FIIT, STU Ilkovičova 2, 842 16 Bratislava

# MBVIT - projekt 2

## Plánovanie kontinuity činností

## Havarijný plán

Ondrej Ambruš, Michal Minár

Študijný program: Informatika Ročník: 2.

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

# 1 Použité skratky

DDoS - Distribuované zabránenie prístupov do systémov spoločnosti (**D**istributed **D**enial **o**f **S**ervice)
BCP - Plán kontinuity činností (**B**usiness **C**ontinuity **P**lan)
DRP - Havarijný plán (**D**isaster **R**ecovery **P**lan)
OI - Obchodná inšpekcia
NBS - Národná banka Slovenska
VPN - Virtuálna privátna sieť (**V**irtual **P**rivate **N**etwork)
Hodn. - Hodnota
MTO - Maximálna doba výpadku (**M**aximum **T**olerable **O**utage)
RTO - Cieľový čas obnovy (**R**ecovery **T**ime **O**bjective)
RPO - Cieľový bod obnovenia (**R**ecovery **P**oint **O**bjective)
HDD - Pevný disk (**H**ard **D**isk **D**rive)
UPS - Zdroj neprerušovaného napájania (**U**ninterruptible **P**ower **S**upply)
AED - Automatický externý defibrilátor
N/A - neaplikovateľné (**N**ot **A**pplicable)

# 2 Slovník pojmov

SIEM - monitorovací a auditný nástroj, ktorý poskytuje centralizovaný pohľad na všetky relevantné bezpečnostné informácie z IT infraštruktúry v reálnom čase a vyhodnocuje rizikové bezpečnostné udalosti
Cloudové služby - sú na internete založený model vývoja a používania počítačových technológií

# 3 Úvod

Hlavným cieľom plánovania kontinuity činnosti (BCP) a havarijného plánu (DRP) je postup obnovy kritickej infraštruktúry v prípade havárie alebo katastrofy spolu s ich možnými následkami a dôsledkami. V dokumente sú zosumarizované kroky, ktoré je potrebné vykonať v prípade narušenia bežného chodu spoločnosti internými alebo externými vplyvmi. V prípade kritickej situácie je nevyhnutné riadiť sa týmto dokumentom, ktorý zaručuje bezpečný chod spoločnosti ako aj jej najdôležitejších systémov.
Jedným z hlavných účelov dokumentu je zaručiť nepretržitý chod systémov, bezpečnosť, integritu, dostupnosť dát, spolu s plynulým chodom celej spoločnosti.

# 4 Ohodnotenie situácie

Organizácia je aktuálne z pohľadu bezpečnosti ovplyvniteľná (aj ovplyvnená) množstvom faktorov, nielen z dôvodu šírenia ochorenia pri styku osôb ale aj pre množstvo zraniteľností a hrozieb, na ktoré je organizácia náchylná (viď 4.1 Analýza rizík). Analýza dopadov s ich možnými následkami je uvedený v sekcii 4.2 Analýza dopadov. Uvedené zraniteľnosti a dopady by mali všeobecne pokryť zabezpečenie organizácie s cieľom o jej nepretržitý chod a pokusy predísť veľkým finančným stratám (pokiaľ to je možné).

## 4.1 Analýza rizík

Analýza rizík je vypracovaná ako samostatný dokument (1).

## 4.2 Analýza dopadov

Spoločnosť má aktuálne obmedzené možnosti týkajúce sa zákazníckych služieb, najmä kvôli pandémii a vyhláškam štátu (ako už bolo spomenuté), ktoré prikazujú mať zavreté pobočky. Spomínané pobočky môžu byť kvôli tomu vo väčšom riziku spolu s peniazmi uloženými v trezoroch priamo na pobočke. Na druhej strane je vyšší dopyt po telefonických službách, čo má za následok väčšie nároky na serveri a zamestnancov pracujúcich pre zákaznícku podporu, a internet bankingu, čo má tiež za následok vyššiu vyťaženosť serverov. Centrála banky pracuje v normálnom režime kritickej infraštruktúry nachádzajúcej sa priamo v budovách banky a ostatní pracovníci sú pripojený pomocou VPN (vzdialeného prístupu) z domu. Zariadenia na pobočkách spolu s trezormi zostali zabezpečené tak aby nedošlo k zbytočným stratám na ich hodnote počas ich doby nevyužívania. Centrálny sklad banky sa naplnil väčším množstvom náhradných dielov do server, pre prípad nedostatku jednotlivých komponentov z dôvodu pandémie, takže je v skladoch banky umiestnených viacej aktív ako je odporúčané.
V tabuľke číslo 1 sú kategorizované možné dopady v prípade narušenia kritickej infraštruktúry spoločnosti. Uvedené kategórie sú číslované od 0 (nulový vplyv / dopad na spoločnosť) až po 5 (likvidačný vplyv na spoločnosť). Spolu s prevádzkovými dopadmi, sú uvedené aj možné legislatívne opatrenia, odhadovaný finančný dopad a reputačný dopad.
V tabuľke číslo 2 reprezentuje rozsah vplyvu pri výskyte ohrozenia kritickej zraniteľnosti a kategorizuje ich do jednotlivých zodpovedajúcich úrovní od *nízkeho* po *vysoký* vplyv. Uvedená tabuľka je využitá v tabuľke v sekcii 5.2 Návrh stratégie obnovy.

| Hodn. | Popis dopadu | Prevádzkový dopad | Legislatívny dopad | Finančný dopad (€) | Reputačný dopad |
|---|---|---|---|---|---|
| **0** | **Nulový vplyv** | - | - | - | - |
| **1** | **Nezanedbateľný vplyv** | Krátkodobé zníženie výkonu oddelenia | Disciplinárne konanie | 0 - 10 000 | Nespokojnosť na úrovni oddelenia |
| **2** | **Minimálny vplyv** | Krátkodobé zníženie výkonu spoločnosti | Kontrola z OI | 10 000 - 100 000 | Nespokojnosť viacerých oddelení |
| **3** | **Nemalý vplyv** | Odstavenie možností zakladania účtov a investovania | Kontrola z OI | 100 000 - 1 000 000 | Nespokojnosť zákazníkov |
| **4** | **Viditeľný vplyv** | Odstavenie možností čerpania úverov a pôžičiek | Kontrola z OI | 1 000 000 - 10 000 000 | Nespokojnosť zákazníkov a zamestnancov |
| **5** | **Významný vplyv** | Rušenie pobočiek spoločnosti s možnosťou prepúšťania zamestnancov | Kontrola z NBS | 10 000 000 - 20 000 000 | Negatívna národná reputácia |
| **6** | **Likvidačný vplyv** | Zrušenie zákazníckych účtov, neposkytovanie úverov, veľké prepúšťanie zamestnancov | Správne konanie na úrovni Európskeho súdneho dvoru | > 20 000 000 | Negatívna medzinárodná reputácia |

*Tabuľka 1: Kategorizácia dopadov podľa finančného a legislatívneho dopadu*

| **Tabuľka dopadov** | **Časové rozsahy** | | | | | | |
|---|---|---|---|---|---|---|---|
| | < 10 minút | < 30 minút | < 1 hodiny | < 12 hodín | < 1 deň | < 7 dní | > 7 dní |
| **Rozsah vplyvu** | Nízky | Nízky | Stredný | Stredný | Vysoký | Vysoký | Vysoký |

*Tabuľka 2: Rozdelenie časových rozsahov v závislosti od rozsahu vplyvu*

# 5 Plánovanie

V sekciách nižšie je plánovanie z aktuálneho pohľadu a kapacity zdrojov (sekcia 5.1) a definovaní strategických cieľov obnovy a postupu pri samotnej katastrofe alebo zlyhaní niektorej z kritických bodov infraštruktúry.

## 5.1 Rozdielová analýza

Aktuálne zdroje spoločnosti sú veľmi obmedzené v prípade výpadku jedného zo zdrojov kritickej infraštruktúry. Analýza nižšie podrobne rozpisuje súčasnú možnú obnovu biznis procesov a požiadaviek v prípade katastrofy.

1. V prípade výpadku dvoch ľubovoľných serverov, je možné obnoviť len jeden z nich nakoľko má organizácia v zálohe len jeden záložný server. Pokiaľ by však vypadol aplikačný a databázový server, nebolo by možné vykonávať transakcie, lebo iba jeden zo serverov - či už aplikačný potrebný na beh softvéru alebo databázový na ukladanie dát - by sa nedal adekvátne rýchlo obnoviť.
2. Medzi ďalšie biznis požiadavky organizácie patrí neustále pripojenie na internet, nakoľko spoločnosť spracováva množstvo bankových transakcii. Voči tejto požiadavke nie sú vedené žiadne protiopatrenia a je zazmluvnený len jeden prevádzkovateľ pripojenia na internet, ktorý v prípade výpadku nebude schopný dostatočne pokryť potreby organizácie.
3. Nakoľko organizácia nepretržite spracováva bankové transakcie, je jednou z požiadaviek 24 hodinová prevádzka kritických systémov. Tieto systémy sú závislé na elektrickej energií, avšak organizácia nemá dostatočne zabezpečený záložný zdroj, ktorý by v prípade výpadku napájania udržal tieto systémy v prevádzke.
4. V spoločnosti sú vedené dôverné informácie z pohľadu napríklad plánov do najbližšej budúcnosti, ale aj dlhodobých. Na druhej strane je implementovaná veľmi slabá bezpečnostná konfigurácia databázových a úložiskových serverov, čo môže mať za následok odcudzenie týchto informácii.
5. Mnohí zamestnanci firmy majú prístup k dôverným dátam klientov. Jednou z požiadaviek je udržanie týchto dát v bezpečí. Problém môže nastať v prípade, že sa nespokojný zamestnanec rozhodne tieto informácie zverejniť poprípade zneužiť.
6. Aktuálna poloha spoločnosti je veľmi náchylná na povodne, ktoré sú v nesúlade s viacerými biznis požiadavkami (neustála prevádzka, dostupnosť cenných dát a ich nenahraditeľnosť). Avšak, dané požiadavky sú v nesúlade s protipovodňovou ochranou priestorov organizácie, zálohovaním cenných dát a ich následnou dostupnosťou pre potreby zamestnancov.

## 5.2 Návrh stratégie obnovy

V tabuľke nižšie sú uvedené strategické ciele obnovy pre prípad výpadku jedného z kritických zdrojov infraštruktúry, spolu s kategóriou dopadu a ideálnym časom obnovy.

| ID | Kategória | Popis prerušenia | Cieľ obnovy | Kat. dopadu | Ideálny čas obnovy |
|---|---|---|---|---|---|
| 6.1.1 | Technológie | Výpadok serveru | Obnoviť pôvodnú funkcionalitu serveru | 4 | Stredný (< 1 hod.) |
| 6.1.2 | | Výpadok internetového pripojenia | Zabezpečiť internetové pripojenie od zmluvného partnera | 5 | Vysoký (< 1 deň) |
| 6.1.3 | | Výpadok dodávky elektriny | Pri krátkodobom výpadku využiť záložné zdroje energie a generátory elektriny | 4 | Vysoký (< 1 deň) |
| 6.1.4 | | Únik informácii | Zabezpečiť obnovu dát a stratených informácii, pokiaľ to je možné | 6 | Stredný (< 12 hod.) |
| 6.1.5 | | Kompromitácia zariadení | Nahradiť zariadenia | 3 | Nízky (< 30 min.) |
| 6.1.6 | | Počítačový útok | Dočasné presunutie infraštruktúry do cloudu | 3 | Stredný (< 1 hod.) |
| 6.1.7 | | Elektrický skrat | Zabezpečiť náhradu poškodeného zariadenia | 0 | Nízky (< 30 min.) |
| 6.1.8 | Ľudské zdroje | Úmrtie pracovníka | Nahradiť pracovníka | 2 | Vysoký (> 7 dní) |
| 6.1.9 | | Zranenie zamestnanca | Ošetrenie zamestnanca a dočasné prerozdelenie povinností v rámci oddelenia | 1 | Stredný (< 1 hod.) |
| 6.1.10 | | Nespokojný zamestnanec | Disciplinárne konanie | 5 | Stredný (< 1 hod.) |
| 6.1.11 | Priestory | Vytopenie priestorov | Dočasne presťahovať a počas toho vrátiť priestory do pôvodného stavu | 3 | Vysoký (> 7 dní) |
| 6.1.12 | | Požiar | Presunutie celej organizácie do nových priestorov v závislosti od závažnosti požiaru | 2 | Vysoký (> 7 dní) |
| 6.1.13 | | Údržba priestorov | Bezpečné a udržiavané priestory organizácie | 0 | Stredný (< 12 hod.) |

# 6 Implementácia

V sekcii nižšie sú rozobrané akčné plány pre prípad ohrozenia kritickej infraštruktúry banky Plán kontinuity činnosti (BCP) a Havarijný plán (DRP). V prípade ohrozenia spoločnosti alebo organizácie, jej častí alebo jednotlivých zamestnancov odporúčame riadiť sa uvedenými pokynmi pokiaľ sú v týchto plánoch obsiahnuté.

## 6.1 Plánovanie kontinuity činnosti a havarijný plán

Plán kontinuity činností je proces podporovaný vedením organizácie, ktorý identifikuje potenciálne dopady a ktorého cieľom je vytvoriť také postupy a prostredie, ktoré umožní kontinuitu a obnovu kritických procesov činností organizácie na vopred stanovenú úroveň v prípade ich narušenia alebo straty (2). Havarijný plán je plán postupov obnovy zdrojov na pôvodnú funkčnosť z času pred ich narušením.
V sekciách nižšie sú rozobrané procesy a scenáre spolu s ich základnými zložkami potrebnými na nápravu a vrátenie kritickej infraštruktúry do pôvodného stavu pokiaľ to je možné, v opačnom prípade sú uvedené kroky na minimalizáciu škôd.

### 6.1.1 Technické zlyhanie úložiskových médií

Úložiskové média (HDD, SSD, USB kľúče) sú staršie ako 3 roky a tým pádom je vyššie riziko ich zlyhania. Samotné zneprístupnenie dokumentov uložených na serveroch znemožňuje zaznamenávanie transakcií, spracovanie zmlúv a ďalší chod spoločnosti.

**Obmedzenia a predpoklady**

V prípade výpadku je potrebné mať skladové zásoby náhradných HDD a kvalifikovaný personál, ktorý dokáže chybný HDD identifikovať a vymeniť.

**Prípravné úlohy**

1. Zabezpečenie náhradného média systémovým administrátorom.
2. Inštalácia náhradného média namiesto poškodeného / zlyhaného média.

**Identifikácia problému**

Nastavenia operačného systému umožňujú odosielanie automatických notifikácii s presnou lokalitou a príčinou výpadku.

**Fáza reakcie**

1. Informovanie spoločnosti o dočasnom výpadku serveru a aplikácii, kde prišlo k zlyhaniu.
2. Zistenie presného média, ktoré zlyhalo.

**Obnovovacie postupy**

1. Dokúpenie náhradného média do skladu.
2. Opätovné upovedomenie spoločnosti o dostupnosti serveru a jednotlivých aplikácii.

| MTO | RTO | RPO |
|---|---|---|
| > 7 dní | < 1 hod. | 30 min |

### 6.1.2 Výpadok internetového pripojenia

Prístupnosť služieb organizácie je plne závislý na internetovom pripojení. Organizácia nemá žiadne záložné pripojenia v prípade výpadku hlavnej linky. K takémuto výpadku môže dôjsť

aj neohlásene, napr. v dôsledku fyzického poškodenia pripojenia vedúceho do budovy. Preto navrhujeme, aby si organizácia zabezpečila záložnú linku, najlepšie od iného dodávateľa.

**Obmedzenia a predpoklady**

Predpokladom rýchlej obnovy je záložné pripojenie na internet, vedené na inej fyzickej linke a od iného dodávateľa aby sa predišlo ich súbežnému výpadku.

**Prípravné úlohy**

1. Overenie funkčnosti záložnej linky.
2. Pripojenie záložnej linky na hlavnú sieť organizácie.

**Identifikácia problému**

V prípade výpadku vyšle router upozornenie IT oddeleniu. Dodávateľ môže informovať organizáciu v prípade plánovanej odstávky pripojenia.

**Fáza reakcie**

1. Router automaticky presmeruje spojenie na záložnú linku.
2. V prípade výpadku záložnej linky prejsť na alternatívny proces.
3. Sieťový administrátor zavolá dodávateľovi a zistí dôvod výpadku, poprípade čas nápravy.

**Alternatívny proces**

1. Sieťoví administrátori zisťujú dôvod výpadku u oboch dodávateľov zároveň.
2. Organizácia informuje svojich klientov a zamestnancov o výpadku a o pravdepodobnom trvaním nápravy.

**Obnovovacie postupy**

1. Počkať na obnovenie spojenia dodávateľom.
2. V prípade dlhodobého výpadku nájsť nové záložné pripojenie zabezpečí Sieťový administrátor na základe kontaktovania slovenským poskytovateľov pripojenia na internet.

**Kontrolné úlohy**

1. Overenie rýchlosti a stability pripojenia.

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 12 hod. | < 18 hod. | < 10 min. |

### 6.1.3 Výpadok elektrickej siete

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 v podobe dieselového generátoru. Tieto generátory musia byť schopné utiahnuť dostupné serveri, pracovné stanice (max. na hodinu, aby mohli zamestnanci dokončiť svoju činnosť, po ktorej budú z práce musieť odísť) a sieťové komponenty. Tento musí mať postačujúcu kapacitu aby pokryl spotrebu všetkých kritických systémov potrebných na kontinuitu činnosti počas výpadku.

**Obmedzenia a predpoklady**

Organizácia by mala mať pripravené záložné zdroje pre všetky kritické systémy ktoré vyžadujú nepretržitú prevádzku. Taktiež by bolo vhodné aby firma mala aj dlhodobý záložný zdroj ako generátor v prípade, že nedôjde k rýchlej obnove.

**Prípravné úlohy**

1. Nabiť batérie v UPS.
2. Overovať funkčnosť generátoru v pravidelných intervaloch.

**Identifikácia problému**

UPS pri výpadku energie spustí alarm. Taktiež dôjde k výpadku osvetlenia a nekritických zariadení v budove.

**Fáza reakcie**

1. Spustenie generátoru pred vyčerpaním batérií v UPS.
2. V prípade zlyhania generátoru vykonať alternatívny proces.
3. Overenie príčiny výpadku s dodávateľmi elektrickej energie.
4. Dopĺňanie paliva do generátoru podľa potreby.

**Alternatívny proces**

1. Bezpečné ukončenie prevádzky pred vyčerpaním batérií v UPS.
2. Informovanie zamestnancov a klientov o nečakanom výpadku služieb.

**Obnovovacie postupy**

1. Počkať na obnovu dodávky elektrickej energie dodávateľov.

**Kontrolné úlohy**

1. Overenie integrity kritických systémov v prípade ich úplného výpadku.
2. Kontrola technického stavu UPS a diesel generátorov.

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 12 hod. | < 18 hod. | N/A |

### 6.1.4 Únik dôverných informácii z dôvodu nesprávnej konfigurácie databázových serverov

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.

**Obmedzenia a predpoklady**

Databázoví administrátori by mali nastaviť politiku prístupu tak, aby každý zamestnanec mal iba nevyhnutný prístup na výkon jeho zamestnania. Taktiež by organizácia mala venovať prostriedky na školenie zamestnancov ohľadom bezpečnosti a ochrany citlivých údajov.

**Prípravné úlohy**

1. Zabezpečiť konfiguráciu databázových serverov.
2. Zlepšiť politiku prístupu k citlivým údajom.
3. Školiť zamestnancov ako bezpečne pristupovať k citlivým údajom.

**Identifikácia problému**

Databázový administrátor identifikuje neoprávnený prístup k citlivým údajom.

**Fáza reakcie**

1. Zablokovanie neoprávneného pripojenia k databázovému serveru.
2. Identifikácia rozsahu narušenia.
3. V prípade rozsiahleho narušenia prejsť na alternatívny proces.
4. Vyvodenie zodpovednosti.

**Alternatívny proces**

1. Odpojenie databázového serveru od siete.
2. Identifikácia a zablokovanie všetkých neoprávnených spojení.
3. Identifikácia rozsahu narušenia.

**Obnovovacie postupy**

1. Informovanie zákazníkov o prípadnom úniku citlivých údajov.

**Kontrolné úlohy**

1. Neustála kontrola prístupu do databázového serveru pomocou SIEM.
2. Pravidelná kontrola dodržiavania politiky hesiel a prístupu k citlivým údajom.

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 1 deň | < 2 dni | < 12 hod. |

### 6.1.5 Kompromitácia zariadení na základe slabej firemnej politiky hesiel

Na základe skúseností je pri nedostatočnej politike hesiel veľká pravdepodobnosť kompromitácie celej firemnej infraštruktúry, čo 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.

**Obmedzenia a predpoklady**

Databázoví administrátori by mali zmeniť konfiguráciu serveru aby prístupové heslá spĺňali najnovšie bezpečnostné štandardy.

**Prípravné úlohy**

1. Sprísniť požiadavky na prístupové heslá.
2. Pravidelné zmeny hesiel všetkých zamestnancov.

**Identifikácia problému**

Databázový administrátor môže identifikovať neštandardný prístup poprípade podozrivú aktivitu na serveri. Môže tiež dôjsť k úniku viacerých hesiel. V tomto prípade sa použije alternatívny proces.

**Fáza reakcie**

1. Zablokovanie podozrivého prístupu.
2. Resetovanie hesla daného účtu.
3. Informovanie daného zamestnanca.

**Alternatívny proces**

1. Resetovanie hesiel celej spoločnosti.
2. Odhlásenie všetkých účtov zo serveru.
3. Informovanie zamestnancov o danom incidente.

**Obnovovacie postupy**

1. Sprísnenie politiky hesiel.
2. Lepšie zabezpečenie databázy prístupových údajov.

**Kontrolné úlohy**

1. Kontrola prístupu kompromitovaného účtu pre prípadné opätovné narušenie.
2. Pravidelné kontrolné úlohy súvisiace s uplatňovaním bezpečnostnej politiky hesiel v organizácii.

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 10 min. | < 5 min. | < 1 hod. |

### 6.1.6 Výpadok internet bankingu v dôsledku DDoS útoku

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.

**Obmedzenia a predpoklady**

V prípade cieleného útoku na firemnú sieť formou útoku typu DDoS je potrebné zabezpečiť vhodný personál (**sieťových a systémových administrátorov**), ktorý daný útok pomocou **SIEM** systému dokáže rozpoznať.

**Identifikácia problému**

Hlásenie v systéme SIEM zabezpečí informovanie pracovníkov v prípade náhleho útoku na firemnú sieť.

**Fáza reakcie**

1. Informovanie poskytovateľa prístupu do internetu.
2. Informovanie zákazníkov o dočasnej nedostupnosti služieb na internete.
3. Informovanie vrchného manažmentu, v prípade rozsiahleho útoku všetkých zamestnancov.

**Alternatívny proces**

V prípade dlho trvajúceho alebo rozsiahleho útoku použiť záložné cloudové služby, kde môžu byť jednotlivé aplikácie organizácie presmerované.

**Kontrolné úlohy**

1. Testovanie pripojenia a rýchlosti internetu.
2. Overenie funkčnosti klientskych aplikácií.
3. Informovanie osôb zmienených vo fázy reakcie o opätovnej dostupnosti všetkých služieb.

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 1 deň | < 10 minút | < 10 minút |

### 6.1.7 Elektrické skraty starých elektrických zariadení

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 zlyhanie ako nové zariadenia. Navrhujeme preto aby sa do organizácie nakúpili nové zariadenia spolu s ich pravidelnou výmenou.

**Obmedzenia a predpoklady**

Organizácia by mala všetok hardvér pravidelne meniť na zabezpečenie bezchybnej funkčnosti. Pokiaľ nie je možné hardvér vymeniť, je potrebné zabezpečiť jeho pravidelnú inšpekciu a potrebnú údržbu.

**Prípravné úlohy**

1. Výmena zastaralého hardvéru.
2. Pravidelná kontrola elektrických zariadení na základe BOZP.

**Identifikácia problému**

V prípade zlyhania hardvéru je potreba takúto udalosť ihneď nahlásiť systémovému administrátorovi. Takéto hlásenie treba podať aj v prípade identifikácie nedostatkov pri kontrole elektrických zariadení.

**Fáza reakcie**

1. Systémový administrátor odstráni poruchu na zariadení.
2. Pokiaľ je zariadenie príliš staré, alebo sa nedá opraviť, prechádza sa na alternatívny proces.

**Alternatívny proces**

1. Administrátor nahradí zariadenie dočasnou alternatívou.
2. Následne objedná nové zariadenie.

**Obnovovacie postupy**

1. Nové alebo opravené zariadenie sa znova začne používať.

**Kontrolné úlohy**

1. Zariadenie sa dočasne kontroluje, či vykonáva všetky funkcie bez chýb alebo ďalších problémov

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 10 min. | < 5 min. | < 1 hod. |

### 6.1.8 Náhla strata zamestnanca

V prípade neželanej alebo tragickej strate zamestnanca nastáva pre organizáciu problém v zmysle nájdenia náhrady a prenechania povinností na inej osobe do trvania zaučenia nového zamestnanca. Spolu so zamestnancom odíde aj jeho know-how a skúsenosti, ktoré do firmy prinášal a bude ich potrebné opätovne získať. Pokiaľ však bol zamestnanec zo sekcie špecialistov, jeho náhrada nebude trvať také obdobie, na rozdiel od nahradenia jedného z vrhného manažmentu organizácie.

**Prípravné úlohy**

Vytvorenie ponuky práce, zálohovanie zamestnancových súborov.

**Identifikácia problému**

1. Nedostavenie sa zamestnanca do práce, prípadné upozornenie na tragickú udalosť či už rodinou alebo políciou.

**Alternatívny proces**

1. Rozdelenie povinností zamestnanca na kolegov, prípadne jeho podriadených

**Obnovovacie postupy**

1. Zozbierať know-how daného zamestnanca.
2. Využiť jeho školiace materiály a súbory, s ktorými pracoval na zaučenie nového kolegu.
3. Školenie nového zamestnanca.

**Kontrolné úlohy**

1. Pravidelne nového zamestnanca kontrolovať.

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 1 mesiac | < 1 mesiac | < 1 týždeň |

### 6.1.9 Zranenie zamestnanca na pracovisku (BOZP)

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.

**Prípravné úlohy**

1. Lekárnička a AED musia byť rozmiestnené po budove.

**Fáza reakcie**

1. Ošetrenie zamestnanca podaním prvej pomoci, lekárničkou a AED v prípade potreby
2. Zavolanie záchrannej služby
3. Informovanie kolegov o dočasnej práceneschopnosti zamestnanca.
4. Evidovať zranenie v knihe pracovných úrazov.

**Obnovovacie postupy**

1. Rozdelenie povinností zamestnanca na jeho kolegov alebo podriadených

**Alternatívny proces**

V prípade veľkého zaťaženia oddelenia najať externú spoločnosť pokým sa zamestnanec nevráti naspäť do práce.

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 7 dní | < 14 dní | < 1 deň |

### 6.1.10 Nespokojný zamestnanec kompromituje alebo zverejní dôverné informácie spoločnosti

Nespokojný alebo mimoriadne nadaný zamestnanec pracujúci s dôvernými informáciami v banke musí byť pod neustálym dohľadom pre prípad kompromitácie, či už jeho zariadenia alebo iných súčastí, úmyselne alebo neúmyselne. Takzvaný “insider” je človek v rámci organizácie, ktorý či už za finančný obnos alebo pre poškodenie spoločnosti vyzradí informácie zhoršujúce jej reputáciu.

**Obmedzenia a predpoklady**

Podmienky vzniku alebo najatia insedera do organizácie sú zriedkavé avšak v prípade odhalenia úniku dát je potrebné myslieť aj na takýto zdroj úniku.

**Prípravné úlohy**

1. Monitorovanie zariadení.
2. Prístupové práva.
3. Zálohovanie všetkých diskov.

**Identifikácia problému**

1. Dôverné informácie sa môžu nachádzať na internetových fórach.
2. Jeden zo zamestnancov si všimne podozrivé emaily.
3. Administrátori budú upovedomený systémom na veľký alebo nepovolený prenos dát z jedného z účtov zamestnancov.

**Fáza reakcie**

1. Odovzdať všetky zariadenia prípadne kópie dát zo zariadení odborníkom (CSIRT), ktorí dokážu incident kvalifikovane vyriešiť.

**Obnovovacie postupy**

1. Upovedomiť vládne a verejné jednotky na kompromitáciu dát.
2. Upovedomiť dotknuté osoby, ktoré zasiahla strata dát.
3. Disciplinárny proces v prípade zistenia páchateľa (resp. súdne konanie).

**Kontrolné úlohy**

1. Pravidelne monitorovať počítače zamestnancov.
2. Kontrolovať internetové fóra, prípadne konkurenciu, či sa jej kroky nezhodujú s budúcimi krokmi organizácie.

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 7 dní | < 3 dni | > 1 mesiac |

### 6.1.11 Nedostupnosť budovy v prípade povodní

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.

**Obmedzenia a predpoklady**

Keďže organizácia sídli v dvoch budovách bezprostredne vedľa seba v blízkosti rieky Dunaj sú povodne jednou z častých ohrození spoločnosti.

**Prípravné úlohy**

1. Overenie funkčnosti VPN serverov.
2. Premiestnenie všetkých aktív do uskladňovacích priestorov.

**Fáza reakcie**

1. Informovanie generálneho riaditeľa, vedúcich oddelení, ktorí pošlú relevantné informácie na svojich zamestnancov.
2. Dočasný presun infraštruktúry (serverov) do cloudu.
3. Nájdenie nových priestorov v prípade väčších povodní.
4. Informovanie zamestnancov o práci z domu pokiaľ sú záplavy.
5. Pozbieranie funkčných aktív z priestorov organizácie.

**Alternatívny proces**

V prípade nefunkčnosti serverov je nutné premiestniť dočasne (alebo natrvalo) celú organizáciu do nových priestorov aj s novým vybavením.

**Obnovovacie postupy**

1. Informovanie zamestnancov o opätovnej práci z priestorov organizácie (či už pôvodných alebo nových).

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 3 dni | < 7 dní | < 7 dní |

### 6.1.12 Požiar v priestoroch organizácie

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.

**Obmedzenia a predpoklady**

Organizácia potrebuje nový systém hlásenia požiaru a taktiež nový protipožiarny systém spĺňajúci najnovšiu certifikáciu.

**Prípravné úlohy**

1. Vymeniť starý systém hlásenia požiaru.
2. Zlepšiť systém automatického potlačenia požiaru.

**Identifikácia problému**

V prípade požiaru sa spustí v budove alarm a vypne sa elektrické napájanie.

**Fáza reakcie**

1. Identifikovať miesto a rozsah požiaru.
2. Použiť ručné protipožiarne zariadenia na potlačenie požiaru.
3. V prípade, že požiar sa napriek tomu rozrastá alebo je príliš rozsiahly treba použiť alternatívny proces.

**Alternatívny proces**

1. Všetci zamestnanci opustia budovu.

**Obnovovacie postupy**

1. Identifikovanie rozsahu škôd.
2. Rekonštrukcia budovy.
3. Nákup nového nábytku a zariadení.
4. Obnovenie priestorov budovy.

**Kontrolné úlohy**

1. Pravidelné statické kontroly na skorú identifikáciu prípadného rozsiahlejšieho poškodenia.

| MTO | RTO | RPO |
|---|---|---|
| < 7 dní | < 14 dní | < 1 mesiac |

### 6.1.13 Neplánovaná údržba priestorov organizácie

Priestory organizácie sú neustále používané zamestnancami a zákazníkmi. Budova je taktiež neustále vystavená prostrediu čo spôsobuje jej opotrebenie. Môže sa stať, že dôjde k nečakanému poškodeniu či už interných priestorov alebo fasády budovy. Takto môže dôjsť k potrebe vykonať neplánovanú údržbu, čím dôjde k zníženiu produktivity daného oddelenia.

**Obmedzenia a predpoklady**

Organizácia by mala byť pripravená neočakávane uvoľniť niektoré priestory pre prípadnú údržbu. Taktiež by mala mať dostatočné financie na rekonštrukciu budovy v prípade jej poškodenia.

**Prípravné úlohy**

1. Organizácia by mala založiť fond opráv do ktorého bude ukladať peniaze na údržbu.
2. Taktiež by mala vykonávať pravidelné kontroly priestorov pre prípadné nedostatky čím sa môže predísť rozsiahlejšiemu poškodeniu.

**Identifikácia problému**

Zamestanec firmy nahlási poškodenie priestorov alebo fasády.

**Fáza reakcie**

1. Organizácia určí minimálny rozsah potrebných opráv aby znížila dopad na produktivitu daného oddelenia.
2. Následne uvoľní potrebný priestor pre vykonanie údržby.
3. Po uvoľnení môže najať firmu, ktorá dané priestory zrekonštruuje.

**Alternatívny proces**

1. V prípade, že sa nejedná o rozsiahly problém, môže dôjsť k náprave aj bez vysťahovania daných priestorov.

**Obnovovacie postupy**

1. Najatá firma zrekonštruuje poškodenú časť budovy organizácie.
2. Organizácia vráti priestor do pôvodného stavu.

**Kontrolné úlohy**

1. Organizácia zabezpečí kontrolu daného priestoru pre prípadnú vadu v rekonštrukcií a jej promptnú reklamáciu.

| **MTO** | **RTO** | **RPO** |
|---|---|---|
| < 1 deň | < 12 hod. | < 6 hod. |

## 6.2 Kontaktné údaje

| ID | Meno | Pozícia | Kontakt |
|---|---|---|---|
| **1** | Jozef Adminovovič | Systémový administrátor | +221 000 001 |
| **2** | Adam Sietovič | Sieťový administrátor | +221 000 002 |
| **3** | Peter Generalovič | Generálny riaditeľ | +221 000 003 |
| **4** | Jana Ľudská | Vedúca oddelenia ľudských zdrojov | +221 000 004 |
| **5** | Alžbeta Držgrošská | Vedúca oddelenia účtovníctva | +221 000 005 |
| **6** | Polícia | | 158 |
| **7** | Záchranná zdravotná služba | | 155 |
| **8** | Hasičský záchranný zbor | | 150 |

# 7 Monitorovanie

Monitorovanie je proces testovania a vyhodnocovania funkčnosti, efektívnosti a realizovateľnosti havarijnych plánov a plánov kontinuity činnosti. Týmto vyhodnocovaním získava organizácia informácie o ich prípadných nedostatkoch ktoré môže neskôr implementovať. Proces monitorovania sa vykonáva pomocou predpripravených individuálnych testov ktorých proces sa podrobne dokumentuje. Použitím tejto dokumentácie sa dajú nedostatky jednotlivých procesov ľahko identifikovať a následne rýchlo napraviť.

| ID | Typ testu | Popis testu | Zložitosť |
|---|---|---|---|
| **1** | Samovolný test | Podľa potreby a času administrátorov sa skontrolujú konfigurácie kritických scenárov | Nízka |
| **2** | Systémový | Overenie funkčnosti jednotlivých systémov a ich konfigurácie auditovania | Nízka |
| **3** | Simulácia | Simulovanie scenáru z sekcie 6.1 | Stredná |
| **4** | Zátažový | Spustenie záťažových testov na systémoch v čase, keď sú najmenej vyťažené | Stredná |
| **5** | Kritický | Test scenárov kritických pre kontinuitu činností organizácie | Stredná |
| **6** | Úplný | Úplný test všetkých scenárov z sekcie 6.1 | Vysoká |

| ID | Typ testu | Cieľ | Postupnosť krokov | Frekvencia |
|---|---|---|---|---|
| **6.1.1** | 3 | Overenie funkčnosti systému v prípade výpadku úložiskových médií | 1. Vytiahnutie HDD z serveru.<br>2. Pozorovanie správania serveru a jeho reakcia.<br>3. Vrátenie HDD naspäť do serveru. | Polročne |
| **6.1.2** | 1 | Zabezpečenie náhradného pripojenia, prípadne odozvy poskytovateľa pripojenia na internet | 1. Odpojenie pripojenia na internet z hlavného prepínača siete.<br>2. Informovanie poskytovateľa pripojenia o problémoch so sieťov.<br>3. Meranie doby odozvy a navrhovaných postupov pre riešenie problému. | Týždenne |
| **6.1.3** | 2 | Odolnosť UPS systému, kapacity batérii a generátorov v prípade výpadku elektrickej siete | 1. Vypnúť hlavné elektrické poistky priestorov organizácie.<br>2. Po dobu 12 hodín sledovať stav batérii a diesel generátorov. | Mesačne |
| **6.1.4** | 5 | Overenie funkcionality systému na meranie podozrivej a neautorizovanej premávky po sieti a jej následné odhalenie | 1. Generovanie nepovolenej premávky na lokálnej sieti v nezvyčajných časoch pre náhodných zamestnancov.<br>2. Chvíľková odstávka premávky<br>3. Pokračovanie v generovaní nepovolenej premávky po sieti a monitorovanie systémov. | Polročne |
| **6.1.5** | 4 | Prelomenie hesiel zamestnancov s cieľom zistiť najslabšie heslá | 1. Stiahnutie interných súborov obsahujúce heslá zamestnancov<br>2. Spustenie nástroja na prelamovanie hesiel (Napr. John the Ripper)<br>3. Upovedomenie zamestnancov s prelomenými heslami. | Mesačne |
| **6.1.6** | 5 | Napadnutie kritických častí infraštruktúry organizácie s cieľom zistenia doby odozvy administrátorov a jej následné vrátenie do požadovaného stavu | Najať profesionálnu spoločnosť na testovanie bezpečnosti firemnej infraštruktúry z pohľadu IT. | Štvrťročne |
| **6.1.7** | 3 | Testovanie hlásičov elektrického skratu | Simulovať skrat niektorého zo serverov odpojením niektorej z jeho kritickej hardvérovej súčasti a sledovanie reakcie systému. | Ročne |
| **6.1.8** | 1 | Preveriť nahraditeľnosť jednotlivých zamestnancov a dokumentovanosť ich pozícii | 1. Nariadiť náhodnému zamestnancovi voľno vrchným manažmentom bez informovania nadriadeného.<br>2. Sledovať prerozdelenie úloh na iných zamestnancov v daný deň na oddelení. | Ročne |
| **6.1.9** | 2 | Sledovať stav lekárničiek na pracovisku | Preveriť záruky a neporušenosť jednotlivých lekárničiek na pracovisku a ich následnú výmenu v prípade potreby. | Štvrťročne |

| | | | | |
|---|---|---|---|---|
| **6.1.10** | 6 | Preveriť funkčnosť SIEM softvéru | Simulovať kompromitáciu interného zariadenia vnútorným zamestnancom inštalovaním ransomware na uzavretej časti siete a následnej reakcie systému. | Mesačne |
| **6.1.11** | 4 | Pripravenosť zamestnancov na náhlu záplavu alebo povodeň spolu s ich časom odozvy | Zapnúť alarm pre zvýšenú hladinu toku a monitorovať čas príchodu jednotlivých zamestnancov na vopred určené miesta. | Ročne |
| **6.1.12** | 6 | Pripravenosť zamestnancov na náhly výskyt požiaru v budove a pravidelný tréning na uvedené udalosti | Zapnúť alarm pre výskyt požiaru a monitorovať pohyb zamestnancov po chodbách pre zistenie nedostatkov v školeniach BOZP. | Ročne |
| **6.1.13** | 2 | Cieľom je overiť pripravenosť v prípade skutočnej neplánovanej údržby hardvérových komponentov dátových centier organizácie | Raz ročne vykonať plánovanú údržbu hardvérových komponentov jedného dátového centra spoločnosti bez vedomia systémových administrátorov formou dodávateľskej spoločnosti a sledovať ich reakčný čas. | Ročne |

# 8 Záver

V tomto dokumente sú rozobrané dve hlavné zložky zabezpečenia chodu firmy aj napriek ohrozeniu alebo výpadku jednej z častí kritickej infraštruktúry. Plán kontinuity činností a havarijný plán sú rozobrané v hlavnej sekcii dokumentu 6. Kľúčové osoby uvedené v sekcii kontaktov sú nútené držať sa poskytnutých činností a krokov uvedených v tomto dokumente. V prípade odchýlok alebo chýbajúcich postupov kontaktovať nadriadené osoby, ktoré tento problém budú musieť vyriešiť. Samotné scenáre sú uvedené formou krokov potrebných pre minimalizáciu škôd organizácie, prípadne jej reputácie a preto odporúčame uvedený plán pravidelne kontrolovať, aktualizovať. a testovať pre prípad výmeny personálu, pridania nových procesov, a podobne.

# 9 Zdroje


(1) Ondrej Ambruš, Michal Minár (Apríl 2021). MBvIT projekt 1 - Analýza rizík pre spoločnosť B.R.A.
(2) Michal Bubák (Jún 2013). Plánovanie kontinuity činností.
(3) Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci - znenie účinné od 01.04.2021
(4) Zákon č. 18/2018 Z. z. o ochrane osobných údajov - znenie účinné od 01.09.2019
(5) STN ISO/IEC 27001 Informačné technológie Bezpečnostné metódy Systémy riadenia informačnej bezpečnosti Požiadavky (2014).
(6) STN ISO/IEC 27002 Informačné technológie Bezpečnostné metódy Pravidlá dobrej praxe riadenia informačnej bezpečnosti (2014).