**SYSTÉM ŘÍZENÍ RIZIK KYBERNETICKÉ BEZPEČNOSTI**

|  |  |
| --- | --- |
| Vypracoval: |  |
| Schválil: |  |
| Směrnice nabývá platnosti ode dne: |  |
| Změny ve směrnici jsou prováděny formou číslovaných písemných dodatků, které tvoří součást tohoto předpisu. Směrnice je součástí organizačního řádu školy. |

**Obecná ustanovení**:

Systém řízení rizik kybernetické bezpečnosti organizace vychází z analýzy požadavků:

* Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a jeho prováděcích předpisů, zejména pak z Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).
* Obecné nařízení o ochraně osobních údajů - GDPR
* Zákon č. 110/2019 Sb., o zpracování osobních údajů
* ČSN ISO/IEC 27001:2014 Informační technologie-bezpečnostní techniky-systémy řízení bezpečnosti informací-požadavky
* Zvláštní zákony, závazné pro jednotlivá odvětví

**1. Směrnice vychází z provedení analýzy rizik, kde vstupem je identifikace jednotlivých aktiv. Ta jsou též použita jako primární vstup do procesu analýzy rizik.**

**Aktivum** - Informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém příspěvkové organizace.

**Hrozba** - Potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu.

**Identifikace aktiv** - Identifikace aktiv spočívá v provedení obecného rozboru činností organizace, ve kterých v rámci svých jednotlivých agend dochází ke zpracování dat, a to jak v listinné, tak i elektronické formě. Vlastníkem aktiva (procesu) musí být vždy odpovědný pracovník, který má o aktivu nejlepší přehled a je za něj odpovědný (např. za personální agendu odpovídá Vedoucí personálního oddělení nebo personalista).

Pozn.: Při identifikování jednotlivých aktiv je důležité zaměřit se na ty zásadní činnosti, které organizace vykonává. Je podstatné nastavit vhodnou a přiměřenou úroveň, při které se dané procesy vyhodnotí jako relevantní aktiva.

**2. Hodnocení aktiv - Aktiva se hodnotí podle požadavků na „důvěrnost“, „integritu“, „dostupnost a odolnost“ a „kritičnost“ daného aktiva.**

**DŮVĚRNOST**

• Zajištění, že informace (data) jsou přístupné nebo sděleny pouze osobám k tomu oprávněným.

• Porušení důvěrnosti znamená nežádoucí zpřístupnění informace (dat) neoprávněné osobě; může mít negativní vliv na organizaci.

• Informace, obsažené v jednotlivých procesech, obsahují různě citlivá data a jejich kompromitace by mohla způsobit jiné dopady na organizaci.

**INTEGRITA**

• Zajištění správnosti a úplnosti informací (dat).

• Pokud dojde k nežádoucí změně dat, a to ať už úmyslně, náhodou, nebo technickým selháním, nemusí být tato nežádoucí změna vůbec odhalena a může uplynout dlouhá doba, než bude zaregistrována. Čím později se na tento bezpečnostní incident přijde, tím závažnější může být jeho dopad na subjekty údajů.

**DOSTUPNOST**

• Zajištění, že data jsou pro oprávněné uživatele přístupná v okamžiku jejich potřeby. Jedná se o důsledek zničení dat, úmyslné blokování či zahlcení technických prostředků, prostřednictvím kterých mají být tyto osobní údaje přístupny v požadovaném čase.

**KRITIČNOST**

• Vyjadřuje míru závislosti fungování organizace na realizaci hodnoceného aktiva.

• Hodnotí se na stupnici 1 až 10, kdy hodnota 1 vyjadřuje, že hodnocené aktivum je postradatelné, a naopak hodnota 10 označuje aktivum, bez kterého není možné fungování systému, nebo danou činnost realizovat.

• V případě hodnocení aktiv se hodnotí důležitost aktiva na fungování celé organizace.

• Stanovení hodnoty kritičnosti závisí na úsudku respondenta, který hodnocení provádí.

**3. Stupnice pro hodnocení důvěrnosti**

|  |
| --- |
| **Klasifikace dle vyhlášky č. 82/2018 Sb.**  |
| **Úroveň**  | **Popis**  | **Příklady požadavků na ochranu aktiva**  |
| Nízká - 1  | Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.  | Není vyžadována žádná ochrana.  |
| Střední - 2  | Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.  | Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.  |
| Vysoká - 3  | Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).  | Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikačních sítí jsou chráněny pomocí kryptografických prostředků.  |
| Kritická - 4  | Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).  | Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.  |

**4. Stupnice pro hodnocení integrity**

|  |
| --- |
| **Klasifikace dle vyhlášky č. 82/2018 Sb.**  |
| **Úroveň**  | **Popis**  | **Ochrana**  |
| Nízká – 1  | Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.  | Není vyžadována žádná ochrana.  |
| Střední – 2  | Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.  | Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).  |
| Vysoká – 3  | Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.  | Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.  |
| Kritická – 4  | Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.  | Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).  |

**5. Stupnice pro hodnocení dostupnosti**

|  |
| --- |
| **Klasifikace dle vyhlášky č. 82/2018 Sb.**  |
| **Úroveň**  | **Popis**  | **Ochrana**  |
| Nízká – 1  | Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).  | Pro ochranu dostupnosti je postačující pravidelné zálohování.  |
| Střední – 2  | Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.  | Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.  |
| Vysoká – 3  | Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.  | Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.  |
| Kritická – 4  | Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.  | Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.  |

**6. Stupnice pro hodnocení kritičnosti**



**7. Stanovení úrovně hrozeb**

|  |  |  |  |
| --- | --- | --- | --- |
| **Úroveň**  | **Stupeň hrozby**  | **Frekvence**  | **Zranitelnost**  |
| **1**  | Velmi nízká  | • hrozba je nepravděpodobná • hrozba nebyla realizována v posledních 5 letech • nepředpokládá se, že daná situace může nastat  | • zranitelnost neexistuje • existují kvalitní procesy a opatření, které hrozbě brání • nejsou zaznamenány pokusy o překonání opatření  |
| **2**  | Nízká  | • hrozba je mírně pravděpodobná • hrozba byla realizována déle než před rokem • je možné, že se daná situace může znovu opakovat  | • zranitelnost neexistuje • existují kvalitní procesy a opatření, které hrozbě přímo brání • nejsou zaznamenány pokusy o překonání opatření  |
| **3**  | Střední  | • hrozba je pravděpodobná • hrozba byla realizována v posledním roce • je možné, že se daná situace může znovu opakovat  | • zranitelnost je možná • existují kvalitní procesy a opatření, které hrozbě přímo brání • jsou zaznamenány neúspěšné pokusy o překonání opatření  |
| **4**  | Středně vysoká  | • hrozba je pravděpodobná • hrozba byla realizována v posledním roce • lze očekávat, že se daná situace může znovu opakovat  | • zranitelnost existuje • procesy a technická a/nebo organizační opatření jsou zavedeny částečně a plně dané hrozbě nebrání • jsou známy částečně úspěšné pokusy o narušení bezpečnosti  |
| **5**  | Vysoká  | • hrozba je vysoce pravděpodobná • hrozba byla realizována v posledním měsíci • lze s praktickou jistotou očekávat, že se daná situace může znovu opakovat  | • zranitelnost existuje • procesy a technická a/nebo organizační opatření jsou zavedeny částečně a plně dané hrozbě nebrání • jsou známy částečně úspěšné pokusy o narušení bezpečnosti  |
| **6**  | Kritická  | • hrozba je vysoce pravděpodobná • hrozba byla realizována v posledním měsíci • lze s praktickou jistotou očekávat, že se daná situace může znovu opakovat ve velmi blízké budoucnosti  | • zranitelnost existuje • procesy a technická a/nebo organizační opatření bránící dané hrozbě neexistují • jsou známy úspěšné pokusy o narušení bezpečnosti  |

**8. Výpočet rizika**

Míra rizika je určena jako součin číselných parametrů hodnoty aktiva a úrovně hrozby. Míra rizika je kalkulována pro každou kombinaci aktivum/hrozba.

Kalkulace probíhá dle vzorce:

R = Ha × Úh, kde: R = Výsledné parciální riziko Ha = Hodnota aktiva (bod 2 – 6)

Pro stanovení **Hodnoty aktiva** se využívá vzorec: 𝑯𝒂=𝑫+𝑰+𝑫𝑶+𝑲

(D = Důvěrnost, I = Integrita, DO = Dostupnost, K = Kritičnost)

Úh = Úroveň hrozby (bod 7)

**9. Stupnice pro hodnocení rizika**

|  |  |  |  |
| --- | --- | --- | --- |
| **Označení**  | **Riziko**  | **Popis rizika**  | **Hodnota rizika** |
| **Bez barvy**  | **Nízké**  | Riziko je považováno za přijatelné.  | 0-19  |
| **Barva zelená**  | **Střední**  | Riziko je dlouhodobě akceptovatelné, ale v rámci zlepšování bezpečnosti systému by měly být podniknuty systematické kroky k jeho snížení.  | 20-41  |
| **Barva žlutá**  | **Vysoké**  | Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho snížení v blízké budoucnosti.  | 42-71  |
| **Barva červená**  | **Kritické**  | Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.  | 72-132  |

**10. Parciální rizika Střední školy, Základní školy a Mateřské školy, Frýdek-Místek, p.o.**

(prázdná tabulka ke stáhnutí zde)

**11. Kontrolní plán k zabezpečení rizik**

|  |  |  |  |
| --- | --- | --- | --- |
|   |   | **Měsíc**   |  |
|  | **Oblast kontroly**  | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **Kontrolu provedl (jméno + podpis)** |
| Automatizované, člověk provádí kontrolu anomálií | Kontrola zabezpečení počítačů v nepřítomnosti zaměstnance (vypnutí PC)  | \* | \* | \* | \* | \* | \* | \* | \* | \* | \* | \* | \* |   |
| Kontrola dodržování pravidel nakládání s přihlašovacími údaji – denně  | \* | \* | \* | \* | \* | \* | \* | \* | \* | \* | \* | \* |   |
| sledování a analýza technických zranitelností provozu sítě, monitoring DNS záznamů | \* | \* | \* | \* | \* | \* | \* | \* | \* | \* | \* | \* |   |
| Provádí člověk | kontrola důležitých bezpečnostních logů firewallu (využití sítě) – měsíčně  | \*  | \* | \* | \*  | \* | \* | \* | \* | \* | \* | \*  | \* |   |
| Školení zaměstnanců - dodržování pravidel kybernetické a fyzické bezpečnosti  |   | \*  |   |   |   |   |   | \*  |   |   |   |   |   |
| Kontrola anomálií technických zranitelností provozu sítě | \* |   |   |   |   |   | \* |   |   |   |   |   |   |
| kontrola zálohy konfigurací databáze v zabezpečeném úložišti, příp. fyzická kontrola serveru |   | \* |   |   |   | \* |   |   |   | \* |   |   |   |
| přezkoumání přístupových oprávnění uživatelů a administrátorů  |   | \*  |   |   |   |   |   |   | \* |   |   |   |   |
| kontrola záznamů o přístupech k místním a sdíleným aplikacím  |   |   | \*  |   |   |   |   |   |   | \* |   |   |   |
| kontrola zálohování dat (čitelnost a obnova dat)  | \*  |   |   |   |   |   | \*  |   |   |   |   |   |   |
| kontrola legálnosti a správnosti instalovaného SW a aplikací |   |   |   | \*  |   |   |   |   |   |   |   | \*  |   |
| kontrola zaměstnanců a techniky s povoleným VPN přístupem k síti |   | \* |   |   |   |   |   |   | \* |   |   |   |   |
|  | kontrola uživatelský oprávnění |  |  |  |  |  |  | \* |  |  |  |  |  |  |