Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Bezpečnost technických prostředků pro práci s osobními údaji ve sportovním klubu

Bakalářská práce

Petr Voldán

Školitel: RNDr. Libor Dostálek

České Budějovice 2020

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÉ PRÁCE

Student: Petr Voldán
(jméno, příjmení, tituly)

Obor – zaměření studia: Aplikovaná informatika

Katedra/ústav PřF JU, kde bude práce vypracována a obhájena: UAI

Školitel: RNDr. Libor Dostálek
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Garant z PřF JU: .....
(jméno, příjmení, tituly, katedra – jen v případě externího školitele)

Školitel – specialista, konzultant: Ing. Petr Břehovský
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Téma bakalářské práce: Bezpečnost technických prostředků pro práci s osobními údaji ve sportovním klubu

Cíle práce:

- Rešerše nařízení GDPR pro potřeby bakalářské práce, tj, která ustanovení GDPR jsou relevantní pro oblast kvalifikační práce a proč
- Analyzovat možnosti zabezpečení osobních údajů
- Identifikovat nejčastější slabiny zabezpečení
- Navrhnout bezpečnostní opatření pro různé typy organizací
- Vypracování vzor kodexu (příručky) pro sportovní klub

Základní doporučená literatura:

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679

Financování práce .....

Školitel práce .....podpis: .....

U externích vedoucích fakultní garant práce .....podpis: .....

Garant oboru bak. studia (nepožaduje se u oboru biologie) .....podpis: .....

Vedoucí katedry/ústavu PřF JU, kde proběhne obhajoba.....podpis: .....

V Českých Budějovicích dne .....Podpis studenta .....

Bibliografické údaje:

Voldán, P., 2020: Bezpečnost technických prostředků pro práci s osobními údaji ve sportovním klubu. [Security of the technical means used for personal data processing in sports organizations, Bc. Thesis, in Czech], – 39 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace:

Tato práce se zabývá ochranou a bezpečností zpracování osobních údajů ve sportovních organizacích. Vysvětluje náležitosti, za jakých podmínek je možné osobní údaje legitimně zpracovávat, a jak zajistit jejich bezpečnost. Na závěr předkládá návrh transparentních a korektních pravidel pro práci s osobními údaji.

Abstract:

This thesis deals with the protection and the security of personal data processing in sports organizations. It explains under which conditions it is legitimate to process those data and how to achieve their security. It the end, it proposes transparent and correct rules for the personal data processing.

Klíčová slova: osobní údaje, GDPR, sportovní organizace, bezpečnost

Keywords: personal data, GDPR, sports organizations, security

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracovala samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb., v platném znění, souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb., zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledků obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích, 09.12. 2019 Podpis.....

Poděkování

Děkuji všem, kteří se podíleli na aspektech důležitých pro vznik této práce za jejich cenné rady a vyslovenou důvěru.

Obsah

Úvod

Osobní údaje se v poslední době stávají široce obchodovatelným artiklem. Zejména v prostředí internetu jsou tyto informace více než cenné. Z tohoto sběru osobních údajů, a nemusí jít zrovna o zažité „jméno a adresa“, může být každý z nás v tomto prostředí svým způsobem monitorován, a posléze jsou mu nabízeny relevantní nebo nevyžádané nabídky služeb.

Právě s postupujícím sběrem, a následným použitím, osobních údajů vznikla potřeba tento sběr regulovat a kontrolovat. Zejména velké společnosti díky svým kapacitám byly schopny shromáždit a zpracovat více dat, než bylo dosud vůbec myslitelné, a náležitě je využít.

Díky právním předpisům, regulacím, právům a možnostem kontroly má fyzická osoba větší přehled o tom, k jakému účelu jsou jeho údaje sbírány a zpracovávány. Obzvlášť poslední právní úprava, Obecné nařízení (EU) o ochraně osobních údajů (Obecné nařízení 2016/679, známé jako „GDPR“), přinesla do této problematiky nový dech, reagující na moderní dobu a její požadavky, zejména v oboru nových technologií a s postupem rozvíjející se globalizace.

Problémem ochrany osobních údajů není jen oprávněnost tyto údaje shromáždit a dále zpracovávat, ale je věnována pozornost i problematice jejich uchovávání a zabezpečení, aby se k údajům nedostala neoprávněnou cestou i třetí strana.

Problematika zabezpečení osobních údajů není v dokumentu GDPR dále rozebírána, opírá se o obecné definice, jelikož není možné v obecných právních předpisech zakotvit konkrétní postupy a nástroje, právě kvůli nutnosti být aktuální, bez ohledu na v současnosti dostupné technologie. Navíc, ne každé zpracování je stejné, a proto je důležité pro každou situaci stanovit okolnosti zabezpečení „na míru“ podle účelu, rozsahu, kontextu a citlivosti tohoto zpracování.

Sportovní organizace shromažďují a uchovávají osobní údaje o svých a jiných členech, a proto se povinnost řídit se při zpracování těchto údajů nařízením GDPR nevyhýbá ani jim. Problémem, k jehož řešení má tato práce přispět, je obzvláště fakt, že malé sportovní kluby, fungující na bázi dobrovolnosti, nemají o problematice hluboké povědomí a se správnou implementací GDPR tápou.

V těchto klubech však dochází ke zpracování osobních údajů, přinejmenším k evidenci členů klubu. Zároveň mohou používat techniku, která z pohledu bezpečnosti nemusí být vůbec bezpečná.
Může se jednat např. o staré počítače, přenos dat po otevřené síti, nebo přenosy dat pomocí nezabezpečených flash disků.

Tato práce by měla právě těmto subjektům pomoci při aplikaci zákonných požadavků nebo při kontrole již aplikovaného postupu zpracování dat. Měla by vysvětlit jakých zásad se má zpracovatel osobních údajů (tj. sportovní klub) držet a jak zabezpečit technické prostředky proti bezpečnostním rizikům.

1 Ochrana osobních údajů

1.1 Úvod

Historie ochrany osobních údajů sahá daleko do minulosti, avšak jako její první uchopitelný důkaz se dá považovat Deklarace práv člověka a občana z roku 1789 (Francie), která se stala východiskem pro následující listiny zabývající se lidskými právy až do dnešních dní. Během let prošla ochrana osobních údajů spoustou proměn, a my se tak dostáváme do současnosti, kdy je ve světě rozvíjející se globalizace potřeba nastavit jednotná mezinárodní pravidla.

1.2 Obecné nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů, známé jako GDPR, je právním dokumentem Evropské unie a jedná se o právní akt nařízení. Nařízení je přímo aplikovatelný právní předpis ve všech státech Evropské unie v plném znění. Naproti tomu směrnice je jakýsi standard, do jehož podoby musí všechny státy přizpůsobit svou legislativu. (1)

Toto nařízení, po svém vstoupení v platnost, nahradilo dřívější právní úpravy ochrany osobních údajů, kterými byly zejména Směrnice Evropského parlamentu a Rady 95/46/ES a zákon č. 101/2000 Sb. o ochraně osobních údajů. (2, s. 1)

Dřívější právní úpravy, zejména mezinárodní, nebyly schopné reagovat na rychlý nástup technologií (mobilní telefony, cloudové služby, sociální sítě) a vzhledem k mezinárodnímu, až globálnímu přesahu těchto technologií bylo nutné tyto požadavky naplnit na bázi vyššího než národního celku (v tomto případě Evropské unie). Zároveň se toto nařízení vztahuje i na mimoevropské organizace, které shromažďují a zpracovávají údaje občanů Evropské unie.

Další výhodou nynější právní úpravy je určitá volnost ve vztahu ke správnému zpracování osobních údajů. Správnost zpracování není dána pomocí výčtu opatření nebo striktního postupu. Každé zpracování může probíhat jiným způsobem, a proto se jeho správnost řídí pomocí kriteriální analýzy ve vztahu k účelu, rozsahu, kontextu a citlivosti zpracování. (3)

1.3 Základní pojmy

Pro potřeby této práce jsou zde citovány základní pojmy převzaté z článku 4 Nařízení, zákona č. 115/2001 Sb., o podpoře sportu, a některé další dále používané pojmy (2, s. 33).

Rozumí se:

- „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

- „zpracováním“ jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

- „evidencí“ jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

- „správcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;

- „zpracovatelem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

- „příjemcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování;

- „souhlasem“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

- „porušením zabezpečení osobních údajů“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

- „sportovní organizací“ právnická osoba založená za jiným účelem než dosažení zisku, zahrnuje-li předmět činnosti této právnické osoby činnost v oblasti sportu,

- „subjektem údajů“ člen sportovní organizace, fyzická osoba.

2 Sportovní klub

2.1 Úvod

Sportovním klubem (dále také jen „klub“) se rozumí dobrovolné sdružení občanů zapsané jako spolek podle OZ a dále, podle definice, právnická osoba založená za jiným účelem než dosažení zisku, zahrnuje-li předmět činnosti této právnické osoby činnost v oblasti sportu. (4)(5)

Pro potřeby této práce budeme vycházet z toho, že sportovní klub žádá o podporu ze státního rozpočtu, a proto se na něj vztahují některá ustanovení ze zákona č. 115/2001 Sb., o podpoře sportu.

Sportovní klub potřebuje ke své činnosti potřebuje v základu evidovat své členy – sportovce, trenéry a jiné osoby. Povinnost vést evidenci pro něj vyplývá právě ze zákona č. 115/2001 Sb., o podpoře sportu. Pro potřeby této práce jde zejména o tyto údaje členů (5):

- Jméno a příjmení
- Rodné číslo, příp. datum narození
- Adresa místa pobytu

Dalšími údaji potřebnými shromažďovanými a dále zpracovávanými pro legitimní činnost sportovního klubu můžou být:

- Audiovizuální záznamy
- Sportovní výsledky

2.2 Zákonnost zpracování

K zabezpečení legitimity zpracování osobních údajů sportovní klub potřebuje naplnit podstatu některé z podmínek podle čl. 6 odst. 1 Nařízení, kterými jsou (2, s. 36):

- subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Pro potřeby zajištění činnosti sportovního klubu přicházejí v úvahu následující tři právní tituly.

2.2.1 Právní povinnost

(ve smyslu čl. 6 ods.1 bod c)

V některých případech je zpracování osobních údajů nutné k naplnění právní povinnosti vůči státu. V případě sportovního klubu se může jednat například o zákon č. 115/2001 Sb., o podpoře sportu, kde je v § 3e uvedeno:

(2) Sportovní organizace žádající o podporu ze státního rozpočtu podle § 6b odst. 1 písm. a) je povinna bez zbytečného odkladu zapsat do rejstříku tyto údaje a jejich změny:

c) jméno, popřípadě jména, příjmení a rodné číslo sportovců a trenérů evidovaných ve sportovní organizaci; v případě cizinců rovněž datum narození, adresa místa pobytu5) a státní občanství,

d) datum, od kdy sportovec nebo trenér začal vykonávat činnost, pro kterou byl u sportovní organizace v daném kalendářním roce evidován,

e) datum, od kdy sportovec nebo trenér přestal vykonávat činnost uvedenou v písmenu d),

V tomto případě, kdy je nutné zpracovávat osobní údaje podle právní povinnosti, není již nutné hledat pro tento účel zpracování (vedení evidence) další zákonné důvody.

2.2.2 Oprávněný zájem

(ve smyslu čl. 6 ods.1 bod f)

V různých případech je potřeba zpracovávat osobní údaje potřebné pro legitimní činnost klubu, jakou může být prezentace klubu, zveřejňování sportovních výsledků členů, nebo evidence dalších údajů členů klubu. V takovém případě nemůže být zpracování odůvodněno výše uvedenou právní povinností, jelikož ta se vztahuje pouze na omezený rozsah údajů. Nabízí se použití Souhlasu, a v prvopočátku platnosti Nařízení byl nadužíván téměř jako jediný zákonný titul (16), nicméně u něj existuje stále možnost jeho odvolatelnosti, která není pro potřeby klubu příliš vhodná (např. výsledkové listiny s nezveřejněným jménem vítěze). Dále není možné podmiňovat vstup do sportovního klubu podepsáním Souhlasu, jelikož Souhlas musí být svobodný a v případě jeho odmítnutí není možné bránit přístupu ke službě (= členství v klubu) (2, s. 37). Takový souhlas by mohl být považován za vynucený, tedy nikoliv svobodný.

V případě použití Oprávněného zájmu jako zákonného titulu je potřeba zvážit, jestli díky uplatňování zájmů organizace nejsou závažně dotčena práva a svobody subjektů údajů. V případě nevyváženosti těchto zájmů a svobod není možné Oprávněný zájem použít a musí se najít jiný titul. (7)(17)

2.2.3 Souhlas

(ve smyslu čl. 6 ods.1 bod a)

Souhlas se použije tehdy, pokud nelze zákonnosti zpracování dosáhnout jinými důvody uvedenými v ods.1 čl. 6 Nařízení. Pomocí Souhlasu tedy sportovní klub může také získat zákonnou pravomoc nakládat s osobními údaji subjektů údajů. (2, s. 37) (3)(6)

Souhlas se poskytuje k předem stanovenému účelu zpracování.

Souhlas musí být:

- Svobodný – „nesouhlas“ nesmí být překážkou přístupu ke „službě“ – zde např. členství ve sportovním klubu
- Konkrétní – stanovený pro konkrétní určitý účel
- Informovaný – subjekt musí být transparentně informován o tom, jak budou jeho údaje zpracovávány a na koho se v případě dalších dotazů obrátit
- Jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

Určitým „problémem“ při použití Souhlasu je fakt, že ho může subjekt údajů kdykoliv odvolat (viz. příklad v 2.2.2).

Ve všech případech musí být člen klubu o zpracování osobních údajů transparentně informován.

3 Bezpečnost

3.1 Úvod

Obecné nařízení není v otázce zabezpečení osobních údajů nijak konkrétní. Je to jednak proto, že není možné obsáhnout veškeré technické možnosti zpracování a také kvůli tomu, aby se legislativa příliš neupnula na v současnosti dostupné technologie, jelikož by se musela neustále novelizovat. Proto je znění prvního odstavce článku 32 následující (2, s. 51):

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.

Dále v odstavci jsou uvedené některé případné, ale pouze rámcové způsoby zabezpečení:

a) *pseudonymizace a šifrování osobních údajů;*
b) *schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;*
c) *schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;*
d) *procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.*

Shrnutím požadavků legislativy nám vychází, že pro výběr vhodných nástrojů pro zajištění bezpečnosti pro zajištění organizační a technické bezpečnosti zpracování dat, bude potřeba nejdříve provést analýzu rizik.

3.2 Hrozby a rizika

Zprvu je nutné si vyjasnit, jaké jsou obecně nejčastější hrozby a rizika, které mohou hrozit datům nebo výpočetní technice používaným ve sportovním klubu.

3.2.1 Data

Datům v principu hrozí tři základní hrozby:

Ztráta (Krádež) – Data jsou ztracena (ztráta notebooku, externího disku, flash disku) nebo ukradena

Zničení – Data jsou zničena (přírodní živly, selhání disku, požár)

Změna (Neoprávněná, Náhodná) – neoprávněná osoba se dostane k datům a provede v nich změnu; informační systém (program) provede náhodnou změnu a tím data kompromituje (zneplatní)

Z každé z těchto hrozeb vychází rizika, která pro klub mohou být závažná nebo kritická a musíme se pokusit je snížit či eliminovat.

Těmi nejzávažnějšími riziky v našem případě mohou být:

- Ztráta informací
- Kompromitace informací
- Odcizení osobních údajů
- Krádež identity (díky znalosti osobních údajů osoby se za ni může někdo jiný vydávat)

3.2.2 Technika

V základu se mohou techniky týkat následující hrozby:

- **Neoprávněný přístup** – k technice se dostane někdo cizí (krádež techniky s daty, instalace malwaru, změna nastavení)
- **Poruchy hardware** – nejsme schopni s technikou pracovat
- **Neoprávněné využívání výpočetního výkonu** – „útočníkovi“ nejde o data, ale o náš výkon

Hrozby můžeme dále rozdělit podle způsobu, jak k nim došlo na:

- Cizí úmysl
- Lidská chyba
- Technické selhání

3.2.3 Aktuální hrozby

V současné době se na poli kybernetické bezpečnosti objevují některé významné skutečnosti, ne které ve své výroční zprávě reaguje Národní úřad pro kybernetickou bezpečnost (8)

Mezi takové skutečnosti patří:

- Úniky dat
- Riziko odcizení dat
- DDoS (přetížení systémů nebo techniky vedoucí k nedostupnosti)
- Kryptomining (neoprávněné využívání výpočetního výkonu náročnými výpočty)
- Zastaralé komponenty
- Zastaralost softwaru
- Aktualizace

3.3 Možnosti zabezpečení

3.3.1 Bezpečnostní opatření

Nyní je třeba si ujasnit, jaké směry opatření můžeme použít ke snížení a eliminaci rizik. Jedná se o opatření:

• **Technická** – opatření na snížení bezpečnostních rizik pomocí prostředků fyzické a technologické povahy

• **Organizační** (resp. procesní) - opatření na snížení bezpečnostních rizik pomocí změn procesů a úpravou vnitřních pravidel a dokumentace

Nejsnáze dosáhneme požadovaného výsledku kombinací obou směrů.

Pro data

- Řízení přístupu
- Šifrování
- Zálohování

Pro techniku

- Řízení přístupu
- Síťové zabezpečení
- Údržba
- Aktualizace
- Antivirový software

3.4 Nejčastější slabiny zabezpečení

V oblasti slabého zabezpečení stále vyvstává jeden problém, který svou závažností překonává všechny ostatní.

3.4.1 Slabá hesla

Podle průzkumu společnosti Avast provedeného v roce 2019 používá slabá hesla až 95 % respondentů. Nejčastějším problémem je používání stejných hesel u více účtů. Dále je to používání veřejných informací jako hesla (např. jména členů rodiny, jméno mazlíčka, datum narození). (9)

Neustále se opakující, přitom jednoduchou obranou je:

- Dostatečná délka (v dnešních podmínkách se doporučuje 16 znaků)
- Používání čísel a speciálních znaků
- Nepoužívat informace nesouvisející s osobou ani s určitou službou

3.5 Analýza rizik ve sportovním klubu

Aby mohl klub správně vyhodnotit svou situaci v oblasti ochrany osobních údajů, musí nejprve provést analýzu a inventarizaci činností zpracování. Pro tuto potřebu byl vytvořen dotazník, který je obsažen v příloze 1. Po jeho vyplnění by měl mít klub přehled o legitimitě zpracování, operacích zpracování a přijatých organizačních a technických opatření zajišťující jejich zabezpečení. Na základě výstupu klub stanoví míru rizika. Podle rizikových parametrů jsou následně přijata bezpečnostní, organizační i technická, opatření. (18)

Pro oblast organizačních a technických opatření byly vypracovány modelové situace různých sportovních organizací, na kterých byla provedena analýza rizik a navrhovaná opatření k jejich snížení či eliminaci.

V následující části práce se nachází neformální kvalitativní analýza rizik jednotlivých případů. Kvantitativní analýza (pomocí tabulky) se nachází v příloze 2.

3.5.1 Případ 1

Situace

Malý sportovní klub do 50 členů, v kanceláři je 1 počítač, který není připojený do sítě. Je v něm uložena evidence osobních údajů členů a pomocí něj jsou vypracovávány výsledkové listiny.

Přihlášky členů jsou uloženy v uzamykatelné schránce.

Klub má omezený rozpočet na zajištění technické bezpečnosti.

Identifikace aktiv:

- Data
    - Údaje členů klubu uložená v tabulce v počítači
    - Přihlášky v listinné podobě v bezpečnostní schránce
- Technika
    - Počítač nepřipojený do sítě

Identifikace relevantních hrozeb a zranitelností:

- **Nedostatečná autentizace** – k datům může kdokoliv
- **Nedostatečné fyzické zabezpečení** – fyzický přístup k aktivům
- **Nedostatečné zálohování**
- **Poruchy HW**
- **Zastaralý SW** – žádné aktualizace, náchylnost k virům přineseným na paměťovém médiu

Shrnout pravděpodobnost a dopad

Počítač a bezpečnostní schránka s dokumenty se nachází v uzamčené kanceláři v neveřejně přístupném objektu. Proto existuje jen malé riziko, že by se k datům nebo technice fyzicky dostal někdo neoprávněně s cílem data odcizit. Data však mohou být kompromitována přímo členy klubu, kteří budou mít do prostoru přístup.

Vzhledem k omezenému rozpočtu se jedná o starý a neaktualizovaný počítač, který vzhledem ke stáří komponentů může kdykoliv selhat a data mohou být ztracena.

Navrhnout opatření

V rámci přístupu k datům by měla být jednoznačně určena pravidla, kdo k nim přístup mít má a kdo nemá. Počítač by tím měl být chráněný heslem. Pokud se v počítači budou nacházet data ve velkém rozsahu nebo citlivá data (nemusí jít přímo o osobní údaje, může jít o jiná citlivá data používaná k činnosti klubu, např. účetnictví, předávací protokoly, protokoly o zápůjčce vybavení sportovcům…) mělo by být zváženo případné šifrování celého disku.

Pokud by byl počítač s diskem odcizen a disk by byl zašifrovaný, může to organizaci zbavit povinnosti hlásit takové porušení zabezpečení Úřadu pro ochranu osobních údajů, jelikož není možné předpokládat, že by se k datům na disku někdo dostal.

Co se týče stavu techniky, vzhledem k jejímu stáří by měl být kladen vysoký důraz na pravidelné zálohování. To může být prováděno například na flash disk, který bude uložený v bezpečnostní schránce. Flash disk by měl být obecně zašifrovaný, jelikož u něj existuje větší riziko ztráty než u jiné techniky.

3.5.2 Případ 2

Situace

Klub do 100 členů, který má ve svých prostorech umístěný server, na kterém je databáze s osobními údaji členů. K databázi přistupuje n uživatelů pomocí n počítačů taktéž umístěných v prostorech klubu (nejedná se o osobní počítače členů). Minimálně jeden z počítačů je přenosný, proto je připojení do sítě realizováno bezdrátově pomocí Wi-Fi. Stejně tak je na bezdrátové síti připojena i tiskárna.

Identifikace aktiv

- Data
    - Údaje členů klubu uložená v databázi na serveru
- Technika
    - 2–n počítačů
    - Server
    - Tiskárna
    - Wi-Fi router

Identifikovat zranitelnosti a hrozby

- **Nedostatečná autentizace**
- Nedostatečné fyzické zabezpečení
- **Nedostatečné zálohování**
- Poruchy HW
- Zastaralý SW
- **Nedostatečně bezpečná síťová architektura**

Shrnout pravděpodobnost a dopad

Prostory klubu se nachází v neveřejném objektu, který je navíc hlídaný bezpečnostní službou. Nedá se tedy předpokládat riziko neoprávněného fyzického přístupu.

Prvním možným rizikem je neoprávněný přístup do databáze nebo neprokazatelnost, kdo provedl v databázi změny.

Dalším rizikem může být neoprávněný přístup do sítě a posléze k technickým prostředkům v případě nedostatečného zabezpečení sítě, například během konání sportovní akce.

Není pravděpodobné, že by byl používaný SW zastaralý, jelikož je pravidelně aktualizován. To samé se týká i poruch HW, který je udržován a podle potřeby nahrazován.

Navrhnout opatření

Nejprve je nutné vyřešit zákonitosti neoprávněného přístupu k datům a technice. Měla by být určena jasná pravidla, kdo a k jakým datům je oprávněn přistupovat. Toho lze docílit řízením přístupu a zároveň logováním změn k jejich případnému prokazování.

V otázce zálohování, v případě shromažďování většího množství dat, jejichž zničení by nás mohlo významně poškodit, je doporučeno zálohovat data i jinam než pouze lokálně. V případě nějaké nepředvídatelné události (např. požár, povodeň) by byla zničena i lokální záloha dat. Proto by měla být data zálohována i do geograficky odlišné lokality.

Pokud je nějakým způsobem používána síť, musíme mít jistotu, že se do ní neoprávněně nedostane někdo další. Není možné, aby byly v prostorách klubu, v místech veřejnosti přístupných, nechráněné síťové zásuvky nevyžadující žádné ověření. V případě použití bezdrátové sítě by taková síť měla používat dostatečné zabezpečení, kterým je dostatečně aktuální protokol a dostatečná složitost hesel.

3.5.3 Případ 3

Situace

Klub do 1000 členů. Údaje členů jsou uložena v informačním systému, ke kterému je přistupováno pomocí N počítačů z vnitřní sítě i z vnější sítě prostřednictvím internetu. Pomocí informačního systému jsou prováděny veškeré operace zpracování osobních údajů.

Identifikovat aktiva a jejich hodnotu

- Data
    - Údaje členů klubu v informačním systému
- Technika
    - N – klientských počítačů
    - Síťové prvky
    - Servery

Identifikovat zranitelnosti a hrozby

- **Nedostatečná autentizace**
- Nedostatečné fyzické zabezpečení
- Nedostatečné zálohování
- Poruchy HW
- Zastaralý SW
- Nedostatečně bezpečná síťová architektura
- Chybné přiřazení přístupových práv
- **Nechráněné komunikační linky**
- **Sociální inženýrství**

Shrnout pravděpodobnost a dopad

Vzhledem k možnému přístupu „zvenčí“ se zde jako nejzávažnější riziko jeví neoprávněný přístup k informačnímu systému v důsledku nedostatečné autentizace nebo případně chybného přiřazení přístupových práv. Takové riziko je závažné pro svobody a práva subjektů údajů, proto mu musí být věnována odpovídající pozornost.

Taktéž může být středním rizikem nedostatečně bezpečná síťová architektura, která dovoluje relativně snadný přístup do vnitřní sítě.

Dalším rizikem je používání nechráněných komunikačních linek ať už při vzdálené práci s osobními údaji, kdy mohou být odposlechnuta samotná data, taktéž i při přístupu do vnitřní sítě nebo k informačnímu systému, kdy mohou být odposlechnuta autentizační data.

Další hrozbou, která se objevuje v případě větších organizací je sociální inženýrství. I v případě, kdy budu mít dostatečná technická bezpečnostní opatření se může stát, že se útočník dostane k aktivům pomocí lidského faktoru.

Navrhnout opatření

V rámci snížení rizika neoprávněného přístupu se jedná zejména o dostatečná organizační opatření týkající se řízení přístupu. Tato problematika musí zohledňovat dostatečné autentizační mechanismy, které musí zabránit uhádnutí nebo prolomení hesla. Práva v rámci informačního systému musí být nastavena způsobem odpovídajícím zpracování, které daná osoba s daty provádí.

Síťová architektura musí respektovat požadavky na bezpečnost podobně jako je uvedeno v předchozím odstavci, nesmí umožňovat neoprávněný a nelogovaný vstup do sítě. Tomu se zabrání pomocí IEEE 802.1X. Dále je potřeba zabránit vzdálenému přístupu k vnitřním prvkům, čehož dosáhneme pomocí firewallu.

Co se týká problematiky sociálního inženýrství, zde neexistuje jednoznačná a vždy fungující obrana. Záleží na schopnostech útočníka a stejně tak na obezřetnosti vnitřních pracovníků. V principu se jako organizační opatření doporučuje dostatečné školení pracovníků a mezi technická opatření by šlo zařadit například podepisování mailů elektronickým podpisem.

4 Kodex chování

4.1 Úvod

Vzhledem k tomu, že obecným nařízením nelze dosáhnout na každý konkrétní detail ve všech odvětvích pro všechny potřeby, jsou na různých úrovních institucí a podniků vypracovávány kodexy chování (dále také jen „kodex“), které mají společný základ pro dané odvětví. (13)

Může se jednat například o kodexy chování bank, škol, cestovních kanceláří.

V této kapitole práce budou shrnuty informace z předchozích kapitol a následně z nich bude vypracován návrh na společný kodex chování pro potřeby sportovních klubů.

4.1.1 Teorie

Kodexy chování vycházejí z článku 40 Nařízení a jejich účelem je upřesnění uplatňování zásad při práci s osobními údaji v různých odvětvích nebo skupinách správců, v nichž dochází ke stejnému nebo obdobnému druhu zpracování osobních údajů. (2, s. 56)

Upřesnění provádění povinností podle Nařízení se v kodexu chování mohou týkat mimo jiné:

- oprávněné zájmy, jež správci v konkrétních situacích sledují;
- shromažďování osobních údajů;
- informace poskytované dětem a jejich ochranu a způsob získávání souhlasu nositele rodičovské zodpovědnosti nad dítětem;
- opatření a postupy uvedené v článcích 24 a 25 a opatření k zajištění bezpečnosti zpracování podle článku 32;
- ohlašování případů porušení zabezpečení osobních údajů dozorovým úřadům a oznamování těchto případů porušení subjektům údajů;

Kodex chování je formou samoregulace, není právně vymahatelný. Má sloužit právě k řešení nejasností a specifik, která se vyskytují v odvětvích nebo ve společenstvích správců se stejným nebo obdobným způsobem zpracování osobních údajů.

Kodex musí projít schvalovacím procesem Úřadu pro ochranu osobních údajů („ÚOOÚ“), není možné, aby si takový kodex vytvořil Správce jako interní dokument, nebo ve spolupráci mezi omezeným počtem Správců a vydával ho za kodex chování ve smyslu GDPR. K takovému „internímu“ kodexu ÚOOÚ při posuzování souladu s GDPR při zpracování a ochraně osobních údajů nepřihlíží.

Pokud se Správce přihlásí k dodržování schváleného Kodexu chování, je povinen zajistit pravidelné monitorování jeho plnění nezávislým subjektem. V opačném případě bude ze subjektů přihlášených k dodržování Kodexu vyloučen.

V současné době tedy nemůže žádný správce nebo skupina správců prohlašovat, že používá kodex chování dle GDPR, neboť ÚOOÚ doposud žádný takový kodex chování neschválil. Tvorba takového kodexu chování je komplexním a dlouhodobým procesem.

4.1.2 Doporučení

Před samotným kodexem by bylo vhodné zopakovat některé zásady sběru a zpracování osobních údajů (2, s. 35):

1. Zákonnost, korektnost a transparentnost – údaje jsou sbírány a zpracovávány pouze po splnění jedné z podmínek zákonnosti zpracování
2. Určitý účel – údaje jsou shromažďovány a zpracovávány pouze pro vyslovený určitý účel a nesmějí být zpracovávány pro jiný účel – v tu chvíli je potřeba nový Souhlas, Právní povinnost, nebo Oprávněný zájem
3. Minimalizace údajů – údaje jsou shromažďovány pouze v nezbytném rozsahu ve vztahu k účelu
4. Přesnost – údaje jsou v případě potřeby aktualizovány, pokud to není možné, musí být bezodkladně vymazány
5. Integrita a důvěrnost – údaje jsou náležitě zabezpečené pomocí technických a organizačních opatření před neoprávněným zpracováním a před ztrátou, zničením nebo poškozením.

4.2 Kodex chování sportovního klubu

4.2.1 Úvod

Z výše uvedené teorie je jasné, že není možné vypracovat Kodex chování v rámci jedné osoby nebo jednoho klubu. Kodex by musel být vypracován na úrovni vyššího celku, například. sportovní svaz nebo sportovní asociace. Navíc, v každém oboru sportu jsou jiné potřeby pro zpracování osobních údajů, proto by nemohl být vypracován jeden kodex pro sportovní organizace, ke kterému by se mohly všechny organizace přihlásit.

Vzhledem k náplni práce bylo nakonec rozhodnuto, že budou vypracovány nejdůležitější body relevantní pro problematiku sportovních organizací, které může organizace použít jako svůj interní kodex – nejedná se tedy o oficiální schválený Kodex chování, ale slouží jako nástroj transparentnosti.

K vypracování takového kodexu byla použita přizpůsobená struktura doporučená metodikou Úřadu pro ochranu osobních údajů. (14)

4.2.2 Příklad interního kodexu

V příloze č. 3.

Závěr

Závěrem práce bych se pokusil shrnout co se v průběhu práce změnilo a jak se podařilo naplnit jednotlivé cíle.

- Rešerše nařízení GDPR pro potřeby bakalářské práce, tj. která ustanovení GDPR jsou relevantní pro oblast kvalifikační práce a proč

V práci je vysvětleno, co GDPR přináší, jaké jsou hlavní přínosy oproti dřívějším úpravám, a dále za jakých podmínek je vůbec možné v prostředí sportovního klubu zpracování osobních údajů provádět.

- Analyzovat možnosti zabezpečení osobních údajů
- Identifikovat nejčastější slabiny zabezpečení
- Navrhnout bezpečností opatření pro různé typy organizací

V rámci řešení těchto cílů bylo nejprve nutné zjistit, co nám o zabezpečení osobních údajů říká Nařízení. Vzhledem k obecnému popisu opatření bylo nutné identifikovat relevantní rizika a jak na ně reagovat.

Identifikace nejčastějších slabin zabezpečení byla provedena rešerší reportů společností a organizací zabývajícími se kybernetickou a IT bezpečností. Podle nich byly vybrány relevantní zranitelnosti, které byly vzaty v úvahu při návrhu opatření.

Podle typu organizace byla identifikována jejich aktiva a zranitelnosti které jsou pro tato aktiva relevantní a navrhnuta opatření ke snížení rizik.

- Vypracování Kodexu chování (příručky) pro sportovní klub

Tento bod se nepodařilo zcela naplnit, jelikož není možné v jedné osobě, nebo v rámci jednoho sportovního klubu vytvořit kodex chování pro celé odvětví (nebo skupinu relevantních klubů). V kapitole je nejprve teoreticky popsáno, co kodex znamená, a shrnutí potřebných kroků k jeho tvorbě. Z metodické struktury Kodexu chováni byly vybrány nejdůležitější relevantní body a ty byly dále rozebrány pro tvorbu interního kodexu sportovní organizace.

Praktickým přesahem této práce je pokus o vytvořená legitimních a transparentních pravidel pro zpracování osobních údajů – interního kodexu malého sportovního klubu. Tento interní kodex nemá žádnou právní závaznost a není možné žádným způsobem vyžadovat jeho dodržování. Jedná se však o nástroj transparentnosti a čestnosti klubu, který se k osobním údajům chová zodpovědně a korektně

Takový interní kodex chování, ač existuje pouze na lokální úrovní klubu, se může stát důležitou součástí dalšího procesu, ve kterém se budou postupně utvářet kodexy vyšších celků, případně podobně zaměřených nebo podobně velkých klubů, a v konečném důsledku, po jednáních a korekcích na vyšší úrovni organizace, může být předložen Úřadu pro ochranu osobních údajů k posouzení a schválení. Tím by vznikl Kodex chování, který by definoval operace zpracování a nakládání s daty pro celé odvětví, čímž vy vznikly transparentní záruky o korektnosti přístupu o ochraně osobních údajů.

Mým cílem nebylo nastavit jednotná pravidla pro každý jednotlivý klub s různými specifiky, ale pokusit se alespoň rozhýbat kolečka ve svém nejbližším okolí a přispět tím k budoucímu řešení v celém sektoru.

Seznam použité literatury

[1] Nařízení, směrnice a další právní akty. *Europa.eu* [online]. [cit. 2019-11-20]. Dostupné z: https://europa.eu/european-union/eu-law/legal-acts_cs

[2] *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).*

[3] Základní příručka k GDPR. *Úřad pro ochranu osobních údajů* [online]. [cit. 2019-11-20]. Dostupné z: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/archiv=0&p1=3938

[4] *Zákon č. 89/2012 Sb., občanský zákoník*

[5] *Zákon č. 115/2001 Sb., o podpoře sportu.*

[6] *Pracovní skupina zřízená podle článku 29 - Pokyny pro souhlas podle nařízení 2016/679.*Dostupné také z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31896

[7] *Stanovisko č. 6 /2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES.* Dostupné také z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf

[8] *Zpráva o stavu kybernetické bezpečnosti ČR - 2018* [online]. [cit. 2019-11-20]. Dostupné z: https://www.nukib.cz/download/publikace/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf

[9] Slabá hesla používá 95 % lidí v Česku. *Avast* [online]. [cit. 2019-11-21]. Dostupné z: https://press.avast.com/cs-cz/slaba-hesla-pouziva-95-lidi-v-cesku

[10] Porušení zabezpečení. *Úřad pro ochranu osobních údajů* [online]. [cit. 2019-11-21]. Dostupné z: https://www.uoou.cz/poruseni%2Dzabezpeceni/ds-5020/archiv=0&p1=3938

[11] Desatero zpracování pro správce. *Úřad pro ochranu osobních údajů* [online]. [cit. 2019-11-21]. Dostupné z: https://www.uoou.cz/desatero%2Dzpracovani%2Dpro%2Dspravce/ds-4821/archiv=0&p1=3938

[12] Desatero omylů. *Úřad pro ochranu osobních údajů* [online]. [cit. 2019-11-21]. Dostupné z: https://www.uoou.cz/desatero%2Domylu/ds-4818/p1=4818

[13] Kodexy chování. *Úřad pro ochranu osobních údajů* [online]. [cit. 2019-11-21]. Dostupné z: https://www.uoou.cz/kodexy-chovani/d-29493/p1=3938

[14] Kodexy chování – metodická příručka 2.0. *Úřad pro ochranu osobních údajů* [online]. [cit. 2019-11-21]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=37244

[15] *Zákon č. 110/2019 Sb., o zpracování osobních údajů*

[16] Stanovisko č. 3/2014–K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti. UOOU [online]. [cit. 2019-11-21]. Dostupné z: https://www.uoou.cz/stanovisko-c-3-2014-k-nbsp-nadbytecnemu-vyzadovani-souhlasu-se-nbsp-zpracovanim-osobnich-udaju-a-nbsp-souvisejicimu-nespravnemu-plneni-informacni-povinnosti/d-11913/p1=1099

[17] Co znamenají „důvody oprávněných zájmů "? *Evropská komise* [online]. [cit. 2019-11-21]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_cs

[18] ČSN EN ISO/IEC 27002 (369798) Informační technologie – Bezpečnostní techniky – soubor postupů pro opatření bezpečnosti informací.

[19] JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1

[20] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

Přílohy

Příloha 1

Dotazník

Volně vložená

Příloha 2

Kvantitativní analýza rizik

Volně vložená

Příloha 3

Kodex chování

Příloha vázaná v práci

Kodex chování

Název kodexu chování.

Interní kodex pro potřeby sportovní organizace respektující Obecné nařízení o zpracování osobních údajů.

Určení správců, na které se kodex chování vztahuje (případně zpracovatelů).

Tento kodex se vztahuje na sportovní organizaci, která se zavázala k jeho dodržování.

Popis (operací) zpracování, na které se kodex vztahuje:

• definice a popis účelů zpracování, které správce zpracováním osobních údajů sleduje,

Data jsou zpracovávána v listinné a elektronické podobě.

Účely zpracování osobních údajů mohou být následující:

- Evidence členů klubu
- Prezentace činnosti klubu
- Marketingu (propagační materiály organizace)
- Žádosti o dotace na základě Zákona o podpoře sportu a ze soukromého sektoru

• rozsah údajů, které budou zpracovány (minimalizace rozsahu)

Pro účel **Evidence**:

- Jméno a příjmení
- Datum narození
- Adresu místa pobytu
- Kontaktní údaje

Dále pro účel **Prezentace** (například)**:**

- Audiovizuální záznamy
- Sportovní výsledky

• doba uchování údajů

Údaje jsou zpracovávány a uchovávány po celou dobu trvání účelů zpracování, a následujících n let poté, co subjekt údajů přestane vykonávat činnost (dobu uchovávání údajů po skončení účelu zpracování je nutné rozumně nastavit v závislosti na konkrétních případech).

• předávání osobních údajů (subjekty údajů, zpracovatelé, správci, předávání do zahraničí).

Údaje jsou předávány vyšším organizačním celkům (např sportovní svaz, sportovní asociace), dále příslušným státním orgánům a také poskytovatelům dotací z veřejného i soukromého sektoru.

Postupy pro zajištění aktualizace a přesnosti údajů.

Údaje jsou uchovávány v takové podobě, aby byla mohla být zajištěna jejich případná aktualizovatelnost. Členové klubu neprodleně nahlásí změnu v osobních údajích (např. změna bydliště) osobě pověřené za správu osobních údajů.

Postupy pro zajištění zákonnosti zpracování.

V otázce zajištění zákonnosti zpracování je vybrán odpovídající právní titul podle analýzy zpracovávaných dat.

Tam, kde je to možné, bude v rozsahu Jméno, Příjmení, Datum narození, Adresa, v případě, že se jedná o klub podléhající zákonu č. 115/2001 Sb., o podpoře sportu, bude použit jako právní titul **Právní povinnost**

Tam, kde se jedná o zpracování osobních údajů pro legitimní činnost klubu, kterými je evidence, prezentace, zveřejňování výsledků bude použit jako právní titul **Oprávněný zájem**

V ostatních případech, například pokud práva a svobody členů převyšují oprávněný zájem klubu, například za účelem použití audiovizuálních záznamů pro marketingové účely, bude použit **Souhlas.**

Postupy pro zajištění informovanosti subjektu údajů a veřejnosti.

Současně s přihláškou do sportovní organizace je zájemce informován o způsobu zpracování osobních údajů. Je informován o účelech zpracování, které jsou určité a předem známé, o délce doby zpracovávání údajů, o případném předávání údajů jiným Zpracovatelům a je srozuměn se svými právy ohledně přístupu k osobním údajům.

Postupy pro zajištění bezpečnosti osobních údajů:

• posouzení bezpečnosti

V rámci zajištění bezpečnosti je třeba provést inventarizaci všech zpracování osobních údajů a již existujících opatření (viz. Dotazník v příloze 1)

• soubor technických a organizačních opatření (řízení fyzického přístupu, řízení logického přístupu, zajištění čitelnosti osobních údajů oprávněnými osobami (včetně šifrování), logování a monitorování, použití identifikace a autentizace, použití hesel, zabezpečení komunikačního prostředí, zajištění funkčnosti, zálohování, archivace, kontinuita činnosti/obnova po mimořádné situaci, likvidace dat a datových nosičů, personální opatření atd.)

Následně je nutné provést analýzu rizik, tzn. identifikovat aktiva a hrozby, které těmto aktivům hrozí. V závislosti na provedené analýze rizik je potřeba na zjištěná rizika adekvátně reagovat. Příklady modelových situací a reakcí na rizika jsou uvedeny v části 3.5 této práce.

• způsob a periodicita ověření účinnosti přijatých technických a organizačních opatření

V případě, že se nějakým způsobem změní okolnosti zpracování (např. nasazení jiných technických prostředků) nebo nastane změna v účelech nebo rozsahu zpracování, je nutné provést novou analýzu. Jinak se analýza provádí minimálně jednou za rok.