v praktickej časti:

Tab. 2 Hodnoty I a integrita aktíva

Hodnota I	Názov	Popis
1	okrajové	porušenie integrity aktíva nespôsobí škody
2	vážne	integrita aktíva je pre podnik dôležitá
4	kritické	porušenie integrity aktíva spôsobí podniku vážne problémy
8	katastrofálne	porušenie integrity tohto aktíva by mohlo znamenať existenčné problémy podniku

Dostupnosť (A) aktíva vyjadruje jeho dostupnosť podľa potreby autorizovaným osobám:

Tab. 3 Hodnoty A a dostupnosť aktíva

Hodnota A	Názov	Popis
1	zanedbateľné	nedostupnosť aktíva nespôsobí žiadne škody
2	akceptovateľné	dostupnosť aktíva je pre podnik dôležitá
4	poškodzujúce	nedostupnosť aktíva spôsobí vážne problémy
8	neakceptovateľné	nedostupnosť tohto aktíva by mohla znamenať existenčné problémy podniku

Parameter aktíva – **kritický čas obnovy – RTO** (recovery time objective) sa stanovuje v časových jednotkách, znamená maximálnu dobu, do akej doby je funkcionalitu systému potrebné obnoviť zo záloh. Pre naše potreby v praktickej časti zostavíme stupnicu s hodnotami (R) :

Tab. 4 Hodnoty R pre účel výpočtu a hodnoty RTO

Hodnota R	Hodnota RTO
1	48 hodín
2	72 hodín
4	1 týždeň
8	1 mesiac

Pre výpočet klasifikácie aktíva použijeme tento vzťah (Informačná bezpečnosť, 2013):

$$K = \frac{C\ I\ A}{RTO} \tag{1}$$

Kategóriu aktíva zvolíme výberom tohto výsledku z tabuľky č. 5, ktorú sme si pre účely klasifikácie vytvorili:

Tab. 5 Hodnoty K a kategórie aktív

Hodnota K	Názov	Popis
$K < 4$	bežné	Aktíva, ktoré v prípade straty činnosť podniku neohrozia
$4 \leq K < 64$	dôležité	Aktíva, ktoré sú pre podnik dôležité, ale ich strata ešte nemusí znamenať zánik podniku.
$K \geq 64$	kritické	Zaistenie bezpečnosti týchto aktív je pre podnik kľúčové.

K jednotlivým aktívam podniku je potrebné priradiť vlastníka, najlepšie vedúceho zamestnanca oddelenia, ktorý bude za aktívum a jeho funkčnosť zodpovedný.

4.4 Analýza rizík

Po klasifikácii aktív je vhodným postupom analýza rizík. Tá nám pomôže vytvoriť vodiaci rámec pre posudzovanie významnosti zraniteľnosti v kontexte klasifikácie aktív a následne uľahčí rozhodovanie pri zavádzaní bezpečnostných opatrení a voľbe ich priority.

Je viac spôsobov prístupu k hodnoteniu rizík informačnej bezpečnosti. Podľa prístupu k analýze rizík sa metódy delia na:

- **Kvalitatívne analýzy rizík** popisujú pravdepodobnosti a dopady slovne. Nevýhodou tohto prístupu je značná miera subjektivity a zvolených vyjadrovacích prostriedkov hodnotiteľom, čo môže viesť k nepochopeniu výslednej správy. Nevýhodou je takisto nekonzistentnosť takýchto analýz, nemožnosť porovnania s ostatnými organizáciami. Kvalitatívne analýzy rizík sa využívajú najmä tam, kde nie je možné hodnotiť pravdepodobnosti alebo dopady numericky.
- **Kvantitatívne analýzy rizík** využívajú pri hodnotení číselné hodnoty. Výhodou oproti kvalitatívnej analýze rizík je do istej miery eliminácia subjektivity hodnotiteľa. Nevýhodou tohto typu analýzy je potreba dostatočných číselných údajov k ohodnoteniu pravdepodobností a dopadov. Je pomerne ťažké nastavenie stupníc hodnotenia. S každým ďalším stupňom stúpa počet kombinácií pravdepodobnosti a dopadu. Pre kvantitatívne analýzy rizík existujú i špecializované softvérové nástroje.

V praktickej časti práce budeme posudzovať pravdepodobnosť hrozby zneužitím zraniteľnosti aktíva, dopad hrozby – do akej miery hrozba ovplyvní aktívum a klasifikáciu aktíva. Pre zjednodušenie vyberieme 21 základných hrozieb z katalógu nemeckého spolkového Úradu pre informačnú bezpečnosť (IT Grundschutz Catalogues, 2013)

V kvantitatívnej analýze rizík použijeme trojstupňovú stupnicu pravdepodobnosti hrozby (P) zneužitím zraniteľnosti:

Tab. 6 Hodnoty P a pravdepodobnosti hrozby

Hodnota P	Pravdepodobnosť hrozby
1	nepravdepodobné
2	málo pravdepodobné
3	pravdepodobné

Pre hodnotenie dopadu hrozby (D) zvolíme tiež trojstupňovú stupnicu:

Tab. 7 Hodnoty D a dopady hrozby

Hodnota D	Dopad hrozby
1	zanedbateľný
2	vážny
3	katastrofálny

Pre hodnotenie úrovne rizika volíme tento vzťah a tabuľku (Informačná bezpečnosť, 2013):

$$R = PD \tag{2}$$

Tab. 8 Hodnoty R a úrovne rizika

Hodnoty R	Úroveň rizika
1	zanedbateľná
2, 3, 4	akceptovateľná
6	poškodzujúca
9	neakceptovateľná

Riziká vyplývajúce z analýzy rizík, ktoré sú ohodnotené ako riziká poškodzujúce a neakceptovateľné, môžu mať významný negatívny vplyv na chod podniku. Je preto potrebné začať od neakceptovateľných rizík, znížiť ich úroveň na akceptovateľnú prijatím bezpečnostných opatrení.

4.5 Bezpečnostné opatrenia na zníženie miery rizika

Pri prijímaní bezpečnostných opatrení v organizácii je vhodné sa riadiť taktiež Demingovou metodikou. Len vypracovaním plánu ich implementácie, implementáciou, pravidelnou kontrolou ich účinnosti a nápravou prípadných nedostatkov môžeme docieliť želaný efekt.

Bezpečnostné opatrenia musia byť v pláne nasledujúcom po analýze rizík volené starostlivo. Je potrebné ich posudzovať v kontexte s ostatnými rizikami tak, aby sa vzájomne neprekrývali, nevylučovali a aby zavedením opatrenia nevzniklo nové riziko vytvorením novej zraniteľnosti aktíva.

4.6 Havarijné plány a plány obnovy

V podniku je dôležité myslieť i na zachovanie kontinuity jeho činností v prípade havárií. BCM (*Business Continuity Management*), v slovenskom jazyku ako riadenie kontinuity činností, má ako hlavný cieľ ochrániť majetok, dobré meno, povesť spoločnosti a tým pádom i majiteľov podniku pred finančnými stratami. Zavádzanie BCM sa odporúča ako pre veľké, tak i pre malé a stredné podniky.

Plány vypracovávané v rámci BCM by mali popisovať presné postupy po havárii tak, aby bolo možné v čo najkratšom čase obnoviť služby na minimálnu potrebnú úroveň. Docieliť takejto obnovy je možné len v prípade, ak bude mať podnik v

pláne BCM zadefinované pravidelné a dostatočné zálohovanie dát, pripravené náhradné softvérové, hardvérové a personálne zdroje. Plány by mali obsahovať podmienky spustenia havarijného plánu, poradie jednotlivých nápravných krokov, umiestnenia alternatívnych zdrojov, personálne role a ich úlohy.

Každý z informačných systémov by mal mať stanovené dva parametre:

- **RTO** sme si popísali už v analýze rizík. To, či dodržíme požadovanú hodnotu RTO závisí okrem veľkosti dát i na spôsobe zálohovania, pokiaľ máme dostatočnú kapacitu zálohovacích médií a môžeme si dovoliť zálohovať nielen dáta, ale i celý operačný systém. V prípade inkrementálnych alebo rozdelených záloh softvéru a dát sa táto doba väčšinou predlžuje, ale je obyčajne i úspornejšia.

  Ak poskytujeme externé služby, kde je podstatná i podmienka nepretržitej funkcionality, je pri stanovovaní RTO je potrebné zobrať do úvahy i maximálne doby tolerovaného výpadku v zmluvách so zákazníkmi. To, či systém plní systém zálohovania zvolený parameter RTO, je najvhodnejšie určiť testovaním procesu obnovy.
- **RPO (recovery point objective)** – stanovuje sa v časových jednotkách a popisuje, aký maximálny časový úsek si môže organizácia dovoliť stratiť od poslednej zálohy. Ak chceme, aby dáta pri obnove boli obnovené z predošlého dňa, postačí nastavenie na 24 hodín. To znamená, že budeme zálohovať každý deň, napr. v noci. Niektoré sofistikované systémy, ktoré zálohujú dáta systémom snímok (tzv. snapshot) neustále, sú schopné dodržať hodnotu RPO dokonca iba niekoľko desiatok minút. Takéto zálohovanie však už vyžaduje veľmi vysoké vstupné a prevádzkové finančné náklady.

Riadenie kontinuity činností podrobnejšie popisuje norma *BS 25999* vydaná britským normalizačným úradom. Podľa tejto normy je možné spoločnosť i certifikovať.

4.7 Efektívny systém riadenia informačnej bezpečnosti

Vo verejnej a súkromnej sfére sa výdavky na ochranu aktív neustále zvyšujú. Je to zapríčinené rýchlym vývojom technológii a informatizáciou jednotlivých činností podniku.

Je ale dôležité poukázať na fakt, že v časoch ekonomickej krízy je znižovanie nákladov na chod podniku často spojené s odsúvaním implementácie bezpečnostných opatrení na dobu neurčitú. Veľakrát sa k opatreniam, ktoré boli v pláne, vedenie podniku nevráti. Dôležitá je preto pravidelnosť analýzy rizík, prehodnocovanie potreby týchto opatrení, prípadne hľadanie alternatívnych, menej finančne náročných bezpečnostných opatrení a neustále obhajovanie ich dôležitosti manažmentu podniku.

Z pohľadu manažmentu podniku je nevyhnutné porovnávať výšku strát spôsobených využitím zraniteľností s výškou nákladov na bezpečnostné opatrenia, ktoré ich minimalizujú. Prílišný dôraz na úroveň informačnej bezpečnosti by však

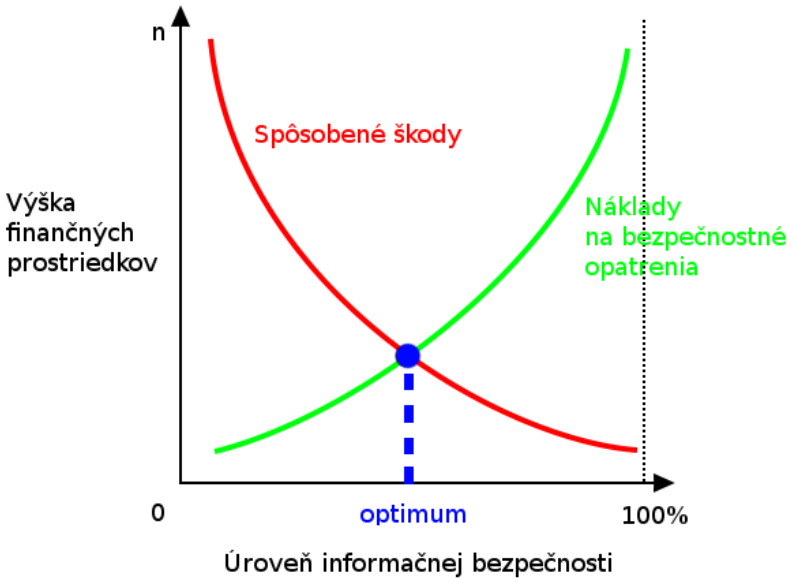
mohol mať za dôsledok zníženie pracovnej produktivity zamestnancov, vedomé obchádzanie bezpečnostných opatrení zamestnancami z dôvodu ich komplikovanosti alebo jednoducho nedostatku času.

4.8 Analýza dopadov na podnikanie

Po analýze rizík, návrhu protiopatrení a vytvorení plánov obnovy kontinuity činností sa v podnikoch často stáva, že sú parametre obnovy kontinuity nastavené príliš prísne, pretože každý vlastník aktíva požaduje po havárií obnovenie činnosti ihneď, čo stojí nemalé finančné a personálne prostriedky.

K efektívnemu nastaveniu nám pomôže vypracovanie analýzy dopadov chýbajúceho aktíva na podnikanie – **Business Impact Analysis**. Táto analýza by mala dať podniku odpovede na otázky ako dlho si môže podnik dovoliť nedostupnosť aktíva a koľko podnik bude táto nedostupnosť aktíva stáť.

Optimum výšky nákladov na bezpečnostné opatrenia sa nachádza v bode, kedy sú vynaložené prostriedky rovné výške potenciálne spôsobenej škody. V nasledujúcom grafe (Obr. 2) je znázornená naľavo od optima nedostatočná úroveň informačnej bezpečnosti, kedy je spôsobená škoda vyššia ako vynaložené prostriedky. Napravo je zobrazená taká úroveň bezpečnosti, ktorej zaistenie vyžaduje viac finančných prostriedkov ako je v skutočnosti hodnota chráneného aktíva, t.j. cena prípadných škôd je nižšia ako cena ochrany aktíva. V grafe je zároveň vidieť, že stopercentnú úroveň informačnej bezpečnosti nie je možné nikdy zaistiť.



Obr. 2 Graf zobrazujúci optimum nákladov na bezpečnostné opatrenia
Zdroj: Finance a bezpečnost, aneb peníze až na prvním místě, 2006.

Pri ohodnocovaní potenciálnej škody si musíme uvedomiť, že pri vyčleňovaní financií na bezpečnostné opatrenia nemôžeme brať do úvahy len stratené financie

spôsobené obmedzením podnikateľskej činnosti. Dlhodobejšie neposkytovanie zmluvných služieb zákazníkom, únik alebo krádež citlivých informácií, to sú situácie, v ktorých nám hrozí ukončenie zmluvy so zákazníkom, nemalé zmluvné sankcie alebo dokonca trestné oznámenie. Okrem zákazníkov nám môže pokutu vymerať Úrad na ochranu osobných údajov Slovenskej republiky v prípade, že sa medzi uniknutými informáciami nachádzajú osobné údaje. Ak má úrad dokonca pochybnosti o bezpečnosti spracúvania, je pravdepodobné, že podniku okrem pokuty zakáže spracúvanie osobných údajov na dlhšiu dobu.

Z obrázku je možné interpretovať i všeobecne rozšírený výrok, že podnik s veľmi vysokou úrovňou informačnej bezpečnosti má zraniteľnosti, ktoré môže potenciálny útočník využiť k útoku, otázkou je len výška sumy, ktorú je za získané citlivé dáta alebo diskreditáciu objektu ochotný objednávateľ útočníkovi zaplatiť napr. na čiernom trhu. Dôkazom, že niektoré organizácie sú schopné zaplatiť naozaj vysoké sumy, sú úspešné útoky na Pentagon v septembri 2015 (Telegraph, 2015) alebo na spoločnosť JPMorgan v roku 2014 (CNN, 2015).

5 Praktická časť

Ako ukážku testovania zraniteľností a následný návrh opatrení a finančného porovnávania sme si vybrali podnik z prostredia malého a stredného podnikania. Z pochopiteľného dôvodu nezverejňovania citlivých údajov zistených testovaním sme firmu pomenovali fiktívnym názvom Firma ABC, s.r.o. Premenovali sme a anonymizovali i všetky ostatné údaje, napr. názvy zákazníkov, IP adresy, mená zamestnancov, ktoré by mohli odhaliť identitu firmy.

5.1 Test zraniteľností vonkajšieho prostredia

5.1.1 Doména podniku

Podľa názvu firmy sme v internetovom vyhľadávači našli, že firma má internetovú stránku na doméne firmaabc.sk. Pomocou stránok národného správcu domén SK-NIC, a.s. www.sk-nic.sk sme zistili, že firma ABC je držiteľom danej domény. Zo záznamov sme tiež zistili, že registrátorom domény je registrátor s identifikátorom WEBS-0001, spoločnosť Websupport, s.r.o., ktorá je zároveň zrejme poskytovateľom webhostingových služieb.

5.1.2 DNS záznamy domény

Príkazom dig zisťujeme podrobnosti o doménových záznamy domény firmaabc.sk:

- **Zistené DNS servery domény:**
  - ns1.websupport.sk
  - ns2.websupport.sk
  - ns3.websupport.sk

- **Servery pre odosielanie elektronickej pošty:**
  - mailin1.firmaabc.sk
  - mailin2.firmaabc.sk
  - mailinbackup1.firmaabc.sk

- **SPF záznamy** – sú záznamy, ktoré povoľujú odosielanie elektronickej pošty z domény pre počítače mimo tejto domény.Podľa našich zistení je odosielanie povolené pre počítače v doméne websupport.sk.

```
mato@ares:~$ dig +nocmd firmaabc.sk any +multiline +noall +answer
firmaabc.sk.          10800 IN SOA ns1.websupport.sk. admin.websupport.sk. (
                            2014120101 ; serial
                            3600       ; refresh (1 hour)
                            2700       ; retry (45 minutes)
                            1048576    ; expire (1 week 5 days 3 hours 16 minutes 16 seconds)
                            2560       ; minimum (42 minutes 40 seconds)
                            )
firmaabc.sk.          86400 IN NS ns2.websupport.sk.
firmaabc.sk.          86400 IN NS ns3.websupport.sk.
firmaabc.sk.          86400 IN NS ns1.websupport.sk.
firmaabc.sk.          600 IN TXT "spf2.0/pra a mx include:_sid.websupport.sk -all"
firmaabc.sk.          600 IN TXT "v=spf1 a mx include:_spf.websupport.sk -all"
firmaabc.sk.          600 IN MX 10 mailin2.firmaabc.sk.
firmaabc.sk.          600 IN MX 100 mailinbackup1.firmaabc.sk.
firmaabc.sk.          600 IN MX 5 mailin1.firmaabc.sk.
firmaabc.sk.          600 IN A 37.9.175.12
```

Obr. 3 DNS záznamy domény firmaabc.sk príkazom dig

5.1.3 Subdomény domény firmaabc.sk

Na hľadanie subdomén sme využili program Knockpy. Zo všeobecne používaných subdomén sme našli týmto spôsobom 4 aktívne subdomény.

```
root@ares:~/knock/knockpy# knockpy firmaabc.sk
Target information firmaabc.sk

Ip Address        Target Name
----------        -----------
37.9.175.12       firmaabc.sk

Code              Reason
----------        -----------
301               Moved Permanently

Field             Value
----------        -----------
content-length    0
vary              User-Agent
server            openresty
connection        keep-alive
location          http://www.firmaabc.sk/
date              Tue, 16 Jun 2015 11:01:25 GMT
content-type      text/html; charset=UTF-8
x-pingback        http://www.firmaabc.sk/xmlrpc.php

: wildcard detected: 404

Loaded local wordlist with 1905 item(s)

Getting subdomain for firmaabc.sk

Ip Address        Domain Name
----------        -----------
195.210.29.66     admin.firmaabc.sk
37.9.175.12       mail.firmaabc.sk
37.9.175.12       webmail.firmaabc.sk
37.9.175.12       db.firmaabc.sk

Found 4 subdomain(s) in 2 host(s).
```

Obr. 4 Hľadanie subdomén domény firmabc.sk programom Knockpy

Spätným prekladom IP adries prichádzame na to, že tieto dve IP adresy patria spoločnosti, ktorá poskytuje webhosting.

```
mato@ares:~$ host 195.210.29.66
66.29.210.195.in-addr.arpa domain name pointer webadmin.websupport.sk.
mato@ares:~$ host 37.9.175.12
12.175.9.37.in-addr.arpa domain name pointer lb-proxy-10.websupport.sk.
```

Obr. 5 Zistenie reverzného záznamu IP adries príkazom host

Keďže slovník programu Knockpy neobsahuje názov softvérového produktu AbcSecure, ktorý je uvedený na internetovej stránke firmy, pokúsime sa otestovať ešte subdoménu abcsecure.firmaabc.sk, na ktorej je prevádzkovaná prezentačná stránka produktu príkazom host:

```
mato@ares:~$ host abcsecure.firmaabc.sk
abcsecure.firmaabc.sk has address 83.168.XXX.XXX
mato@ares:~$ host 83.168.XXX.XXX
XXX.XXX.168.83.in-addr.arpa domain name pointer 83-168-XXX-XXX.rev.swan.sk.
```

Obr. 6 Preklad doménového mena abcsecure.firmaabc.sk a zistenie reverzného záznamu

Zistením IP adresy subdomény a jej reverzného záznamu sme zistili, že IP adresa patrí do rozsahu spoločnosti, ktorá poskytuje v Slovenskej republike internetové pripojenie. Zrejme sa bude jednať o verejnú IP adresu firmy.

5.1.4 Zraniteľnosti webovej stránky www.firmaabc.sk

Zobrazením zdrojového kódu webovej stránky v internetovom prehliadači sme zistili, že HTML značka „meta“ s názvom „generator“ obsahuje hodnotu „WordPress 3.9.9" predpokladáme, že webová stránka na doméne www.firmaabc.sk používa systém na správu obsahu WordPress. Z tohto dôvodu použijeme nástroj WPScan a zisťujeme, že webová stránka používa tému vzhľadu „Spacious“, doplnok „Contact Form 7“ vo verzii 3.9.

Obr. 7 Testovanie zraniteľností redakčného systému WordPress

V čase testovania bola aktuálna verzia CMS WordPress 4.3.1, k nej i príslušná verzia tohto doplnku. Nové verzie opravujú viacero závažných bezpečnostných chýb, ich podrobné skúmanie nie je predmetom tejto práce.

5.1.5 Služby na verejnej IP adrese podniku

Keďže testujeme bezpečnosť počítačovej siete podniku, zaujíma nás z pohľadu testovania vonkajšieho prostredia podniku len zistená verejná IP adresa 83.168.XXX.XXX. Adresu otestujeme na povolené ICMP Echo Request.

```
mato@ares:~$ ping -c 10 83.168.XXX.XXX
PING 83.168.XXX.XXX (83.168.XXX.XXX) 56(84) bytes of data.

--- 83.168.XXX.XXX ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9070ms
```

Obr. 8 Preklad doménového mena abcsecure.firmaabc.sk a zistenie reverzného záznamu

Z výsledku príkazu zisťujeme, že ICMP Echo Request (Ping) nie je povolené. ďalej budeme skenovať porty tcp v rozsahu 1-10000, pretože niektoré služby (napr. vývojové servery) bežia na portoch vyšších ako štandardne bez tejto voľby program Nmap testuje. Porty udp nie sú predmetom nášho skúmania z dôvodu veľmi zdĺhavého skenovania (Port Scanning Techniques, 2015).

Testujeme teda IP adresu na otvorené porty tcp 1-10000 programom Nmap s voľbami:

- -v – výpis detailov
- -O – detekcia operačného systému
- -sV – Zistiť verziu a typ služby na otvorených portoch
- -sS – skenovanie pomocou TCP SYN paketu

Skenovaním sme zistili, že na portoch 80/tcp a 443/tcp funguje webový server Apache2 s modulmi mod_fastcgi, mod_wsgi s podporou programovacieho jazyka Python 2.7.3 a knižnice OpenSSL/1.0.1.

Verzia webového servera. Apache 2.4.16 je podľa stránky produktu posledná stabilná verzia serveru. Server je pravdepodobne pravidelne aktualizovaný.

Na porte 2223/tcp počúva služba SSH vo verzii OpenSSH 5.9p1, a pokiaľ je operačný systém servera pravidelne aktualizovaný, nemal by obsahovať žiadne kritické zraniteľnosti.

```
mato@ares:~$ nmap -v -O -sV -sS -p 1-10000 83.168.XXX.XXX
Starting Nmap 6.00 ( http://nmap.org ) at 2015-08-21 12:56 EEST
NSE: Loaded 17 scripts for scanning.
Initiating SYN Stealth Scan at 12:56
Scanning 83.168.XXX.XXX (83.168.XXX.XXX) [10000 ports]
Discovered open port 80/tcp on 83.168.XXX.XXX
Discovered open port 443/tcp on 83.168.XXX.XXX
Increasing send delay for 83.168.XXX.XXX from 0 to 5 due to 11 out of 16 dropped probes since last
increase.
SYN Stealth Scan Timing: About 4.56% done; ETC: 09:07 (0:10:49 remaining)
Increasing send delay for 83.168.XXX.XXX from 5 to 10 due to 11 out of 16 dropped probes since last
increase.
SYN Stealth Scan Timing: About 5.45% done; ETC: 09:15 (0:17:39 remaining)
SYN Stealth Scan Timing: About 6.24% done; ETC: 09:20 (0:22:49 remaining)
SYN Stealth Scan Timing: About 7.20% done; ETC: 09:24 (0:26:01 remaining)
SYN Stealth Scan Timing: About 8.34% done; ETC: 09:26 (0:27:40 remaining)
SYN Stealth Scan Timing: About 20.11% done; ETC: 09:29 (0:26:05 remaining)
SYN Stealth Scan Timing: About 25.86% done; ETC: 09:29 (0:24:25 remaining)
SYN Stealth Scan Timing: About 31.40% done; ETC: 09:29 (0:22:45 remaining)
Discovered open port 2223/tcp on 83.168.XXX.XXX
SYN Stealth Scan Timing: About 36.12% done; ETC: 09:29 (0:21:04 remaining)
SYN Stealth Scan Timing: About 40.98% done; ETC: 09:29 (0:19:24 remaining)
SYN Stealth Scan Timing: About 46.23% done; ETC: 09:29 (0:17:42 remaining)
SYN Stealth Scan Timing: About 51.47% done; ETC: 09:29 (0:16:03 remaining)
SYN Stealth Scan Timing: About 56.63% done; ETC: 09:29 (0:14:22 remaining)
SYN Stealth Scan Timing: About 61.69% done; ETC: 09:29 (0:12:41 remaining)
SYN Stealth Scan Timing: About 66.68% done; ETC: 09:29 (0:11:02 remaining)
SYN Stealth Scan Timing: About 71.80% done; ETC: 09:29 (0:09:22 remaining)
SYN Stealth Scan Timing: About 76.85% done; ETC: 09:29 (0:07:42 remaining)
SYN Stealth Scan Timing: About 82.04% done; ETC: 09:30 (0:05:59 remaining)
SYN Stealth Scan Timing: About 87.09% done; ETC: 09:29 (0:04:18 remaining)
SYN Stealth Scan Timing: About 92.22% done; ETC: 09:29 (0:02:35 remaining)
SYN Stealth Scan Timing: About 97.34% done; ETC: 09:30 (0:00:53 remaining)
Completed SYN Stealth Scan at 13:30, 2001.07s elapsed (10000 total ports)
Initiating Service scan at 13:30
Scanning 3 services on 83.168.XXX.XXX (83.168.XXX.XXX)
Completed Service scan at 13:30, 13.60s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 83.168.XXX.XXX (83.168.XXX.XXX)
Retrying OS detection (try #2) against 83.168.XXX.XXX (83.168.XXX.XXX)
NSE: Script scanning 83.168.XXX.XXX.
[+] Nmap scan report for 83.168.XXX.XXX (83.168.XXX.XXX)
Host is up (0.068s latency).
Not shown: 9997 filtered ports
PORT      STATE   SERVICE   VERSION
80/tcp    open    http      Apache httpd 2.4.16 ((Ubuntu) mod_fastcgi/mod_fastcgi-SNAP-0910052141
OpenSSL/1.0.1 mod_wsgi/3.4 Python/2.7.3)
443/tcp   open    ssl/http  Apache httpd 2.4.16 ((Ubuntu) mod_fastcgi/mod_fastcgi-SNAP-0910052141
OpenSSL/1.0.1 mod_wsgi/3.4 Python/2.7.3)
2223/tcp  open    ssh       OpenSSH 5.9p1 Debian 5ubuntu1.7 (protocol 2.0)
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (87%)
OS CPE: cpe:/o:linux:kernel:2.6
Aggressive OS guesses: Linux 2.6.32 - 2.6.38 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 126.853 days (since Tue Jun 2 13:02:16 2015)
Network Distance: 15 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```

Obr. 9 Skenovanie vonkajšej IP adresy programom Nmap

Analýzou zdrojového kódu internetovej stránky na portoch 80 a 443 zisťujeme, že stránka je vygenerovaná programom HTTrack.

```
<!-- Mirrored by HTTrack Website Copier/3.x [XR&CO'2010] -->
<!-- Added by HTTrack --><meta http-equiv="content-type" content="text/html; charset=UTF-8" ><!-- /Added by HTTrack -->
```

Obr. 10 Úsek HTML kódu internetovej stránky produktu

Podľa internetovej stránky tohto programu tento program slúži na generovanie statickej verzie internetovej stránky z dynamickej verzie. Stránku ďalej ne-

skúmame, pretože pravdepodobne neobsahuje žiadne dynamické prvky – skripty – ktoré by bolo možné zneužiť na prípadný útok.

5.1.6 Zistené zraniteľnosti z vonkajšieho prostredia

Testovaním vonkajšieho prostredia sme nezistili žiadne závažné bezpečnostné zraniteľnosti počítačovej siete, ktoré by mohli podnik ohroziť. Najväčšou bezpečnostnou slabinou podniku v budúcnosti môže byť internetová stránka podniku, ktorá využíva na správu obsahu systém WordPress. Ten by mal byť pravidelne aktualizovaný.

Ďalšou potenciálnou zraniteľnosťou môže byť prípadné nedodržovanie vnútorných pravidiel podniku týkajúcich sa používania hesiel. Tie môžu byť ľahko uhádnuteľné slovníkovým útokom na službu SSH. Po rozhovoroch so správcom IT je však na bráne podniku nainštalovaný program, ktorý blokuje tie IP adresy po dobu 1 týždňa, z ktorých používateľ zadal päťkrát nesprávne heslo počas 1 dňa. Z tohto dôvodu zraniteľnosť nepovažujeme za závažnú.

5.2 Informačná bezpečnosť z vnútorného prostredia podniku

5.2.1 Popis podniku

Firma ABC, s.r.o. patrí medzi malé podniky, v súčasnosti veľmi rýchlo rastie. Hlavným zdrojom príjmov je vývoj a prevádzka aplikácie AbcSecure, ktorá slúži na komunikáciu firiem so zákazníkmi, evidenciu zmlúv a stráženie kľúčových termínov, evidenciu práce jednotlivých zamestnancov a ako nástroj na ukladanie internej dokumentácie firiem.

V čase testovania poskytovala tieto služby pre 11 klientov z oblasti malého a stredného podnikania, pričom najväčším klientom je finančná spoločnosť, ktorá aktívne využíva 150 používateľských účtov. Podnik zamestnáva v súčasnosti 9 zamestnancov:

- riaditeľ podniku a zároveň obchodný zástupca,
- expert na legislatívu,
- analytik,
- 3 programátori,
- dizajnér,
- správca IT,
- personalistka a účtovníčka v 1 osobe.

5.2.2 Okolie podniku

Oblasť sídla podniku sa nenachádza v záplavovej oblasti, nie je ohrozená častými požiarmi a ani nepatrí medzi seizmologicky aktívne oblasti. Živelné katastrofy nikdy nemožno úplne vylúčiť, ale pre účely skúmania zraniteľností počítačovej siete podniku je pravdepodobnosť týchto hrozieb zanedbateľná. Podnik má priestory

navyše proti živelným katastrofám poistené a je teda možné ich z potenciálnych zraniteľností vylúčiť.

5.2.3 Fyzická bezpečnosť podnikových priestorov

Firma ABC, s.r.o. sídli v kanceláriách na 1. poschodí budovy, ktorej časť si podnik prenajíma od spoločnosti poskytujúcej prenájom kancelárskych priestorov. Táto spoločnosť prenajíma kancelárie v celej budove, sú strážené bezpečnostnou službou a kamerovým systémom. Firma používa k zabezpečeniu vlastných priestorov vlastný elektronický zabezpečovací systém s integrovanou kamerou a pohybovými detektormi s GSM hlásičom prepojeným na majiteľa firmy a správcu IT.

Aplikačný server a diskové pole sú v miestnosti bez okien a oddelenej od kancelárie mrežou so zámkom a chránené okrem detektora pohybu u protipožiarnym detektorom. V miestnosti je funkčná klimatizačná jednotka. V stenách a nad miestnosťou nie sú rozvody vody alebo odpadov, ktoré by v prípade ich prasknutia mohli ohroziť zariadenia v miestnosti.

Optické káble internetového pripojenia a elektrickej inštalácie vedúce do kancelárií sú oddelené od chodieb stenou a revízne dvere stúpačiek sú chránené zámkom a kamerovým systémom majiteľa budovy. Bezprostredne teda nehrozí riziko odpočúvania komunikácie na fyzickej úrovni.

Vzhľadom k veľkosti firmy a citlivosti spracúvaných dát považujeme fyzickú bezpečnosť podnikových priestorov za adekvátnu.

5.2.4 Stav systému riadenia informačnej bezpečnosti a dokumentácie

Pohovorom s riaditeľom firmy sme zistili, že systém riadenia informačnej bezpečnosti nie je implementovaný, nie je vypracovaný ani plán, či analýza rizík. Bezpečnostné opatrenia týkajúce sa bezprostredne počítačovej siete aplikuje správca bez akejkoľvek koncepcie IT podľa potreby. Odolnosť počítačovej siete nie je pravidelne testovaná.

Podnik nemá vypracovanú bezpečnostnú politiku. Pri malej firme to nepovažujeme za zraniteľnosť, avšak jej vypracovanie a prípadné zverejnenie by podniku pridalo na dôveryhodnosti.

Podnik v informačných systémoch spracúva osobné údaje a informačný systém AbcSecure, ktorý spracúva osobné údaje, je prístupný z verejnej siete. Z tohto dôvodu musí mať podnik zo zákona č. 164/2013 Z. z. o ochrane osobných údajov vypracovaný bezpečnostný projekt, ktorý zahŕňa bezpečnostný zámer, evidenciu informačných údajov a bezpečnostné smernice.

Podnik má tiež na Úrade na ochranu osobných údajov zaregistrovanú zodpovednú osobu, ktorú vykonáva zamestnanec – expert na legislatívu – ktorý má zároveň platný certifikát - skúšku zodpovednej osoby. Z tohto dôvodu nie je potrebné tieto systémy registrovať na Úrade na ochranu osobných údajov Slovenskej republiky.

Bezpečnostný projekt podnik vypracovaný nemá, udržuje len evidenčné listy informačných systémov osobných údajov a z bezpečnostného projektu dokumen-

táciu tvoria len bezpečnostné smernice, ktoré sa týkajú informačnej bezpečnosti a je v nich zmienka o ochrane osobných údajov.

5.3 Identifikácia aktív podniku

Po konzultácii s riaditeľom podniku a správcom IT sme identifikovali základné aktíva podniku, ktoré sa týkajú informačnej bezpečnosti, určili požiadavky na dôvernosť, integritu a dostupnosť. Rozhovorom s riaditeľom podniku o poskytovaných službách zákazníkom vyplývajúcich zo zmlúv, ktoré spoločnosť uzavrela, sme určili parameter RTO. Následne sme previedli klasifikáciu aktív do 3 kategórií.

Tab. 9 Klasifikácia aktív spoločnosti Firma ABC, s.r.o.

Aktívum	Dostupnosť	Dôvernosť	Integrita	RTO	Klasifikácia
Diskové pole a aplikačný server	neakceptovateľné	mimoriadne citlivé	kritické	48 hodín	kritické
Aplikácia AbcSecure	neakceptovateľné	mimoriadne citlivé	katastrofálne	48 hodín	kritické
Webová stránka	poškodzujúce	verejné	vážne	72 hodín	dôležité
Server elektronickej pošty	poškodzujúce	citlivé	vážne	72 hodín	dôležité
Mobilné zariadenia	akceptovateľné	citlivé	vážne	1 týždeň	dôležité
Osobné počítače	poškodzujúce	interné	kritické	48 hodín	dôležité
Osobné údaje	poškodzujúce	mimoriadne citlivé	kritické	72 hodín	kritické
Sieťová infraštruktúra	neakceptovateľné	citlivé	kritické	48 hodín	kritické
Používateľská dokumentácia	zanedbateľné	interné	okrajové	2 týždne	bežné
Kancelársky softvér	poškodzujúce	interné	kritické	2 týždne	dôležité
Dokumentácia podniku	poškodzujúce	citlivé	kritické	1 týždeň	dôležité

5.4 Analýza rizík kritických aktív

Z klasifikácie aktív vyberieme pre testovanie zraniteľností z vnútorného prostredia len tie aktíva, ktoré sú klasifikované ako kritické. Prevedieme analýzu rizík kritických aktív. Riziká s poškodzujúcou a neakceptovateľnou úrovňou spôsobujú zraniteľnosti, ktoré stručne k jednotlivým aktívam popíšeme.

5.4.1 Diskové pole a aplikačný server

Tab. 10 Tabuľka analýzy rizík kritického aktíva „Diskové pole a aplikačný server“

Č.	Hrozba	Pravdepodobnosť	Dopad	Miera rizika
1.1	Chyby zamestnancov	málo pravdepodobné	vážny	zanedbateľná
1.2	Chyby dodávateľa	nepravdepodobné	katastrofálny	akceptovateľná
1.3	Neautorizovaná činnosť	nepravdepodobné	vážny	akceptovateľná
1.4	Chyby komunikácie	málo pravdepodobné	vážny	akceptovateľná
1.5	Chyby a poruchy zariadenia	málo pravdepodobné	katastrofálny	poškodzujúca
1.6	Chyby programového vybavenia	nepravdepodobné	vážny	akceptovateľná
1.7	Podvod	nepravdepodobné	vážny	akceptovateľná
1.8	Zničenie údajov a konfigurácii	málo pravdepodobné	vážny	akceptovateľná
1.9	Krádež	nepravdepodobné	katastrofálny	akceptovateľná
1.10	Nedostatok ľudských zdrojov	málo pravdepodobné	vážny	akceptovateľná
1.11	Zhromažďovanie údajov	málo pravdepodobné	vážny	akceptovateľná
1.12	Nedostatok finančných zdrojov	málo pravdepodobné	vážny	akceptovateľná
1.13	Odmietnutie služby	málo pravdepodobné	vážny	akceptovateľná
1.14	Narušenie dodávok elektrickej energie	málo pravdepodobné	vážny	akceptovateľná
1.15	Únik údajov	nepravdepodobné	katastrofálny	akceptovateľná
1.16	Prinútenie k spolupráci	nepravdepodobné	katastrofálny	akceptovateľná
1.17	Nesprávne interpretovaná legislatíva	nepravdepodobné	zanedbateľný	zanedbateľná
1.18	Negatívne vplyvy prostredia	nepravdepodobné	vážny	akceptovateľná
1.19	Výtržnosti a protesty	nepravdepodobné	vážny	akceptovateľná
1.20	Prírodné katastrofy a priemyselné nehody	nepravdepodobné	vážny	akceptovateľná
1.21	Terorizmus	nepravdepodobné	vážny	akceptovateľná

5.4.2 Aplikácia AbcSecure

Tab. 11 Tabuľka analýzy rizík kritického aktíva „Aplikácia AbcSecure“

Č	Hrozba	Pravdepodobnosť	Dopad	Miera rizika
2.1	Chyby zamestnancov	málo pravdepodobné	katastrofálny	poškodzujúca
2.2	Chyby dodávateľa	nepravdepodobné	zanedbateľný	zanedbateľná
2.3	Neautorizovaná činnosť	málo pravdepodobné	katastrofálny	poškodzujúca
2.4	Chyby komunikácie	nepravdepodobné	vážny	akceptovateľná
2.5	Chyby a poruchy zariadenia	nepravdepodobné	katastrofálny	akceptovateľná
2.6	Chyby programového vybavenia	pravdepodobné	katastrofálny	neakceptovateľná
2.7	Podvod	nepravdepodobné	katastrofálny	akceptovateľná
2.8	Zničenie údajov a konfigurácii	málo pravdepodobné	katastrofálny	poškodzujúca

2.9	Krádež	nepravdepodobné	katastrofálny	akceptovateľná
2.10	Nedostatok ľudských zdrojov	málo pravdepodobné	vážny	akceptovateľná
2.11	Zhromažďovanie údajov	málo pravdepodobné	vážny	akceptovateľná
2.12	Nedostatok finančných zdrojov	málo pravdepodobné	vážny	akceptovateľná
2.13	Odmietnutie služby	málo pravdepodobné	vážny	akceptovateľná
2.14	Narušenie dodávok elektrickej energie	málo pravdepodobné	vážny	akceptovateľná
2.15	Únik údajov	pravdepodobné	katastrofálny	neakceptovateľná
2.16	Prinútenie k spolupráci	nepravdepodobné	katastrofálny	akceptovateľná
2.17	Nesprávne interpretovaná legislatíva	nepravdepodobné	vážny	akceptovateľná
2.18	Negatívne vplyvy prostredia	nepravdepodobné	zanedbateľný	zanedbateľná
2.19	Výtržnosti a protesty	nepravdepodobné	zanedbateľný	zanedbateľná
2.20	Prírodné katastrofy a priemyselné nehody	nepravdepodobné	zanedbateľný	zanedbateľná
2.21	Terorizmus	nepravdepodobné	vážny	akceptovateľná

5.4.3 Sieťová infraštruktúra

Tab. 12 Tabuľka analýzy rizík kritického aktíva „Sieťová infraštruktúra“

Č	Hrozba	Pravdepodobnosť	Dopad	Miera rizika
3.1	Chyby zamestnancov	málo pravdepodobné	katastrofálny	poškodzujúca
3.2	Chyby dodávateľa	nepravdepodobné	zanedbateľný	zanedbateľná
3.3	Neautorizovaná činnosť	málo pravdepodobné	katastrofálny	poškodzujúca
3.4	Chyby komunikácie	málo pravdepodobné	vážny	akceptovateľná
3.5	Chyby a poruchy zariadenia	málo pravdepodobné	katastrofálny	poškodzujúca
3.6	Chyby programového vybavenia	málo pravdepodobné	katastrofálny	poškodzujúca
3.7	Podvod	nepravdepodobné	vážny	akceptovateľná
3.8	Zničenie údajov a konfigurácii	málo pravdepodobné	katastrofálny	poškodzujúca
3.9	Krádež	nepravdepodobné	vážny	akceptovateľná
3.10	Nedostatok ľudských zdrojov	málo pravdepodobné	vážny	akceptovateľná
3.11	Zhromažďovanie údajov	málo pravdepodobné	vážny	akceptovateľná
3.12	Nedostatok finančných zdrojov	málo pravdepodobné	vážny	akceptovateľná
3.13	Odmietnutie služby	málo pravdepodobné	katastrofálny	poškodzujúca
3.14	Narušenie dodávok elektrickej energie	málo pravdepodobné	vážny	akceptovateľná
3.15	Únik údajov	málo pravdepodobné	vážny	akceptovateľná
3.16	Prinútenie k spolupráci	nepravdepodobné	katastrofálny	akceptovateľná
3.17	Nesprávne interpretovaná legislatíva	nepravdepodobné	zanedbateľný	zanedbateľná
3.18	Negatívne vplyvy prostredia	nepravdepodobné	zanedbateľný	zanedbateľná
3.19	Výtržnosti a protesty	nepravdepodobné	zanedbateľný	zanedbateľná
3.20	Prírodné katastrofy	nepravdepodobné	zanedbateľný	zanedbateľná

	a priemyselné nehody			
3.21	Terorizmus	nepravdepodobné	vážny	akceptovateľná

5.4.4 Osobné údaje

Tab. 13 Tabuľka analýzy rizík kritického aktíva „Osobné údaje“

Č.	Hrozba	Pravdepodobnosť	Dopad	Miera rizika
4.1	Chyby zamestnancov	málo pravdepodobné	katastrofálny	poškodzujúca
4.2	Chyby dodávateľa	nepravdepodobné	zanedbateľný	zanedbateľná
4.3	Neautorizovaná činnosť	málo pravdepodobné	katastrofálny	poškodzujúca
4.4	Chyby komunikácie	nepravdepodobné	vážny	akceptovateľná
4.5	Chyby a poruchy zariadenia	nepravdepodobné	zanedbateľný	zanedbateľná
4.6	Chyby programového vybavenia	nepravdepodobné	zanedbateľný	zanedbateľná
4.7	Podvod	nepravdepodobné	vážny	akceptovateľná
4.8	Zničenie údajov a konfigurácii	nepravdepodobné	katastrofálny	akceptovateľná
4.9	Krádež	málo pravdepodobné	katastrofálny	poškodzujúca
4.10	Nedostatok ľudských zdrojov	málo pravdepodobné	zanedbateľný	akceptovateľná
4.11	Zhromažďovanie údajov	málo pravdepodobné	vážny	akceptovateľná
4.12	Nedostatok finančných zdrojov	málo pravdepodobné	vážny	akceptovateľná
4.13	Odmietnutie služby	málo pravdepodobné	zanedbateľný	akceptovateľná
4.14	Narušenie dodávok elektrickej energie	málo pravdepodobné	vážny	akceptovateľná
4.15	Únik údajov	málo pravdepodobné	katastrofálny	poškodzujúca
4.16	Prinútenie k spolupráci	nepravdepodobné	katastrofálny	akceptovateľná
4.17	Nesprávne interpretovaná legislatíva	málo pravdepodobné	katastrofálny	poškodzujúca
4.18	Negatívne vplyvy prostredia	nepravdepodobné	zanedbateľný	zanedbateľná
4.19	Výtržnosti a protesty	nepravdepodobné	zanedbateľný	zanedbateľná
4.20	Prírodné katastrofy a priemyselné nehody	nepravdepodobné	zanedbateľný	zanedbateľná
4.21	Terorizmus	nepravdepodobné	vážny	akceptovateľná

5.5 Zraniteľnosti kritických aktív

5.5.1 Diskové pole a aplikačný server

Zariadenia sú umiestnené v serverovej miestnosti. Kompletný servis hardvéru zabezpečuje externý dodávateľ. Hardvér bol zakúpený v roku 2011. V budúcnosti je možné očakávať častejšie výpadky z dôvodu nepretržitej prevádzky a vyššiemu veku komponentov. Posledný rok boli chyby hardvéru pomerne časté, na mesačnej báze. Dodávateľ problém vždy vyriešil do 3 dní v súlade so servisnou zmluvou.

Softvér aplikačného servera a diskového poľa spravuje interný správca IT, ktorý je skúseným správcom operačných systémov Linux. Softvér diskového poľa

a aplikačného servera je pravidelne aktualizovaný a zálohované sú iba nastavenia operačného systému a aplikácii, nie celý obraz systému. Zálohy prebiehajú automaticky každú noc na špeciálne zálohovacie média zálohovacím zariadením spolu s dátami aplikačného softvéru. Pásky v zariadení rotujú. Raz za týždeň v zariadení správca IT vymieňa najaktuálnejšiu zálohovaciu pásku za najstaršiu z 3 kusov, ktoré sú je ponechané v zamknutej skrini v kancelárii pre prípad zlyhania zálohovacieho zariadenia.

Diskové pole a aplikačný server sú pripojené na záložný zdroj dostatočnej kapacity, nedávno bol vymenený akumulátor.

Tab. 14 Zistené zraniteľnosti aktíva „Diskové pole a aplikačný server“

Číslo	Zraniteľnosť	Riziká
Z 1.1	**Pravdepodobná chyba hardvéru diskového poľa** Servis diskového poľa podniku je zmluvne ošetrený s dodávateľom, ktorému zo servisnej zmluvy vyplývajú povinnosti zabezpečiť opravu diskového poľa do 3 pracovných dní od nahlásenia chyby. Závada diskového poľa však spôsobí kompletnú nedostupnosť akýchkoľvek dát systému AbcSecure, podnik bude musieť počítať so zmluvnými pokutami a nižším ziskom alebo dokonca stratou.	R 1.5
Z 1.2	**Pravdepodobná chyba hardvéru aplikačného servera** Servis aplikačného serveru podniku je zmluvne ošetrený s dodávateľom, ktorému zo servisnej zmluvy vyplývajú povinnosti zabezpečiť opravu diskového poľa do 3 pracovných dní od nahlásenia chyby. Závada diskového poľa však spôsobí kompletnú nedostupnosť akýchkoľvek dát systému AbcSecure, podnik bude musieť počítať so zmluvnými pokutami a strateným ziskom.	R 1.5
Z 1.3	**Nedostatočné zálohovanie aplikačného servera** Zálohované sú iba konfigurácie servera. V prípade výpadku môže táto konfigurácia spôsobiť spomalenie obnovy z dôvodu nutnosti inštalácie celého operačného systému.	R 1.5
Z 1.4	**Zálohy nie sú umiestnené mimo budovu podniku** V prípade požiaru alebo inej prírodnej katastrofy môžu byť zálohy nenávratne zničené.	R 1.8

5.5.2 Aplikácia AbcSecure

Aplikácia AbcSecure je prevádzkovaná vo virtuálnom prostredí na aplikačnom serveri. Každý zákazník má vyhradené dva virtuálne servery, jeden produkčný a jeden testovací. K obom verziám pristupuje cez „site-to-site“ VPN tunel, ktorý je pre každého zo zákazníkov vytvorený zvlášť. Každý virtuálny server je zálohovaný pomocou snímok, dáta sú zálohované vcelku každú noc. Zálohovanie prebieha spoločne so zálohovaním aplikačného servera. Výpadky systému doteraz v podniku zaznamenané neboli.

Tab. 15 Zraniteľnosti aktíva „Aplikácia AbcSecure“

Číslo	Zraniteľnosť	Riziká
Z 2.1	**Testovacie rozhranie aplikácie je prístupné z internetu** Testovacie rozhranie aplikácie pre niektoré firmy je dostupné z internetu na verejnej IP adrese podniku na porte tcp/443. Je možné, že je to pozostatok z testovania VPN tunelov. Testovacia verzia môže obsahovať rôzne zraniteľnosti, ktoré neboli ešte otestované a opravené. Útočník môže tieto zraniteľnosti zneužiť a získať citlivé údaje alebo pozmeniť zdrojový kód aplikácie.	R 2.3, R 2.6, R 2.8, R 2.15
Z 2.2	**Testovacie verzie môžu obsahovať osobné údaje a iné citlivé údaje** Bezpečnostné smernice žiadnym spôsobom neupravujú používanie dát v testovacích verziách. Kvôli neopraveným zraniteľnostiam hrozí únik citlivých a osobných údajov.	R 2.1, R 2.3, R 2.6, R 2.8, R 2.15
Z 2.3	**Nedostatočné testovanie aplikácie pred nasadením do produkčného prostredia** Príliš časté chyby môžu viesť k nespokojnosti zákazníka, strate alebo únikom dát, obídeniu autorizačných mechanizmov používateľov, nesprávnej funkcionalite aplikácie. Podnik nevenuje veľkú pozornosť dôkladnému testovaniu aplikácie.	R 2.3, R 2.6, R 2.8, R 2.15
Z 2.4	**Zálohy nie sú umiestnené mimo budovu podniku** V prípade požiaru alebo inej prírodnej katastrofy môžu byť zálohy nenávratne zničené.	R 2.8

5.5.1 Sieťová infraštruktúra

Sieťová infraštruktúra je tvorená tromi rozbočovačmi a chránená bránou FortiGate od spoločnosti Fortinet. Podnik má uzavretú zmluvu s poskytovateľom internetového pripojenia so garanciou opravy chýb pripojenia do 12 hodín.
Samotná počítačová sieť je rozdelená na 4 podsiete:

- **10.0.0.0/24**
  V tejto počítačovej sieti sú pripojené počítače zamestnancov. Prístup z tejto podsiete je povolený len smerom do internetu, do siete 10.0.10.0/24 a na virtuálne servery pre zákazníkov v rozsahu 10.0.20.10 až 10.0.20.21.
- **10.0.10.0/24**
  Táto sieť je vyhradená pre diskové pole, aplikačný server a server s webom produktu AbcSecure, službami elektronickej pošty a zdieľaným priečinkom.
- **10.0.20.0/24**
  V tejto sieti sú jednotlivé virtuálne servery s aplikáciou AbcSecure pre zákazníkov, prístup z tejto siete je povolený len k serverom s aktualizáciami operačného systému a e-mailovému serveru, ktorý beží v sieti 10.0.10/24.
- **10.0.30.0/24**

Sieť vytvorená pre VPN prístup zákazníkov. Každý zákazník má pridelenú pevnú IP adresu. Z jednotlivých IP adries sú povolené prístupy len k potrebným službám príslušných virtuálnych serverov zákazníka v podsieti 10.0.20.0/24.

Tab. 16 Zraniteľnosti aktíva „Sieťová infraštruktúra“

Číslo	Zraniteľnosť	Riziká
Z 3.1	**Podnik nemá zavedenú autentizáciu v počítačovej sieti** Sieťové prvky Zamestnanec môže pripojiť akékoľvek zariadenie do počítačovej siete, zariadeniu bude pridelená IP adresa. Pokiaľ je na pripojenom zariadení nainštalovaný škodlivý softvér, môže dôjsť k odpočúvaniu sieťovej komunikácie, zachytávaniu citlivých informácií, únikom dát, prípadne k jeho rozšíreniu na počítače zamestnancov.	R 3.1, R 3.3
Z 3.2	**Podnik nedisponuje záložnými sieťovými prvkami** V prípade poruchy sieťovej brány (zariadenie FortiGate) alebo rozbočovačov zostane nefunkčná celá sieť. Pre uvedenie do pôvodného stavu je potrebné chybný prvok zakúpiť a nakonfigurovať.	R 3.5
Z 3.3	**Softvér sieťovej brány nie je aktuálny** Podnik už druhý rok neplatí softvérovú podporu - aktualizácie operačného systému FortiGate. Je možné, že neaktualizovaná verzia obsahuje chyby, ktoré môže zneužiť útočník k získaniu prístupu k citlivým dátam, nedostatočnú ochranu pred novými zraniteľnosťami, nedostatočné filtrovanie elektronickej pošty.	R 3.3, R 3.6
Z 3.4	**Konfiguračné súbory sieťovej brány nie sú pravidelne zálohované** V prípade poruchy sieťovej brány je potrebné okrem zakúpenia bránu i manuálne nakonfigurovať, čo násobne predlžuje čas obnovy a môže spôsobiť chyby v konfigurácii.	R 3.8
Z 3.5	**Chýba zabezpečenie voči útokom odmietnutia služby (DoS)** Útoky odmietnutia služby (DoS – denial of service) sú spravidla útokom z vonkajšieho prostredia podniku. Spôsobujú preťaženie zariadení/aplikácií veľmi vysokým počtom požiadaviek, z dôvodu ktorého sa služby, ktoré poskytujú, spomalia, prípadne stanú nedostupnými. Sieťová brána podniku obsahuje modul, ktorý je schopný zabrániť útokom odmietnutia služby. Nie je však aktívny, pretože podnik nemá platenú softvérovú podporu zariadenia od spoločnosti Fortinet.	R 3.13

5.5.2 Osobné údaje

Osobné údaje podnik spracúva ako v aplikácii AbcSecure, tak i v internej dokumentácii podniku – personálnej a mzdovej agende. V týchto systémoch podnik

spracúva i všeobecný identifikátor osôb – rodné číslo, ktorý je považovaný podľa zákona za osobný údaj osobitnej kategórie.

V aplikácii AbcSecure, ktorá je prístupná z verejnej siete, sa spracúvajú najmä osobné údaje o zamestnancoch zákazníka a jeho klientov.

Vzhľadom na hlavnú činnosť podnikania všetci zamestnanci podniku prichádzajú do styku s osobnými údajmi a teda povereným zamestnancom je každý z nich. Školenie zamestnancov podniku o ochrane osobných údajov neprebieha pravidelne, zamestnanci sú poučení len pri nástupe do zamestnania.

Tab. 17 Zraniteľnosti aktíva „Osobné údaje“

Číslo	Zraniteľnosť	Riziká
Z 4.1	**Chýba pravidelné školenie zamestnancov** Zamestnanci sú školení len pri nástupe do zamestnania. Absencia pravidelných školení zamestnancov znižuje povedomie o potrebe ochrany osobných údajov.	R 4.1
Z 4.2	**Dokumentácia týkajúca sa ochrany osobných údajov podniku nie je v súlade s legislatívou** • chýba vypracovaná analýza rizík, • bezpečnostné smernice sú nedostatočné z pohľadu ochrany osobných údajov.	R 4.17
Z 4.3	**Dáta nie sú bezpečne vymazané pred odovzdaním na likvidáciu alebo servis** Odovzdanie média alebo zariadenia, z ktorého je možné zrekonštruovať citlivé alebo osobné údaje, ktoré boli na ňom uchovávané, znamená únik informácií. Predpis, ktorý toto prikazuje, chýba v bezpečnostných smerniciach.	R 4.15
Z 4.4	**Osobné údaje sa nachádzajú v testovacej verzii aplikácie AbcSecure** Testovacia verzia môže obsahovať zraniteľnosti, ktoré umožnia únik alebo krádež osobných údajov. V prípade zraniteľnosti mechanizmu oprávnení môže dôjsť k neautorizovanej činnosti.	R 4.3, R 4.9, R 4.15
Z 4.5	**Zálohy osobných údajov nie sú umiestnené mimo budovu podniku** V prípade požiaru alebo inej prírodnej katastrofy môžu byť osobné údaje nenávratne zničené.	R 4.8

5.6 Navrhnuté bezpečnostné opatrenia

Zraniteľnosti odstránime opatreniami, ktoré sme navrhli v tabuľke. V tabuľke č. 18 sú čísla zraniteľností, na ktoré sa opatrenia vzťahujú.

Tab. 18 Navrhnuté bezpečnostné opatrenia

Číslo	Opatrenie	Zraniteľnosti
O 1	**Zmena parametrov servisnej zmluvy hardvéru diskového poľa a aplikačného serveru** Nastavenie parametrov zmluvy tak, aby bolo možné RTO reálne dodržať.	Z 1.1, Z 1.2
O 2	**Príprava a pravidelné udržiavanie obrazu predinštalovaného systému** Opatrenie výrazne skráti čas obnovy aplikačného servera po havárii. Zálohu bude vykonávať a udržovať správca IT.	Z 1.4
O 3	**Zmena konfigurácie sieťovej brány FortiGate** Zákaz prístupu z internetu na služby testovacieho servera, prístup povoliť len z VPN príslušného zákazníka.	Z 2.1
O 4	**Zakúpenie servisnej podpory brány FortiGate** Z dôvodu pravidelnej aktualizácie softvérového vybavenia brány, ktoré môže obsahovať vážne zraniteľnosti a kvôli dodržaniu stanoveného RTO.	Z 3.2, Z 3.3
O 5	**Zakúpenie modulu pre softvérovú bránu FortiGate obrany pred útokom odmietnutia služby** Zníži riziko obmedzenia poskytovaných služieb.	Z 3.5
O 6	**Pravidelné zálohovanie konfigurácie FortiGate** V prípade obnovy po zlyhaní zariadenia nie je potrebné konfigurovať bránu manuálne. Výrazne skráti čas obnovy. Zálohovanie bude vykonávať správca IT při změně konfigurace.	Z 3.4
O 7	**Zakúpenie náhradného sieťového rozbočovača pre prípad poruchy** V prípade poruchy rozbočovača iba vymeníme zariadenie. Skráti čas obnovy.	Z 3.2
O 8	**Zavedenie autentizačného mechanizmu siete** Prideľovanie pevných IP adries na základe MAC adries zariadení, prípadne implementácia 802.1X.	Z 2.1
O 9	**Úprava dokumentácie** Doplnenie smerníc o pravidlá používania testovacích dát, bezpečnej likvidácie údajov na odovzdávaných médiách a zariadeniach, povinnosť vypracovávať analýzu rizík. Dopracovanie dokumentácie týkajúcej sa ochrany osobných údajov navrhujeme spracovať externou firmou.	Z 2.2, Z 4.2, Z 4.3, Z 4.4
O 10	**Prijatie nového zamestnanca** Náplňou práce bude testovanie aktualizácií aplikácie	Z 2.3

	AbcSecure. Zamestnanca je možné prijať i na znížený úväzok.	
O 11	**Pravidelné vzdelávanie zamestnancov** Školenie by mala zabezpečovať zodpovedná osoba – expert na legislatívu po legislatívnej stránke a správca IT po technickej stránke. Oveľa viac ešte pomôže účasť zamestnancov na externých konferenciách a školeniach týkajúcich sa informačnej bezpečnosti. Zvýši sa tak celkovo povedomie o informačnej bezpečnosti.	Z 2.2, Z 3.1, Z 4.1, Z 4.2, Z 4.3, Z 4.4
O 12	**Udržiavanie záloh v inej lokalite** Ideálnym a najlacnejším riešením je prenájom bankovej schránky, do ktorej bude správca IT pravidelne umiestňovať zálohy.	Z 1.4, Z 2.4, Z 4.5

5.7 Analýza dopadu na podnikanie

V prvom rade musíme rozlišovať dva pojmy, strata alebo zničenie aktíva a prerušenie činnosti aktíva. Pri prerušení činnosti aktíva do finančnej straty vstupuje ušlý zisk a sankcie zo strany zákazníka. V prípade straty aktíva však musíme počítať i s trestnoprávnymi prostriedkami a sankciami zo strany kontrolných inštitúcií.

5.7.1 Ohrozenie prevádzky aplikácie AbcSecure

Hlavným zdrojom príjmov podniku je prevádzka systému AbcSecure. Kritické aktíva „Diskové pole a aplikačný server“ a „Sieťová infraštruktúra“ priamo súvisia s funkčnosťou tretieho aktíva „Aplikácia AbcSecure“. Preto môžeme z pohľadu škôd tieto aktíva zúžiť z pohľadu analýzy do jedného aktíva „Aplikácia AbcSecure“. Podľa získaných informácii o zmluvných sankciách zo strany zákazníkov v prípade zostavíme tabuľku časových úsekov trvania výpadku aplikácie:

Tab. 19 Škody v závislosti od trvania výpadku aplikácie AbcSecure

Čas výpadku	**Spôsobená škoda**
12 hodín	550 €
48 hodín	1100 €
72 hodín	1800 €
1 týždeň	3850 €
2 týždne	7700 €
viac ako 2 týždne	viac ako 7700 €, odstúpenie od zmluvy

Náklady na obnovu pri súčasnej úrovne bezpečnosti sme počítali na dobu 1 mesiaca, pri odhade nákladov na obnovu sme postupovali podľa informácií z podniku poskytnutých správcom IT. V súčasnej situácií je podnik schopný obno-

viť funkčnosť systému do 72 hodín. Mesačná servisná podpora diskového poľa a aplikačného servera podnik stojí 100 €. Počiatočné náklady znamenajú nakúpenie novej techniky, optického pripojenia v prípade kratšieho času obnovy. Pre súčasnú situáciu v podniku počiatočné náklady neuvažujeme. Náklady na ľudské zdroje firmy sme ohodnotili sadzbou 30 €/h.

Tab. 20 Náklady na zabezpečenie obnovy z výpadku v závislosti od času trvania obnovy

Čas obnovy	**Náklady**	
	Počiatočné	**Na 1 mesiac**
12 hodín	12000 €	3000 €
48 hodín	470 €	625 €
72 hodín	0 €	100 €
1 týždeň	0 €	50 €
2 týždne	0 €	0 €
viac ako 2 týždne	0 €	0 €

V tabuľke je vidieť, že náklady na čas obnovy 12 hodín sú pre podnik v astronomickej výške. V nákladoch je vybudovanie zdvojeného sieťového pripojenia, zabezpečenie servisnej podpory hardvéru, plat ďalšieho správcu IT. Pre podnik by bolo toto opatrenie zbytočné a neúnosné. Zaujímavý je pohľad na čas obnovy do 48 hodín. Pre zabezpečenie schopnosti dodržať tento čas, by stačilo zaviesť už navrhnuté tieto opatrenia s finančnými nákladmi v tabuľke:

Tab. 21 Bezpečnostné opatrenia a náklady na implementáciu pri čase obnovy do 48 hodín

Opatrenie	**Počiatočné náklady**	**Náklady na 1 mesiac**
O 1	0 €	300 €
O 2	120 €	30 €
O 4	0 €	250 €
O 5	0 €	15 €
O 6	0 €	30 €
O 7	350 €	0 €

Ak tabuľky porovnáme, zistíme, že náklady na zabezpečenie obnovenia kontinuity činností do 48 hodín sú v porovnaní so spôsobenou škodou oveľa nižšie. Odporúčame firme zabezpečiť implementovať všetky navrhnuté riešenia. Citeľne zníži finančné straty v prípade výpadkov aplikácie AbcSecure.

5.7.2 Strata, únik alebo krádež osobných a iných citlivých údajov

Podnik doposiaľ nezaznamenal krádež, stratu alebo únik osobných a citlivých údajov. Taktiež nemožno presne vyčísliť pokuty, ktoré môžu byť kontrolnými orgánmi uložené podniku. V tabuľke č. 22 zosumarizujeme rozsah možných sankcií a škôd, ktoré podniku hrozia:

Tab. 22 Škody v prípade zničenia, úniku, krádeže alebo neoprávneného poskytnutia informácií

Udalosť	Hodnota škody	Popis
Pokuty udelené Úradom na ochranu osobných údajov SR	0 až 200 000 €	Pokuty od 100 000 € alebo zákaz činnosti sú pre podnik likvidačné.
Náhrada škody určená rozsudkom v prípade žaloby zákazníka a rozsudku v neprospech podniku	neobmedzené	Náhrada škody od 100 000 € alebo zákaz činnosti sú pre podnik likvidačné.
Strata dobrého mena	strata dobrého mena je nevyčísliteľná	Negatívne ovplyvňuje zotrvanie súčasných a získavanie nových zákazníkov.
Strata zákazníkov	strata zákazníkov ovplyvňuje negatívne príjmy podniku	Strata viac ako polovice zákazníkov je pre podnik likvidačná.

Pre zníženie rizika sme navrhli nasledujúce opatrenia, ku ktorým sme odhadli finančné náklady:

Tab. 23 Náklady na opatrenia týkajúce sa bezpečnosti informácií

Opatrenie	Počiatočné náklady	Náklady na 1 mesiac
O 3	30 €	0 €
O 4	0 €	250 €
O 8	240 € až 3000 €	0 €
O 9	1000 €	0 €
O 10	0 €	1500 €
O 11	0 €	270 €
O 12	0 €	3,5 €

Porovnaním hodnôt zisťujeme, že akákoľvek strata, únik alebo krádež údajov môže podnik existenčne ohroziť. Odporúčame všetky opatrenia podrobne navrhnúť v pláne implementácie, následne implementovať a pravidelne preverovať ich účinnosť.

6 Záver

Veľké množstvo manažérov v podnikoch informačnú bezpečnosti neprikladá dostatočný význam. Plány na jej posilnenie odsúvajú do budúcnosti a okrem iného majú obavy i z vysokých finančných nákladov. Často sú im ponúkané drahé a veľakrát zbytočne komplikované softvérové nástroje, ktoré sľubujú zaistenie vysokej úrovne informačnej bezpečnosti. V skutočnosti však neexistuje taký všeliek, takéto systémy nie sú vôbec potrebné a veľakrát ani bez zavedenia iných bezpečnostných opatrení a procesov nemajú zmysel. Zaistenie vyššej úrovne informačnej bezpečnosti v podniku nemusí byť nutne drahé.

V práci sme zistili, že počítačová sieť vybraného podniku obsahuje zraniteľnosti, ktoré môžu priamo ohroziť bezpečnosť spracúvaných údajov ako i činnosť firmy. Odhad finančných nákladov na bezpečnostné opatrenia ukázal, že strach manažmentu z vysokých finančných nákladov na informačnú bezpečnosť nie je oprávnený. Spôsobené škody, ktoré podniku hrozia, môžu mnohonásobne prevýšiť náklady na bezpečnostné opatrenia. Už len malou zmenou konfigurácie sieťových prvkov správcom IT alebo rozšírením vnútorných smerníc je možné zabrániť veľkým škodám.

V prvom rade je však potrebné k implementácii opatrení pristupovať systematicky a podľa vopred navrhnutých plánov. Opatrenia budú plniť svoju úlohu len vtedy, ak budeme pravidelne kontrolovať a prehodnocovať ich účinnosť. Podnik by tiež nemal zabúdať na pravidelné testovanie zraniteľností, pravidelnú analýzu rizík a dopadov, pravidelné školenia zamestnancov a vzdelávanie zodpovedných osôb. Zavedenie systému riadenia informačnej bezpečnosti v podniku je základným krokom k úspešnému podnikaniu.

7 Literatúra

ISO/IEC 27001:2013. 2. vyd. Ženeva: International Standard Organization, 2013.

Informačná bezpečnosť. 1. vyd. Bratislava: Ministerstvo financií Slovenskej republiky, 2013. Dokument vo formáte PDF. [online] [cit. 20.10.2015] Dostupné na http://informatizacia.sk/ext_dok-stud_2014_02_it_ib_ucitelia/16983c.

IT Grundschutz Catalogues. 13. vyd. Bonn: Das Bundesamt für Sicherheit in der Informationstechnik, 2013. Dokument vo formáte PDF. [online] [cit. 28.11.2015] Dostupné na https://gsb.download.bva.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf.

JPMorgan Hack Charges. CNN, 2015. Dokument vo formáte HTML. [online] [cit. 23.11.2015] Dostupné na http://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges.

NÁDENÍČEK, P. *Finance a bezpečnost aneb peníze až na prvním místě*. Dokument vo formáte HTML. [online] [cit. 23.11.2015] Dostupné na http://firmy.finance.cz/zpravy/finance/66819-finance-a-bezpecnost-aneb-penize-az-na-prvnim-miste/.

Nmap: Port Scanning Techniques. Dokument vo formáte HTML. [online] [cit. 20.11.2015] Dostupné na https://nmap.org/book/man-port-scanning-techniques.html.

OLEJÁR, D. *Manažment informačnej bezpečnosti a základy PKI.* 1. vyd. Bratislava: Ministerstvo financií Slovenskej republiky, 2015. Dokument vo formáte PDF. [online] [cit. 9.11.2015] Dostupné na http://informatizacia.sk/ext_dok-ucebnice_nadstavba_2014/19817c.

PRITCHETT, W. – SMET, D. *Kali Linux Cookbook.* Birmingham: Packt Publishing Ltd., 2013. 243 s. ISBN 978-1-78328-959-2.

Russian Hackers Attacked Pentagon. Telegraph, 2015. Dokument vo formáte HTML. [online] [cit. 23.11.2015] Dostupné na http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11788904/Russian-hackers-attacked-Pentagon.html.