Analýza rizik

Audit zahrnoval mapování celkového prostředí klienta, v návaznosti na získané údaje byla zpracována analýza rizik. Na základě této analýzy rizik by měla organizace přijmout vhodná organizační a technická opatření, a to v pořadí vyplývající z analýzy rizik a v souladu s doporučeními uvedenými ve zprávě.

Zpracování probíhá v listinné a elektronické podobě, kdy elektronická evidence vykazuje vysokou míru vyspělosti, avšak neobsahuje všechny kontrolní prvky v kontextu Nařízení GDPR. U listinné podoby zpracování OÚ mnohdy dochází k duplicitám zpracování OÚ. Analýza taktéž prokázala nízkou míru odolnosti listinné podoby zpracování OÚ vůči identifikovaným hrozbám.

Řízení rizik má být vykonáváno podle článku 25 a článku 32 Nařízení Evropského parlamentu a Rady EU 2016/679. Řízení rizik je prováděno s cílem určit vhodná technická a organizační opatření, která je nezbytné zavést pro zajištění bezpečnosti osobních údajů při jejich zpracování Objednatelem a pro zmírnění nebo eliminaci rizik pro práva subjektu údajů vztahujícím se k realizovanému zpracování.

Na základě identifikace primárních aktiv bylo provedeno ohodnocení primárních aktiv dle jejich kritičnosti pro organizaci. Následně byla provedena definice hrozeb a identifikace pravděpodobnosti výskytu hrozeb u daného aktiva. V dalším kroku bylo provedeno expertní posouzení zranitelnosti jednotlivých aktiv vůči hrozbám. Výstupem výpočet celkové míry rizika.

***Celý proces analýzy rizik obsahuje následující kroky:***

* Určení a ohodnocení primárních aktiv
* Identifikace pravděpodobnosti hrozeb
* Identifikace zranitelnosti (rizikovosti)
* Výpočet celkové míry rizika

***Celý proces analýzy rizik obsahuje následující základní pojmy:***

* hrozba (threat) – jakákoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti aktiva;
* zranitelnost (vulnerability) – vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou;
* celková míra rizika – pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti;
* opatření (countermeasure) – technické nebo organizační opatření, které snižuje zranitelnost a chrání aktivum před danou hrozbou;

Zpracovatel určil primární aktiva v kontextu problematiky GDPR na základě úvodního sběru informací a jejich vyhodnocení.

Klíčovým krokem posouzení rizik, která primárním aktivům hrozí, je ohodnocení samotných primárních aktiv. To je provedeno posouzením požadavků na důvěrnost, integritu a dostupnost aktiv, případně dat v aktivech obsažených a služeb aktivy poskytovaných.

Jelikož organizace nemá zavedený registr aktiv, který by obsahoval skutečné hodnoty těchto aktiv, byla Zpracovatelem vytvořena následující stupnice hodnoty primárních aktiv, která vyjadřuje, nakolik jsou tato primární aktiva pro Objednatele kritická:

Tabulka 1: Stupnice hodnocení aktiv

| **Stupeň** | **Hodnota** | **Kritérium** |
| --- | --- | --- |
| 1 | Velmi nízká | Ztráta, poškození, narušení bezpečnosti primárního aktiva má jen nepatrný nebo žádný vliv na ochranu osobních údajů v rámci organizace Objednatele. |
| 2 | Nízká | Ztráta, poškození, narušení bezpečnosti primárního aktiva má nízký dopad na zákonné povinnosti Objednatele v rámci ochrany osobních údajů. Narušením primárního aktiva nedojde k uplatnění sankcí v rámci Nařízení Evropského parlamentu a Rady EU 2016/679. |
| 3 | Střední | Ztráta, poškození, narušení bezpečnosti primárního aktiva má střední dopad na zákonné povinnosti Objednatele v rámci ochrany osobních údajů. Narušením primárního aktiva nedojde k uplatnění sankcí v rámci Nařízení Evropského parlamentu a Rady EU 2016/679. Porušení zákonných povinností nebude mít zásadní vliv na fungování organizace Objednatele jako celku. |
| 4 | Vysoká | Ztráta, poškození, narušení bezpečnosti primárního aktiva je velmi významná, může vést k neakceptovatelnému porušení zákonných požadavků v rámci ochrany osobních údajů. Narušením primárního aktiva pravděpodobně dojde k uplatnění sankcí v rámci Nařízení Evropského parlamentu a Rady EU 2016/679. Porušení zákonných povinností bude mít vliv na fungování organizace Objednatele jako celku. |
| 5 | Velmi vysoká | Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z Nařízení Evropského parlamentu a Rady EU 2016/679. Narušením primárního aktiva dojde k uplatnění sankcí v rámci Nařízení Evropského parlamentu a Rady EU 2016/679. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace Objednatele jako celku. |

Kvalifikace aktiv byla provedena na základě expertního posouzení Zpracovatelem, jelikož přesná hodnota aktiv pro organizaci nebyla stanovena. Tuto metriku je vhodné následně zavést a zařadit ji do pravidelného hodnocení v rámci organizace.

|  |
| --- |
| **Hrozby a identifikace pravděpodobnosti hrozeb**  Prvním krokem hodnocení rizik je identifikace hrozeb a zranitelností. Východiskem tohoto hodnocení je seznam obvyklých hrozeb dle standardů a hrozeb týkající se ochrany osobních údajů vycházejících z Nařízení Evropského parlamentu a Rady EU 2016/679 či vycházející z dané problematiky.  Hrozba představuje vliv, jehož následkem je poškození analyzovaného systému IT a jeho aktiv. Cílem je identifikovat hrozby, kterým mohou být vystavena primární aktiva Správce v jeho správě nebo využívaná v jeho činnosti a pravděpodobnosti výskytu této hrozby. V následující tabulce jsou uvedeny hrozby, která jsou relevantní k posuzovaným primárním aktivům. Vždy je uvedena kategorie hrozeb a vysvětlení, co se pod jejich jednotným označením skrývá. |

Tabulka 2: Popis hrozeb

|  |  |
| --- | --- |
| **Hrozby, kategorie** | **Popis** |
| Vnější útoky | Zneužití přístupu k PC s možností neautorizovaného přístupu k OÚ nebo diskreditace OÚ Zneužití přístupu k počítačové síti s možností neautorizovaného přístupu k OÚ nebo diskreditace OÚ Krádež nebo prolomení hesla do IS nebo aplikace s možností neautorizovaného přístupu k OÚ nebo diskreditace OÚ Útok na IS nebo aplikace s cílem diskreditace či zcizení OÚ nebo omezení funkčnosti Útok na web s možností zcizení nebo modifikace OÚ, která jsou na webové prezentaci uvedeny Cílený útok na OÚ s motivem jejich odcizení a neoprávněného užití s možností cílené diskreditace organizace Narušení referenčních OÚ v aplikacích nebo IS Fyzické zcizení nebo poškození primárního aktiva včetně listinných evidencí s osobními daty Průnik z vnější sítě do vnitřní sítě (prolomení perimetru) s cílem zcizení nebo kompromitace OÚ uložených v IS nebo aplikacích Kompromitace dohledových prostředků nebo prostředků ke sledování a monitorování přístupu k OÚ Kompromitace identity oprávněného uživatele Správce nebo Zpracovatele. |
|
|
|
|
|
|
|
|
|
| Technické chyby | Chyby zálohování Výpadek elektřiny Výpadek hardwaru koncové stanice Výpadek softwaru koncové stanice Poškození nebo ztráta dat Mechanické poškození listinné evidence osobních údajů (požár, voda) Narušení řádné čitelnosti listinné evidence osobních údajů (požár, voda, slunce) Poškození/selhání programového vybavení Nedostatečná ochrana vnějšího perimetru Nedostatečná údržba informačního systému nebo aplikace, kde jsou evidovány OÚ Nedostatečné postupy při identifikaci a odhalení incidentů Dlouhodobé přerušení podpory dodavatele SW Nedostatečná ochrana prostředků IS Technické chyby ochrany úložišť listin obsahující OÚ |
|
|
|
|
|
|
|
|
|
| Lidský faktor | Obecná chyba uživatele Opomenutí uživatele Nedostatečné školení nebo povědomí o nakládání s OÚ nebo jejich ochraně OÚ Zkoušení prolomení zabezpečení uživatelem Poškození fyzické vrstvy sítě Zavlečení škodlivého SW Porušení bezpečnostní politiky uživatelem Zneužití oprávnění ze strany uživatelů Zneužití oprávnění ze strany administrátorů Narušení fyzické bezpečnosti – kancelář, serverovna Nepřítomnost/zranění/smrt administrátora informačního systému Nedostatečné vymezení bezpečnostních pravidel Nedostatečná míra nezávislé kontroly Nedostatečná ochrana úložišť listin obsahující OÚ |
|
|
|
|
|
|
|
|
| Narušení integrity OÚ | Neoprávněné manipulování evidencemi OÚ na úrovni IS nebo aplikací pod správou Správce Neoprávněné manipulování s listinnými evidencemi obsahující OÚ Provedení neoprávněných činností Zneužití vedených osobních údajů Nevhodné či nesprávné nastavení přístupových oprávnění Fyzické narušení listiny obsahující OÚ |
|
|
|
|
| Neoprávněný přístup | K OÚ má přístup osoba, která k danému úkonu nemá oprávnění Modifikace vedených OÚ Nedostatečné monitorování činnosti uživatelů Nedostatečné monitorování činnosti administrátorů |
|
|
|
| Narušení dostupnosti | Nedostupnost osobních údajů z důvodu pochybení organizačního charakteru Nedostupnost osobních údajů z důvodu technického pochybení |
|
| Ztráta osobních údajů | Nevhodná manipulace s listinnou evidencí obsahující OÚ Technické chyby v IS uchovávající osobní údaje Úmyslné zcizení OÚ v listinné podobě z listinné evidence Úmyslný export OÚ z IS nebo aplikací Výmaz OÚ z IS nebo aplikací Předání listinné evidence OÚ neautorizované osobě bez udání důvodu a bez dostatečné evidence a povinnosti navrátit předané OÚ |
| Narušení práv a svobod subjektu údajů | Narušení práva na soukromí Narušení práva na ochranu cti a důstojnosti Narušení práva na informační sebeurčení Narušení práva na život Narušení práva na duševní a tělesnou integritu Narušení práva na informace Narušení práva na ochranu osobních údajů Úmyslná kompromitace osobních údajů třetím subjektem Narušení zákazu diskriminace Narušení ochrany identity Hmotné ztráty subjektu údajů Neoprávněné zrušení pseudonymizace |

Tabulka 3: Stupnice hodnocení pravděpodobnosti hrozby

|  |  |  |
| --- | --- | --- |
| **Stupeň** | **Četnost výskytu** | **Kritérium** |
| 1 | Velmi nízká | Uplatnění hrozby je vysoce nepravděpodobné nebo je pravděpodobnost nulová. |
| 2 | Nízká | Hrozba se může uplatnit méně než 1 x za rok, respektive se uplatnila, nebo se může projevit v určitém kritickém období. |
| 3 | Střední | Hrozba se může uplatnit zhruba 1x za rok, resp. hrozba se jednou uplatnila v průběhu kritického období. |
| 4 | Vysoká | Hrozba se může uplatnit zhruba 1x za měsíc, resp. hrozba se uplatnila více než 1x v kritickém období. |
| 5 | Velmi vysoká | Hrozba se může uplatnit zhruba 1x týdně, resp. hrozba se uplatnila denně v kritickém období |
|

|  |
| --- |
| **Identifikace zranitelnosti (rizikovosti)**  Odhad zranitelností zahrnuje slabá místa posuzovaných aktiv. Pro analýzu budou použita následující kritéria pro hodnocení zranitelností: |

Tabulka 4: Stupnice hodnocení zranitelnosti aktiv

|  |  |  |
| --- | --- | --- |
| **Stupeň** | **Zranitelnost aktiva** | **Kritérium** |
| 1 | Velmi nízká | Hrozba se nemůže vůči aktivu uplatnit. |
| 2 | Nízká | Aktivum je chráněno, resp. je odolné velmi dobře proti uplatnění hrozby. |
| 3 | Střední | Aktivum je chráněno částečně, respektive je mírně odolné proti uplatnění hrozby. |
| 4 | Vysoká | Aktivum je chráněno, resp. je odolné velmi nedostatečně proti uplatnění hrozby. |
| 5 | Velmi vysoká | Aktivum není chráněno vůbec. |

|  |  |
| --- | --- |
| Míra zranitelnosti a účinnost existujících ochranných opatření spolu úzce souvisí. Míra zranitelnosti určitou hrozbou je vlastností aktiva. Může být snížena jedině vhodným protiopatřením. | |
| **Celková míra rizika (riziková expozice)**  Cílem identifikace míry rizika je zajištění optimálního výběru ochranných nebo nápravných opatření, která působí proti těmto rizikům.  Ohodnocení míry rizika se provádí jako kombinace (součin) tří hodnot: | |
|  | Hodnota aktiva na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.  Pravděpodobnost hrozby na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.  Zranitelnost na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká. |
| **Rizikové skóre se vypočítává podle níže uvedené rovnice:**  Rizikové skóre = hodnota aktiva \* pravděpodobnost \* zranitelnost  Rizikové skóre se pohybuje v rozmezí 0–125 bodů.  Hranice akceptovatelného rizika je předmětem manažerského rozhodnutí na straně klienta. | |

**Příklad (slíbený), jak může analýza vypadat:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **AKTIVUM** | **HROZBA** | **ZRANITELNOST** | **RIZIKO** |
| **1** | **Osobní složky**  **zaměstnanců** | Zcizení | Neuzamykatelná skříň | 3 |
|  | Opatření: | V rozpočtu na příští rok alokovat částku 30 tis. Kč na instalaci zámků | |  |
| **2** | **Mzdová agenda** | Únik osobních dat | Není uzavřen dodatek GDPR | 5 |
|  | Opatření: | Bez odkladu uzavřít dodatek ke smlouvě s externím zpracovatelem mzdové agendy | |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Slíbené příklady konkrétních hrozeb:**

* Útočník vloží do formuláře na webových stránkách nebezpečný kód;
* Útočník zašle nebezpečný kód prostřednictvím e-mailu;
* cizí osoba nebo i zaměstnanec při setkání na vašem pracovišti ukradne přenosný pevný disk, flash paměť s daty apod.;
* cizí osoba nebo i zaměstnanec si vyfotí náhodně rozložené dokumenty s osobními údaji dalších zaměstnanců;
* zaměstnanec omylem nebo úmyslně odstraní data z IS;
* déšť otevřeným oknem či místností vedoucí vodovodní trubky zatopí a zničí počítačové servery a telekomunikace;
* black out;
* oknem odhozený nedopalek do spisovny (umístěna ve sklepě, pouze malá okna směřující do ulice) způsobí požár spisovny atd.

Celkové výsledky rizikového skóre jsou uvedeny v „RA ve vazbě na GDPR“. Z nich vyplývá následující.

V každém případě je nutno pracovat s bezpečnostním povědomím zaměstnanců s cílem zvýšit jejich zodpovědnost za ochranu osobních údajů. K tomu je nutné jim připravit vhodné technické podmínky, a to jak na úrovni fyzického zabezpečení (uzamykání kanceláří, ordinací apod., uzamykání registratur/skříní se spisy, …), tak i v rámci nezbytné podpory ze strany ICT. Zároveň ale platí, že aby ICT mohlo plnohodnotně tuto podporu uživatelům poskytovat, musí k tomu mít ty správné prostředky a připraveno vhodné prostředí.

***Základní doporučení na základě analýzy:***

1. Seznámit se s novými právními normami, které řeší problematiku ochrany osobních údajů (GDPR).
2. Zpracovat nový přehled osobních údajů ve škole (účel zpracování, osobní a údaje zvláštní kategorie, zákonné zpracování, zpracování se souhlasem, …). Minimalizovat zpracovávané osobní údaje.
3. Připravit tzv. karty záznamů o činnostech zpracování podle čl. 30 nařízení.
4. Nastavit vnitřní procesy zacházení s osobními údaji (nová směrnice ředitele školy k ochraně osobních údajů podle nového nařízení EU).
5. Doplnit o problematiku GDPR další dokumenty školy (Organizační řád, Spisový a skartační řád, Školní řád, pracovní náplně, kamerový systém, …).
6. Jmenovat pověřence pro ochranu osobních údajů, stanovit mu pracovní náplň a plat.
7. Zkontrolovat platné smlouvy se zpracovateli osobních údajů (poskytovatelé informačních systémů, čipových a vstupních karet, zpracování platů, cloudové uložiště a další)
8. Zpracovat ochranu osobních údajů i ve vztahu k firmám (fakturace, kupní smlouvy, …)
9. Dát žákům, zaměstnancům a zákonným zástupcům zaměstnanců podepsat nový informovaný souhlas se zpracováním osobních údajů.
10. Revize formulářů školy s osobními údaji (zda neobsahují nadbytečné osobní údaje, zákaz používání nevhodných formulářů na internetu, …).
11. Zákaz předávání osobních údajů žáků a zaměstnanců školy třetím osobám soukromého práva (nabídky pomůcek, knih, aktivit pro žáky a zaměstnance, …).
12. Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu.
13. Informovat zaměstnance, žáky, zákonné zástupce žáků o zpracování osobních údajů (GDPR).
14. Pravidelná kontrola dodržování ochrany osobních údajů ze strany vedení školy.
15. Do školního vzdělávacího programu zapracovat problematiku prevence a výchov k ochraně osobních údajů.