# Orientační analýza rizik a kvalitativní analýzy rizik (AR) dle popisu organizace

## Stanovení rozsahu analýzy rizik a metodiky

### 1. Stupnice zranitelnosti:

Zranitelnost bude stanovena na základě technických a organizačních faktorů, které by mohly vést k neoprávněnému přístupu nebo ztrátě dat. Tato stupnice bude zohledňovat jak fyzické, tak digitální aspekty školy, včetně infrastruktury, procesů a lidských zdrojů.

| **Stupnice** | **Popis** |
| --- | --- |
| 1 | Minimální zranitelnost |
| 2 | Nízká zranitelnost |
| 3 | Střední zranitelnost |
| 4 | Vysoká zranitelnost |
| 5 | Extrémní zranitelnost |

### 2. Stupnice hodnoty aktiva:

Hodnota aktiva bude určena na základě významu pro chod školy a citlivosti dat, která jsou na nich uložena.

| **Stupnice** | **Popis** |
| --- | --- |
| 1 | Nepodstatné aktiva |
| 2 | Nižší hodnota aktiva |
| 3 | Střední hodnota aktiva |
| 4 | Vyšší hodnota aktiva |
| 5 | Kritická hodnota aktiva |

### 3. Stupnice míry rizika:

Míra rizika bude kombinací zranitelnosti a hodnoty aktiva a bude určena pro každé identifikované riziko.

| **Stupnice** | **Popis** |
| --- | --- |
| 1 | Minimální míra rizika |
| 2 | Nízká míra rizika |
| 3 | Střední míra rizika |
| 4 | Vysoká míra rizika |
| 5 | Extrémní míra rizika |

Tímto způsobem budeme schopni identifikovat a ohodnotit rizika v souladu s potřebami a specifiky BSPŠ-IT.

V další fázi se zaměříme na identifikaci konkrétních aktiv, hrozeb a pravděpodobnosti jejich uskutečnění, stejně jako na stanovení míry zranitelnosti a rizika pro jednotlivá aktiva a hrozby. Poté přejdeme k části B, kde navrhneme opatření pro minimalizaci identifikovaných rizik v různých oblastech kybernetické bezpečnosti.

## Identifikace a ohodnocení aktiv

Pro identifikaci a ohodnocení aktiv budeme vycházet z uvedeného hardware (HW) a software (SW) a dalších prvků dle činnosti organizace, tj. BSPŠ-IT. Zde jsou identifikované aktiva a jejich ohodnocení:

| **Aktiva** | **Hodnota aktiva** | **Popis** |
| --- | --- | --- |
| Počítače (PC a notebooky) | 4 | Vzhledem k jejich významu pro vzdělávací proces a data |
| Učebny výpočetní techniky | 5 | Klíčová pro výuku a cvičení studentů |
| Webový server | 5 | Centrální bod pro školní informační systém a webové stránky |
| Fyzické a virtuální servery | 5 | Důležité pro provoz školního informačního systému |
| WiFi AP a síťové prvky | 4 | Zajišťují připojení k síti pro učebny a administrativu |
| Router | 5 | Zajišťuje připojení k internetu pro školu |
| Specializovaný software | 5 | Důležitý pro výuku a správu školních systémů |

Každé aktivum bylo ohodnoceno na základě jeho významu a kritičnosti pro chod školy. Další prvky, jako jsou licence na software a další infrastrukturální prvky, by měly být také zohledněny a ohodnoceny podle jejich významu a kritičnosti.

Nyní budeme pokračovat s definicí hrozeb a pravděpodobností jejich uskutečnění v souladu s činností organizace.

## Definice hrozeb:

1. **Malware:**
   * **Popis:** Infekce počítačových systémů školy malware, včetně virů, ransomware a spyware, které mohou ohrozit integritu a dostupnost dat.
   * **Pravděpodobnost:** Vysoká, protože škola disponuje mnoha počítači, které mohou být náchylné k infekci.
2. **Fyzické poškození zařízení:**
   * **Popis:** Možnost fyzického poškození počítačů, serverů nebo síťové infrastruktury v důsledku nehody, vandalismu nebo přírodních katastrof.
   * **Pravděpodobnost:** Střední, zohledňující okrajovou polohu budovy a možná rizika spojená s tímto faktorem.
3. **Únik citlivých dat:**
   * **Popis:** Možnost, že citlivá data o studentech, zaměstnancích nebo školních systémech mohou uniknout následkem nedbalosti, úmyslného úniku nebo kybernetického útoku.
   * **Pravděpodobnost:** Střední až vysoká, protože škola zpracovává citlivé údaje a může být cílem kybernetických útoků.
4. **Neoprávněný přístup:**
   * **Popis:** Možnost, že neoprávněné osoby získají přístup k školní síti, systémům nebo datům, buď fyzicky nebo prostřednictvím kybernetických útoků.
   * **Pravděpodobnost:** Střední, zohledňující úroveň kybernetické bezpečnosti a školení zaměstnanců.

## Pravděpodobnost uskutečnění hrozeb:

* **Malware:** Vysoká
* **Fyzické poškození zařízení:** Střední
* **Únik citlivých dat:** Střední až vysoká
* **Neoprávněný přístup:** Střední

Tyto hrozby a jejich pravděpodobnost byly definovány na základě specifických charakteristik organizace BSPŠ-IT a aktuálních rizik spojených s její činností a infrastrukturou. Nyní se zaměříme na stanovení míry zranitelnosti pro jednotlivá aktiva a pravděpodobnost uskutečnění hrozeb.

## Stanovení míry zranitelnosti:

1. **Počítače (PC a notebooky):**
   * **Pravděpodobnost hrozby (Malware):** Vysoká
   * **Míra zranitelnosti:** Vysoká - Protože počítače jsou často využívány studenty i zaměstnanci a mohou být náchylné k infekci malwarem.
2. **Učebny výpočetní techniky:**
   * **Pravděpodobnost hrozby (Fyzické poškození zařízení):** Střední
   * **Míra zranitelnosti:** Vysoká - Jelikož učebny jsou důležité pro výuku, jejich fyzické poškození by mohlo způsobit významné přerušení vzdělávacího procesu.
3. **Webový server:**
   * **Pravděpodobnost hrozby (Únik citlivých dat):** Střední až vysoká
   * **Míra zranitelnosti:** Vysoká - Jelikož webový server obsahuje citlivé informace o studentech a školních systémech.
4. **Fyzické a virtuální servery:**
   * **Pravděpodobnost hrozby (Malware, Neoprávněný přístup):** Střední až vysoká
   * **Míra zranitelnosti:** Vysoká - Tyto servery jsou kritické pro provoz školního informačního systému a jejich kompromitace by mohla mít závažné následky.
5. **WiFi AP a síťové prvky:**
   * **Pravděpodobnost hrozby (Neoprávněný přístup):** Střední
   * **Míra zranitelnosti:** Střední až vysoká - Jelikož jsou WiFi AP důležitou součástí školní sítě a mohou být cílem kybernetických útoků.
6. **Router:**
   * **Pravděpodobnost hrozby (Neoprávněný přístup):** Střední
   * **Míra zranitelnosti:** Střední až vysoká - Jelikož router zajišťuje připojení k internetu, jeho kompromitace by mohla mít vážné následky pro školu.
7. **Specializovaný software:**
   * **Pravděpodobnost hrozby (Malware, Únik citlivých dat):** Střední až vysoká
   * **Míra zranitelnosti:** Vysoká - Jelikož tento software je důležitý pro správu školních systémů a citlivé informace.

Míra zranitelnosti byla stanovena na základě kombinace pravděpodobnosti uskutečnění hrozeb a důležitosti jednotlivých aktiv pro školní provoz. Tento přístup nám umožní identifikovat nejzranitelnější aktiva, na která je třeba zaměřit se s opatřeními ke zvýšení jejich ochrany.

## Stanovení míry rizik:

Pro určení míry rizik budeme používat kombinaci stupnice pravděpodobnosti a stupnice míry zranitelnosti, které jsme definovali dříve.

Příklad pro aktiva: Počítače (PC a notebooky)

* **Pravděpodobnost hrozby (Malware):** Vysoká
* **Míra zranitelnosti:** Vysoká

Stupně rizik pro počítače (PC a notebooky):

| **Pravděpodobnost hrozby** | **Míra zranitelnosti** | **Míra rizika** |
| --- | --- | --- |
| Vysoká | Vysoká | Vysoká |

Tento postup provedeme pro každé identifikované aktivum a hrozbu. Výsledkem bude určení stupně rizika pro každou kombinaci aktivum-hrozba, což nám pomůže identifikovat nejrizikovější oblasti, na které je třeba se zaměřit s prioritními opatřeními.

Příklad pro aktivum: Učebny výpočetní techniky

* **Pravděpodobnost hrozby (Fyzické poškození zařízení):** Střední
* **Míra zranitelnosti:** Vysoká

Stupně rizik pro učebny výpočetní techniky:

| **Pravděpodobnost hrozby** | **Míra zranitelnosti** | **Míra rizika** |
| --- | --- | --- |
| Střední | Vysoká | Vysoká |

Pokračujeme v tomto postupu pro všechna aktiva a hrozby, abychom mohli získat komplexní přehled o rizikovém profilu BSPŠ-IT. Poté se budeme moci zaměřit na navrhovaná opatření pro minimalizaci identifikovaných rizik.

# B) Opatření pro minimalizaci identifikovaných rizik

1. **Fyzická bezpečnost:**
   * Instalace bezpečnostních kamer a jejich monitorování pro pokrytí klíčových prostor školy, jako jsou vstupy, serverovna a učebny s důležitým vybavením.
   * Vytvoření a pravidelná aktualizace kontrolních seznamů pro přístup do prostor s důležitou IT infrastrukturou.
   * Zavedení pravidelných kontrol bezpečnostního vybavení, jako jsou zámky, alarmy a detektory pohybu, s průběžným vyhodnocováním jejich účinnosti.
   * Pravidelné školení zaměstnanců ohledně fyzické bezpečnosti, včetně správného zacházení s přístupovými kartami, znalosti bezpečnostních postupů v případě krize a povědomí o možných hrozbách.
   * Implementace mechanismů kontroly a monitorování přístupu zaměstnanců a návštěvníků do budovy školy, včetně záznamů o přítomnosti a identifikace osob.
2. **Nástroje pro ochranu integrity komunikačních sítí:**
   * Implementace firewallů na hranicích sítě a na jednotlivých zařízeních pro monitorování a filtrování příchozího a odchozího provozu.
   * Nasazení systému detekce a prevence útoků (IDS/IPS) pro identifikaci a blokování podezřelého provozu.
   * Pravidelná aktualizace softwaru a firmware na síťových zařízeních pro zajištění bezpečnostních záplat a oprav.
   * Zavedení pravidelných auditů a penetrace sítě pro identifikaci slabých míst a neoprávněných přístupů.
   * Vytvoření a pravidelná aktualizace dokumentace síťové infrastruktury a konfigurace zařízení pro transparentnost a možnost rychlé reakce v případě incidentu.
3. **Nástroje pro ověřování identity uživatelů:**
   * Implementace dvoufaktorové autentizace pro přístup k citlivým datům a aplikacím.
   * Nastavení silných hesel s pravidelnou periodou změny a omezení opakování předchozích hesel.
   * Zavedení systému sledování aktivit uživatelů pro detekci podezřelých pokusů o přihlášení.
   * Implementace monitorovacích nástrojů pro detekci anomálních aktivit a neoprávněných pokusů o přihlášení.
   * Zavedení politiky správy identit a přístupů (IAM) pro centrální správu uživatelských účtů, jejich oprávnění a revize přístupových práv.
4. **Nástroje pro ochranu před škodlivým kódem:**
   * Nasazení antivirového softwaru s pravidelnými aktualizacemi a skenováním všech zařízení v síti.
   * Zavedení systému filtrace e-mailů pro detekci a blokování škodlivých příloh a odkazů.
   * Vytvoření politik pro omezení přístupu uživatelů k neznámým webovým stránkám a aplikacím a pro blokování nevyžádaného softwaru.
   * Zavedení pravidelných školení zaměstnanců ohledně bezpečného chování na internetu, identifikace podezřelých e-mailů a otevírání příloh.
   * Nasazení automatických aktualizací softwaru a operačního systému pro eliminaci zranitelností a potenciálních bodů vstupu pro škodlivý kód.
5. **Nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí:**
   * Nasazení systému správy událostí a informací (SIEM) pro sběr, analýzu a reportování bezpečnostních událostí.
   * Implementace nástrojů pro sledování síťového provozu a logování událostí na všech klíčových zařízeních.
   * Zřízení týmu pro reakci na incidenty (CSIRT) a vytvoření postupů pro rychlou a účinnou reakci na detekované bezpečnostní incidenty.
   * Pravidelné testování postupů pro reakci na incidenty (incident response) a simulace kybernetických útoků pro trénink týmu CSIRT.
   * Implementace systému centrálního logování událostí a automatizovaných alertů pro rychlou identifikaci a odpověď na bezpečnostní incidenty.
6. **Kryptografické prostředky:**
   * Používání šifrování datové komunikace pomocí protokolů jako TLS/SSL pro ochranu citlivých informací přenášených přes síť.
   * Zavedení šifrování uložených dat na serverech a zařízeních pro ochranu před neoprávněným přístupem.
   * Implementace správy klíčů a certifikátů pro řízení a zabezpečení kryptografických operací v síti a aplikacích.
   * Pravidelné revize a aktualizace kryptografických protokolů a šifrovacích algoritmů s ohled

# C) Hodnocení ekonomické náročnosti a návratnosti navržených opatření:

### 1. Fyzická bezpečnost:

1. **Instalace bezpečnostních kamer:**
   * **Ekonomická náročnost:** Vysoká
     + Náklady spojené s pořízením a instalací kamer, včetně infrastruktury pro jejich provoz.
   * **Návratnost investice:** Střední až vysoká
     + Snížení rizika krádeží, vandalismu a neoprávněného vstupu může snížit potenciální náklady spojené s takovými incidenty.
2. **Pravidelné školení zaměstnanců:**
   * **Ekonomická náročnost:** Střední až vysoká
     + Náklady spojené se školením zaměstnanců, včetně času a prostředků věnovaných na trénink.
   * **Návratnost investice:** Vysoká
     + Zvýšená povědomí zaměstnanců o bezpečnostních postupech může snížit riziko lidských chyb a potenciální náklady spojené s kybernetickými incidenty.
3. **Zavedení kontrol přístupu do budovy:**
   * **Ekonomická náročnost:** Střední až vysoká
     + Náklady spojené s implementací systémů kontroly přístupu, včetně pořízení a instalace zařízení.
   * **Návratnost investice:** Střední
     + Zvýšení fyzické bezpečnosti prostřednictvím kontroly přístupu může snížit riziko neoprávněného vstupu a potenciální náklady spojené s krádežemi a vandalismem.

### 2. Nástroje pro ochranu integrity komunikačních sítí:

1. **Implementace firewallů:**
   * **Ekonomická náročnost:** Střední
     + Náklady spojené s pořízením a konfigurací firewallů a dalších zařízení.
   * **Návratnost investice:** Vysoká
     + Zlepšení ochrany sítě před neoprávněným přístupem a škodlivým provozem může snížit riziko kybernetických útoků a potenciální náklady spojené s obnovením sítě po útoku.
2. **Nasazení systému detekce a prevence útoků:**
   * **Ekonomická náročnost:** Střední až vysoká
     + Náklady spojené s pořízením a konfigurací IDS/IPS systémů a dalších bezpečnostních technologií.
   * **Návratnost investice:** Vysoká
     + Identifikace a blokování podezřelého provozu může snížit riziko úspěšného kybernetického útoku a potenciální náklady spojené s následnými škodami a obnovou.

### 3. Nástroje pro ověřování identity uživatelů:

1. **Implementace dvoufaktorové autentizace:**
   * **Ekonomická náročnost:** Střední
     + Náklady spojené s implementací dvoufaktorové autentizace, včetně nákupu a nasazení příslušného softwaru a hardwaru.
   * **Návratnost investice:** Vysoká
     + Zvýšená úroveň ochrany před neoprávněným přístupem může snížit riziko úniku citlivých dat a potenciální náklady spojené s porušením bezpečnosti.
2. **Nastavení silných hesel:**
   * **Ekonomická náročnost:** Nízká
     + Minimální náklady spojené s implementací politiky silných hesel, zejména v porovnání s dalšími opatřeními.
   * **Návratnost investice:** Střední až vysoká
     + Snížení rizika úspěšného prolomení hesel může vést ke snížení nákladů spojených s kybernetickými útoky a ztrátou dat.
3. **Zavedení monitorovacích nástrojů:**
   * **Ekonomická náročnost:** Střední až vysoká
     + Náklady spojené s pořízením a nasazením monitorovacích nástrojů pro sledování aktivit uživatelů.
   * **Návratnost investice:** Vysoká
     + Detekce podezřelých aktivit a neoprávněných pokusů o přihlášení může snížit riziko kybernetických incidentů a potenciální náklady spojené s jejich řešením.

### 4. Nástroje pro ochranu před škodlivým kódem:

1. **Nasazení antivirového softwaru:**
   * **Ekonomická náročnost:** Nízká až střední
     + Náklady spojené s licencemi

# D) Návrh směrnice pro vedení organizace/firmy:

S ohledem na zajištění bezpečnosti práce v oblasti ICT a postupu řešení kybernetických incidentů, a také školení zaměstnanců v oblasti ochrany dat a bezpečnosti infrastruktury, navrhujeme vydání směrnice vedení organizace/firmy. Tato směrnice by měla být závazná pro všechny zaměstnance a zákazníky a měla by obsahovat následující body:

1. **Bezpečnostní opatření:**
   * Vyžaduje se dodržování stanovených bezpečnostních opatření a postupů pro minimalizaci rizika kybernetických hrozeb.
   * Zákazníci jsou povinni dodržovat bezpečnostní předpisy a směrnice stanovené organizací během používání produktů a služeb.
2. **Školení zaměstnanců:**
   * Vyžaduje se pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti a ochrany dat.
   * Noví zaměstnanci musí absolvovat školení v oblasti bezpečnosti před přidělením přístupu k citlivým informacím a systémům.
3. **Řízení incidentů:**
   * Stanoví postupy pro rychlé a efektivní řešení kybernetických incidentů včetně identifikace, vyhodnocení a odstranění hrozeb.
   * Určuje povinnosti jednotlivých oddělení a zaměstnanců v případě detekce nebo podezření na bezpečnostní incident.
4. **Ochrana dat:**
   * Definuje pravidla pro zacházení s citlivými daty, včetně jejich uchovávání, přenosu a zpracování.
   * Zavádí opatření k zajištění integrity, dostupnosti a důvěrnosti dat uložených v systémech organizace.
5. **Zálohování a obnova:**
   * Určuje požadavky na pravidelné zálohování dat a provádění testů obnovy pro minimalizaci ztráty dat v případě havárie nebo útoku.
6. **Pravidla pro přístup:**
   * Stanovuje pravidla pro přidělování a správu přístupových práv k informačním systémům a datům, včetně používání silných hesel a vícefaktorové autentizace.
7. **Audit a revize:**
   * Vyžaduje pravidelné audity a revize bezpečnostních opatření a postupů pro hodnocení jejich účinnosti a dodržování.
8. **Informovanost zaměstnanců:**
   * Stanovuje pravidla pro informování zaměstnanců o aktuálních hrozbách kybernetické bezpečnosti a opatřeních k prevenci.
9. **Závaznost a dodržování:**
   * Upozorňuje na důležitost dodržování této směrnice a varuje před důsledky nedodržení, včetně disciplinárních opatření.

Tato směrnice má za cíl zajistit, že všechny činnosti organizace jsou prováděny s maximální mírou bezpečnosti a že je udržována vysoká úroveň ochrany dat a infrastruktury před kybernetickými hrozbami. Zároveň má sloužit jako východisko pro školení zaměstnanců a informování zákazníků o bezpečnostních postupech a opatřeních.