Statutární město Brno, městská část Brno-střed

BEZPEČNOSTNÍ POLITIKA

Pokyn tajemníka č.: 8
Vydání č.: 1
Účinnost: 16.07.2018

Bc. Petr Štika, MBA, LL.M., v.r.
tajemník ÚMČ Brno-střed

Vydal/schválil: Bc. Petr Štika, MBA, LL.M.
Dne: 10.07.2018
Zpracovatel: Bc. Arnošt Kolbábek, vedoucí OI ÚMČ BS

Tento pokyn tajemníka je závazný pro: Úřad městské části Brno-střed

Projednáno v orgánech: *nejsou*

Osoba pověřená výkladem: Bc. Arnošt Kolbábek, vedoucí OI ÚMČ BS
Četnost kontroly aktuálnosti: ročně
Osoba pověřená kontrolou aktuálnosti: Bc. Arnošt Kolbábek, vedoucí OI ÚMČ BS

Související vnitřní předpisy:
Nejsou

Historie změn:

Datum	Číslo vydán	Strana	Článek	Stručný popis změny

Odkaz na předešlá vydání:
Nejsou

Související záznamy a formuláře:
Nejsou

Zrušovací ustanovení:
Metodický pokyn tajemníka č. 01/2010 – Pravidla provozu počítačové sítě

Článek 1
Účel

Účelem tohoto pokynu tajemníka je stanovení hlavních cílů v oblasti bezpečnosti v návaznosti na Informační koncepci Informačního systému Úřadu městské části Brno-střed v rámci dlouhodobého řízení IS.
Jsou v něm definovány požadavky na bezpečnost a popsány postupy a zásady dosahování bezpečnosti v spravovaných IS. Vymezuje pravomoci a zodpovědnost při ochraně informací a dalších aktiv v oblasti ICT.

Článek 2
Rozsah platnosti

Tento pokyn tajemníka je závazný pro všechny zaměstnance ÚMČ Brno-střed.

Článek 3
Základní terminologie

Identifikace - určení (zjištění, zadání) uživatelovy identity, například tím, že vloží (zapíše nebo potvrdí) své uživatelské jméno nebo kód (username, user-ID).

Uživatelské jméno (username, user-ID) - jméno osoby, která má právo využívat prostředky sítě nebo určitou službu.

Autentizace - proces ověření identity uživatele - ověření toho, že uživatel je skutečně tou osobou, za kterou se vydává. Ověření uživatele může být provedeno pomocí uživatelského hesla, USB tokenu iKey („klíčenka“), čipovou kartou, kartou s magnetickým proužkem.

Přístupové /uživatelské/ heslo (password, user password) - znakový řetězec používaný jako autentizační informace pro rozpoznávání uživatelů oprávněných používat ve stanoveném rozsahu určitý výpočetní prostředek nebo datový zdroj.

Přihlášení (login) - proces přihlášení do systému, kdy uživatel zadává uživatelské jméno a heslo.

Odhlášení (logout, logoff) - proces odhlášení uživatele od systému.

Autorizace - přidělování práv, která uživateli umožňují v informačním systému provádět definované operace. Je založena na právech, která přiděluje uživatelským účtům správce systému. U neanonymních účtů musí autorizaci předcházet autentizace. Nejčastěji jde o přiřazení práv (oprávnění) již ověřené (autentizované) entitě, tj. obvykle uživateli. Každý uživatel je oprávněn k úkonům odpovídajícím roli, kterou zastává. Nastavení přístupových práv uživatele provádí správce IS na základě funkčních míst a uživatelských rolí jednotlivých aplikací provozovaných v IS. Žádný uživatel pak nemá přístup k datům, která nejsou relevantní k jeho funkčnímu zařazení.

Přístupové právo - oprávnění uživatele používat daný objekt předem definovaným způsobem.

Řízení přístupu - je vymezení práv uživatelů při přístupu k prostředkům sítě. Jeho cílem je umožnit přístup autorizovaného uživatele, zabránit přístupu neautorizovaného uživatele, případně zabránit využití zdroje neautorizovaným způsobem.

Informační činnost - získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na hmotné nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na hmotných nosičích. Informační činnost je prováděna správci, provozovateli a uživateli informačních systémů prostřednictvím technických a programových prostředků.

Informační systém - funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností.

Provozní informační systém - informační systém zajišťující informační činnosti nutné pro vnitřní provoz příslušného orgánu, například účetnictví, správu majetku, a nesouvisející bezprostředně s výkonem veřejné správy. Některé integrované IS mohou spadat do obou kategorií, pak je na ně nutno pohlížet jako na ISVS.

Informační systém veřejné správy - soubor informačních systémů, které slouží pro výkon veřejné správy. Jsou jimi i informační systémy zajišťující činnosti podle zvláštních zákonů.

Aktivum - cokoliv, co má pro organizaci nějakou (nepominutelnou) hodnotu.

Škoda - vzniká ztrátou nebo snížením hodnoty aktiva. Škoda může být zanedbatelná, akceptovatelná, významná, katastrofická.

Útok - bývá příčinou ztráty nebo snížení hodnoty aktiva, útok je realizací hrozby.

Hrozba - označení pro potenciální příčinu nežádoucího incidentu, která může vyústit v poškození IS nebo úřadu. Hrozba představuje možnost útoku. Hrozba existuje díky zranitelnosti systému, který obhospodařuje aktiva úřadu.

Zranitelnost - je označení pro vlastnost, slabé místo aktiva nebo skupiny aktiv, které může být využito jednou nebo více hrozbami. Zranitelnost je též daná existencí zranitelných (slabých) míst systému a existencí potenciálních útočníků.

Bezpečnostní událost - je identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky, nebo selhání bezpečnostních opatření. Může se také jednat o jinou situaci, která dříve nenastala a může být z pohledu bezpečnosti informací důležitá.

Bezpečnostní incident - je jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací.

Riziko - kombinace pravděpodobnosti, že dojde k nežádoucí události a následků, které by z takové události mohly vzniknout. Pravděpodobnost uplatnění hrozby, důsledky uplatnění.

Článek 4
Definice, obsah a účel bezpečnostní politiky

Bezpečnostní politika Informačního systému Úřadu městské části Brno-střed je souhrn bezpečnostních zásad, pravidel, opatření, předpisů a procedur definujících způsob zabezpečení provozu IS Úřadu městské části, který má zajistit bezpečnost IS na požadované úrovni, s přihlédnutím k nákladové efektivitě.

Informační bezpečnost je na všech úrovních Úřadu městské části prosazována v souladu s deklarovanými cíli. Za její prosazování obecně odpovídají vedoucí zaměstnanci jednotlivých

organizačních jednotek Úřadu městské části. Základem prosazení informační bezpečnosti je zavedení a realizace jednotného systému řízení informační bezpečnosti do všech oblastí činnosti Úřadu městské části.

Bezpečnostní politika informačního systému Úřadu městské části obsahuje popis bezpečnostních opatření, která Úřad městské části Brno-střed uplatňuje při zajišťování bezpečnosti IS Úřadu městské části a která odpovídají požadavkům na bezpečnost stanoveným v Informační koncepci Úřadu městské části Brno-střed. Požadavky na bezpečnost informačního systému slouží k dosažení dlouhodobých cílů, kterých chce Úřad dosáhnout v oblasti řízení bezpečnosti IS. Těmito cíli jsou vždy:

a) bezpečnost dat, která jsou v IS Úřadu městské části zpracovávána,

b) bezpečnost technických a programových prostředků sloužících pro zajištění informačních činností

c) bezpečnost služeb, které jsou prostřednictvím těchto systémů poskytovány.

Základní bezpečnostní zásady a z nich vyplývající povinnosti uživatelů IS Úřadu městské části jsou uvedeny v Provozním řádu - Základní pravidla pro uživatele IS Úřadu městské části Brno-střed.

Pomocí bezpečnostní politiky IS Úřadu městské části jsou stanovena základní pravidla a doporučení zajišťující bezpečný provoz IS, integritu uložených dat a řízení přístupů do IS a k datům pro oprávněné uživatele na základě jejich funkčního zařazení v organizační struktuře úřadu.

Bezpečnostní politika IS Úřadu městské části rovněž obecně definuje bezpečné používání informačních zdrojů.

Nedílnou součástí systému bezpečnosti je dobré pochopení bezpečnostních opatření všemi zainteresovanými pracovníky a odpovídající povědomí všech zaměstnanců o bezpečnosti informačních systémů.

Bezpečnostní politika určuje normy, pravidla a předpisy, které definují způsob správy, ochrany a distribuce citlivých informací a jiných konkrétních informačních zdrojů v rámci úřadu. Specifikuje bezpečnostní opatření a způsob jejich implementace, stanovuje vhodné organizační postupy a určuje způsob použití výše uvedeného, který zaručuje přiměřenou bezpečnost odpovídající požadavkům bezpečnostní politiky úřadu.

Článek 5
Základní dlouhodobé cíle v oblasti bezpečnosti

Základní dlouhodobé cíle v oblasti bezpečnosti jsou stanoveny v Informační koncepci Úřadu městské části Brno-střed.

Základními bezpečnostními cíli bezpečnostní politiky tudíž je zajištění následujících stavů a činností:

1) trvalé a kvalitní zajištění dostupnosti, důvěrnosti a integrity dat (informací), které jsou zpracovávány v prostředí IS Úřadu městské části,
2) ochrana dat a prostředků IS Úřadu městské části,
3) zajištění bezpečné komunikace s okolím
4) zajištění odpovědnosti uživatele za jeho činnost v IS Úřadu městské části.

Bezpečnostní politika je základním obecným dokumentem pro proces systematického řešení bezpečnosti ICT v úřadu.

Článek 6
Základní požadavky na bezpečnost

Požadavky na bezpečnost IT jsou konkretizací základních bezpečnostních cílů:

TRVALÉ A KVALITNÍ ZAJIŠTĚNÍ DOSTUPNOSTI, DŮVĚRNOSTI, INTEGRITY A AUTENTICITY DAT

- Identifikace, autentizace a autorizace uživatelů – zajištění a aktivní řízení přístupu k IS Úřadu městské části a k datům v IS Úřad městské části (prohlížení, aktualizace) pro oprávněné uživatele na základě jejich funkčního zařazení,
- zajištění soukromí uživatelů – ochrana uživatele před zjištěním nebo zneužitím jeho identity jinými uživateli nebo cizími osobami,
- řízení provozu a monitoring počítačové sítě,
- existence systému pravidelného zálohování a archivace dat
- vytvoření plánu obnovy provozu IS (nebo jeho /kritických/ části) po havárii.

OCHRANA DAT A PROSTŘEDKŮ IS

- zajištění personální bezpečnosti (budování bezpečnostního vědomí uživatelů IS),
- zajištění fyzické bezpečnosti prostředků IS Úřadu městské části: fyzické zabezpečení prostředků IS Úřadu městské části vhodným umístěním (polohou, zábranou), zabránění neoprávněnému vstupu či přístupu, zajištění prostředků IS proti zneužití a odcizení,
- existence systému komplexní ochrany před škodlivými programy (viry, nepřátelské kódy),
- vybudování bezpečnostních mechanismů vůči napadení zevnitř (široká škála bezpečnostních pravidel od úrovně budování, administrace IS Úřadu městské části, po školení zásad, jak se mají uživatelé i správci IS chovat),
- ochrana IS Úřadu městské části před napadením z externích sítí (hackeři, získání dat či porušení integrity dat, vyřazení služeb sítě, apod.) – bezpečnostní opatření zamezující možnosti průniku do vnitřní sítě (ochrana serverů, aktivních prvků a uživatelských stanic),
- ustanovení správce agendy (ISVS nebo provozní agendy), stanovení osobní odpovědnosti za data v IS, popř. za konkrétní HW nebo SW prostředky IS,
- ustanovení správce IS Úřadu městské části.

ZAJIŠTĚNÍ BEZPEČNÉ KOMUNIKACE S OKOLÍM

- používání bezpečných komunikačních cest,
- pravidla bezpečné komunikace mezi úřadem a jinými subjekty (především s orgány veřejné správy),
- používání prostředků pro šifrování přenášených dat.

Článek 7
Role a odpovědnosti v oblasti řízení bezpečnosti

Bezpečnost IS Úřadu městské části spadá do oblasti provozní problematiky úřadu, proto schvalování a vyhlašování realizace bezpečnostní politiky včetně základního personálního obsazení a stanovení rolí a odpovědností v oblasti bezpečnosti provádí tajemník úřadu.

Úřad městské části Brno-střed definuje pro IS Úřad městské části vždy roli

- správce systému (správce IS Úřadu městské části), kterým je zaměstnanec nebo jiná fyzická osoba, která zajišťuje řízení provozu informačního systému Úřadu městské části,
- bezpečnostního správce systému, kterým je zaměstnanec nebo jiná fyzická osoba, která zajišťuje kontrolu bezpečnosti IS Úřadu městské části;

zároveň Úřad definuje pro každou roli soubor určených činností a potřebných oprávnění a pravomocí pro provádění těchto činností v informačním systému Úřadu městské části a souhrn příslušných odpovědností.

Pro bezpečnost IS jsou dále přijata následující organizační opatření:

- definování bezpečnostní komise, její pravomoci a odpovědnosti,
- definování odpovědnosti a povinností uživatelů IS Úřadu městské části.

7.1. Bezpečnostní komise

Bezpečnostní komise má tyto členy:

- vedoucí odboru informatika – předseda komise,
- tajemník
- zástupce vedoucího odboru informatika,
- v případě potřeby pracovník odboru.

Bezpečnostní komise:

- je poradním orgánem tajemníka úřadu,
- formuluje zásady bezpečnostní politiky,
- definuje bezpečnostní cíle a sleduje jejich zavádění,
- navrhuje metody a postupy v oblasti bezpečnosti IS Úřadu městské části,
- podniká kroky vedoucí ke zvýšení bezpečnosti dat a prostředků v IS Úřadu městské části,
- schvaluje specifické role a odpovědnosti v oblasti bezpečnosti IS Úřadu městské části v rámci celého úřadu,
- kontroluje, aby bezpečnost byla součástí procesu plánování v oblasti informatiky,
- koordinuje implementaci opatření v oblasti bezpečnosti IS Úřadu městské části,
- zodpovídá za průběžné monitorování a ověřování funkčnosti zavedených bezpečnostních opatření,
- podporuje iniciativy týkající se bezpečnosti IS Úřadu městské části,

- prosazuje, aby podpora bezpečnostní politiky ze strany vedení byla viditelná v celém úřadě,
- zodpovídá za řízení přístupu k informačním systémům a informačním aktivům,
- definuje potřebné požadavky na lidské znalosti a na finanční náklady,
- prosazuje zvyšování bezpečnostního uvědomění uživatelů IS Úřadu městské části,
- navrhuje řešení disciplinárních problémů vůči bezpečnosti,
- hodnotí účinnost bezpečnostní politiky.

7.2. Bezpečnostní správce

Bezpečnostní správce:

- spolupracuje s bezpečnostní komisí a správcem IS Úřadu městské části,
- zodpovídá za dodržování bezpečnosti IS Úřadu městské části,
- zodpovídá za to, aby bezpečnostní politika byla součástí plánování v oblasti informatiky,
- navrhuje metody a postupy v oblasti bezpečnosti IS Úřadu městské části,
- navrhuje specifické role a odpovědnosti v oblasti bezpečnosti IS Úřadu městské části v rámci celého úřadu,
- navrhuje bezpečnostní opatření a plán jejich implementace,
- navrhuje hlavní kroky vedoucí ke zvýšení bezpečnosti dat a prostředků v IS Úřadu městské části,
- řídí zavádění bezpečnostních opatření podle definovaných bezpečnostních cílů,
- zajišťuje, aby dodavatelé služeb IT dodržovali bezpečnostní politiku úřadu a ostatní relevantní vnitřní předpisy,
- podílí se na zvyšování bezpečnostního uvědomění uživatelů IS Úřadu městské části,
- průběžně monitoruje bezpečnostní incidenty a účinnost bezpečnostní politiky a ověřuje funkčnost zavedených bezpečnostních opatření,
- Bezpečnostní správce IS spravuje seznam administrátorských hesel. Listinná kopie tohoto seznamu je uložena v obálce v trezoru. Obálka je zapečetěna orazítkováním a podpisy bezpečnostní správce IS tak, aby bylo jasně patrno, zda byla či nebyla otevřena. Obálka se otevírá jen v případě nouze, o jejím otevření se následně sepíše krátký protokol, kde je uvedeno datum, důvod a osoby, které obálku s hesly otevřeli. Po nastolení normálního stavu je stejným způsobem založena a uložena nová obálka s novými administrátorskými hesly.

7.3. Uživatelé IS Úřadu městské části

Uživatel IS je povinen:

- řídit se ustanoveními Provozního řádu - Základní pravidla pro uživatele IS Úřadu městské části Brno-střed,
- chránit data a prostředky IS Úřadu městské části,

- používat svěřenou výpočetní techniku pouze k výkonu svého povolání,
- zabezpečit svěřený počítač proti přístupu všech neoprávněných osob,
- při odchodu z pracoviště na delší dobu se odhlásit síťového režimu a ukončit spuštěné programy,
- nastavit si uživatelské heslo a nesdělovat je jiným osobám (v případě pochybností o bezpečnosti či vyzrazení /kompromitaci/ svého uživatelského přístupového hesla své přístupové heslo změnit),
- v případě odmítnutí přístupu k některému objektu IS Úřadu městské části (počítači, souboru, funkci atd.) oznámit tuto skutečnost svému nadřízenému vedoucímu, aby mu přístup byl umožněn,
- při práci v prostředí LAN a WAN sítí důsledně dodržovat předepsaná pravidla zpracování dat a bezpečnostní doporučení správců těchto systémů,
- dodržovat všechna opatření zmíněná v bezpečnostní politice,
- hlásit bezpečnostnímu správci jakýkoliv zjištěný incident v oblasti bezpečnosti IS Úřadu městské části,
- hlásit správci IS všechny poruchy funkčnosti prostředků IS,
- nakládat s osobními údaji a utajovanými skutečnostmi v souladu s platnou legislativou,
- musí dbát i na to, aby prostřednictvím informačních technologií úřadu nevznikla škoda jiným subjektům a nebylo poškozeno dobré jméno úřadu.

Uživateli IS je zakázáno zejména:

- využívat prostředky VT pro jiné než pracovní aktivity,
- jakýmkoliv způsobem měnit konfiguraci přiděleného počítače,
- instalovat jakýkoliv software,
- měnit nastavení používaných aplikací a antivirových programů,
- obcházet stávající prostředky zabezpečení IS Úřadu městské části,
- provádět technické zásahy do prostředků výpočetní techniky a ostatních zařízení s touto technikou souvisejících,
- vynášet jakákoliv záznamová média mimo prostory úřadu bez vědomí odboru informatiky,
- jakýmkoliv způsobem neoprávněně zveřejnit, zpřístupnit nebo odeslat data,
- umožnit přístup cizí osoby k IS Úřadu městské části.
- připojovat jakákoliv média k počítačům

Vedoucí jednotlivých odborů

- jsou odpovědni za dodržování bezpečnostních opatření v jimi řízených útvarech v souladu s bezpečnostní politikou a dalšími předpisy,
- zajišťují, aby podřízení zaměstnanci znali své povinnosti a odpovědnosti,

- zajišťují, aby podřízení zaměstnanci byli vyškoleni v oblasti jimi používaných systémů v potřebné míře.

Článek 8
Základní postupy řízení bezpečnosti a postupy pro dosažení bezpečnostních cílů

8.1. Identifikace možných hrozeb a následků

Na tomto místě jsou uvedeny možné hrozby, které mohou nepříznivě ovlivnit provoz IS Úřadu městské části. Úkolem bezpečnostní politiky je specifikace postupů, které tato rizika snižují na přijatelnou míru. Jsou to hrozby:

- přírodní nebo fyzické – živelná pohroma, požár, zaplavení povodní či vodou z vodovodního potrubí, přerušení dodávky elektrické energie;
- technické – poruchy hardware a sítě, nestandardní chování softwarových produktů, poškození nosiče dat, napadení virem;
- personální – zneužití identity uživatele neoprávněnou osobou, vyzrazení osobních nebo citlivých dat, neoprávněná modifikace dat;
- ostatní – krádež hardware nebo nosiče dat, průnik do IS zvenčí (hacking).

Realizace některých hrozeb může mít pro MČ Brno-střed různé následky. Jedná se především o:

- nedodržení legislativních předpisů a nařízení,
- omezení provozu úřadu,
- finanční ztrátu různého rozsahu,
- ztrátu důležitých dat.

8.2. Bezpečnostní postupy a opatření

Zajištění fyzické bezpečnosti

V rámci zamezení nedovoleného přístupu do prostor úřadu je v budově instalováno elektronické zabezpečovací zařízení. Čidla elektronického zabezpečovacího systému (EZS) budovy jsou umístěná na chodbách, vybraných kancelářích, oknech a vstupních dveřích. EZS je napojeno na pracoviště vrátnice v objektu. EZS se ovládá pomocí kódů, které jsou přiděleny pouze vybraným zaměstnancům úřadu. Pravidla pro práci se zabezpečovacím systémem definuje vnitřní směrnice úřadu. Nepřetržitou ochranu budovy zajišťuje vrátnice.

Běžné kanceláře - pracoviště s počítači uživatelů a periferiemi - jsou zajištěny uzamčením v době nepřítomnosti zaměstnanců Úřadu městské části.

Z důvodu zajištění fyzické bezpečnosti jsou některé prostory, ve kterých se nachází klíčové prostředky IS prohlášeny za neveřejné a vstup do nich je osobám povolen jen v doprovodu správce IS. Jde především o prostory, ve kterých se nalézají síťové servery a centrální aktivní prvky kabelových rozvodů. Tyto prostory jsou vybaveny klimatizací.

Do infrastruktury sítě jsou zabudovány takové síťové prvky, které dokáží zamezit neoprávněnému proniknutí do vnitřní sítě. Míra účinnosti závisí i na jejich umístění, vzájemném zapojení, optimální konfiguraci, nastavení. Tyto síťové prvky jsou umístěny v uzavřených, ale odvětrávaných (resp. chlazených), mechanicky odolných zamykatelných skříních (rack) nebo v zabezpečených místnostech.

V případě vedení kabeláže mimo prostory úřadu je tato vedena tak, aby byla dostatečně chráněna před vnějšími vlivy a byla dodržena všechna bezpečnostní opatření.

Síťové servery a centrální aktivní síťové prvky jsou připojovány do zvláštních elektrických obvodů, zálohovaných záložním zdrojem. Všechna tato zařízení musí být provozována v souladu s doporučením výrobce.

Síťové servery jsou vybaveny systémem nepřetržitého napájení elektrickým proudem (UPS) poskytujícím dostatečný časový prostor pro zastavení provozovaných aplikací a operačních systémů v případě výpadku dodávky elektrické energie.

O umístění počítačů, terminálů, tiskáren a jiných koncových zařízení rozhoduje správce IS Úřadu městské části tak, aby byla dodržena všechna doporučení výrobce zařízení a splněny požadavky na bezpečnost práce. Bez konzultace se správcem IS Úřadu městské části nelze zvolené umístění měnit.

Všechna výpočetní technika (až na výjimky dané charakterem výpočetní techniky) musí být používána pouze v prostorách úřadu. Výjimku tvoří např. notebooky, informační kiosky určené veřejnosti, speciálně instalovaná PC pro přístup veřejnosti, apod.

Reakce na přírodní či fyzické hrozby, jako požár, povodeň a další živelné pohromy

Obecně tuto problematiku řeší interní směrnice Úřadu městské části Brno-střed vydávané tajemníkem úřadu, krizové a evakuační plány atd. Nebezpečí je zaregistrováno buď bezpečnostním elektronickým zařízením, nebo díky lidskému faktoru a je ihned sděleno „krizovému štábu“ v čele se starostou. Ten pak řeší hrozbu globálně.

Vedoucí odboru informatiky je odpovědný za informační systém úřadu. Musí zajistit, aby v případě hrozby došlo k minimálnímu poškození IS.

Prioritním úkolem je záchrana serverů s daty, které je nutné vypnout a odvést mimo dosah nebezpečí.

Neméně důležitým krokem je záchrana paměťových médií s důležitými daty a důležité dokumentace.

Jako poslední a tedy „nejméně důležitým“ krokem je záchrana a odvoz ostatního hardware, kde nejsou uložena žádná data (monitory apod.)

Protipožární ochrana

Protipožární ochrana budovy je řešena pomocí organizačních směrnic Úřadu městské části Brno-střed a v souladu s platnými předpisy. Protipožární zabezpečením budovy: V budově jsou umístěna požární čidla a požární hlásiče. Budova je vybavena hasicími přístroji a požárními hydranty. V souladu s platnými předpisy jsou prováděny pravidelné revize hasicích přístrojů, požárních hydrantů, elektro zařízení i celé budovy. Úřad má zpracovanou a vede dokumentaci a zprávy PO a BOZP, provádí pravidelná školení požární ochrany PO a bezpečnosti a ochrany zdraví při práci BOZP, má pracovníka zajišťujícího PO.

Organizační a administrativní opatření, personální bezpečnost

Jsou jasně stanovena pravidla, kompetence a odpovědnosti v oblasti bezpečnosti IT a každý uživatel s nimi musí být seznámen. Jedná se o soubor interních směrnic a dokumentů obsahujících příslušná ustanovení se vztahem k IS Úřadu městské části spolu s odkazy na platné legislativní nařízení. Jsou to následující dokumenty:

Pracovní řád Úřadu městské části Brno-střed – závazná interní směrnice obsahující ustanovení o povinnosti zachovávat mlčenlivost o citlivých informacích a osobních údajích.

Provozní řád IS Úřadu městské části Brno-střed – popisuje a stanovuje základní všeobecná pravidla provozu IS, závazné pro všechny osoby s pracovním nebo obdobným poměrem.

Plán zálohování dat – stanovuje přesně formu a způsob provádění procesu zálohování dat. Definuje četnost, rozsah a způsob uchovávání archivních datových sad.

Havarijní plán – stanovuje způsob obnovy provozu IS Úřadu městské části, nebo jeho části po bezpečnostním incidentu (havárie, napadení, …).

Zachování důvěrnosti dat - v případě pracovních (funkčních) míst, kde se uživatel IS setkává nebo pracuje s daty, která obsahují osobní informace či jiné citlivé údaje, je nutné prověřit zaměstnance a do pracovní smlouvy zapracovat článek ošetřující zachování důvěrnosti. Postupuje se s respektováním zákona o ochraně osobních údajů případně i zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti resp. zákona o ochraně utajovaných skutečností.

Řízení přístupu do IS Úřadu městské části – uživatel má přístup pouze k takovému uživatelskému programovému vybavení, na které má nárok podle vykonávané funkce. O přístupu k uživatelskému programovému vybavení rozhoduje vedoucí příslušného odboru podle vykonávaných úkolů a funkce jednotlivých uživatelů. Identifikace a přístup uživatelů do IS je spravován centrálně. Bezpečnostní komise úroveň přístupu periodicky reviduje.

Po ukončení práce s programem (transakce) má uživatel povinnost se co nejdříve z programu odhlásit a jde-li o přístup pomocí tenkého klienta, tak uzavřít prohlížeč.

Stanovení odpovědnosti za platnost dat v IS Úřadu městské části – určení konkrétních osob, které jsou zodpovědné za udržování konkrétních dat v aktuálním platném stavu.

Provádění osvěty v oblasti bezpečnosti – základní pravidla bezpečného chování uživatele definuje Provozní řád - Základní pravidla pro uživatele IS Úřadu městské části Brno-střed. Všem uživatelům IS jsou při nástupu do zaměstnání jasně vysvětleny bezpečnostní požadavky, je provedeno poučení a vyškolení nového zaměstnance. Jsou vyškoleni v základních bezpečnostních opatřeních (zacházení s médii, antivirová ochrana, postup při vzniknuvší komplikací mající za následek ohrožení bezpečnosti apod.) Uživatelé jsou rovněž informováni o možných rizicích při zavádění nových agend a způsobů řešení jejich pracovních povinností.

Porušení bezpečnostní politiky – úřad musí definovat sankce pro zaměstnance, kteří poruší bezpečnostní politiku nebo bezpečnostní postupy a opatření definované úřadem.

Hlášení poruch a podezření na porušení bezpečnosti – každý uživatel je povinen nahlásit jakékoliv i jen podezření na porušení bezpečnosti IS Úřadu městské části bezpečnostnímu správci.

Dokumentace – veškeré incidenty mající za následek porušení bezpečnosti IS Úřadu městské části musí být zdokumentovány a záznamy uchovávány. Za dokumentaci odpovídá bezpečnostní správce. Jedná se například o provozní deníky, evidenci poruch apod.

Dostupnost kompetentních osob – v případě nepřítomnosti kompetentních osob (jako je bezpečnostní správce, správce IS, bezpečnostní komise, atd.) musí být k dispozici jejich zástupce, který v případě vzniklých komplikací bude schopen situaci řešit.

Použití informačních technologií / použití technických prostředků

Řízení přístupu – bezpečné nastavení přístupu k datům, dostatečná délka hesel, nastavení automatického odhlašování ze sítě po 120 minutách nečinnosti, zabezpečení prostředků výpočetní techniky (zejména povinnost odhlašování z IS, „ze sítě“) při odchodu z pracoviště, apod.

Pro autentizaci uživatele k IS Úřadu městské části je používáno jednoznačné uživatelské jméno a heslo, které je uživatel povinen držet v tajnosti. Metodika tvorby, používání hesla, zamykání účtu po neúspěšných pokusech o autentizaci je důležitou součástí Provozního řádu IS Úřadu městské části Brno-střed.

Důsledné používání administračních prostředků (modulů) provozovaných operačních systémů a softwarových produktů, pokud jsou jejich součástí.

Používání antivirových programů, jejich nastavení v maximální únosné míře (elektronická pošta, Internet, antivirová kontrola cizích médií,…) a pravidelná, lépe „okamžitá“, aktualizace. Aktuálnost antivirových programů a jejich virových bází je zajištěna formou automatické aktualizace na lokální server dálkovým přístupem přes Internet. Koncové stanice provádějí automatický update či upgrade proti lokálnímu serveru.

Používání prostředků k šifrování dat – slouží především pro ochranu přenášených dat při komunikaci prostřednictvím sítě Internet. Další uplatnění šifrování dat je na přenosných IT zařízeních jako notebooky PDA, iPody i USB flash disky a další, jako ochrana před neoprávněným získáním a možným zneužitím dat v případě ztráty či odcizení přenosného zařízení či nosiče dat.

Přístup na Internet je zabezpečen prostředky na ochranu před neautorizovaným přístupem do vnitřní sítě IS Úřadu městské části (firewall, proxi).

Maximální možné monitorování všech dostupných parametrů bezpečnosti IS Úřadu městské části, pokud možno co nejvíc zautomatizované – zaznamenávání provozu serverů, monitorování přístupů na Internet, fyzických přístupů do neveřejných prostor úřadu, kontrola komunikačních cest, evidence poruch.

Přenosná zařízení a bezpečnostní rizika – notebooky, mobilní telefony, PDA, iPody i („jen“) USB flash disky a další mobilní přenosná zařízení obsahují často citlivé informace. Jejich ztráta může vést k vysokým bezpečnostním či ekonomickým rizikům pro MČ Brno-střed, je nutné zabezpečení pomocí šifrování dat. Dále mobilní zařízení vystavují sítě potenciálním bezpečnostním hrozbám, jako je neoprávněný vstup do IS Úřadu městské části, nebezpečí zavlečení virů, trojských koní či jiného škodlivého SW. Zásady používání a bezpečnosti přenosných ICT zařízení a nosičů dat jsou nedílnou důležitou součástí Provozního řádu IS Úřadu městské části Brno-střed.

Článek 9
Závěr

Vzhledem k dříve realizovaným a průběžně dodržovaným a kontrolovaným opatřením a zavedeným bezpečnostním pravidlům dosahuje informační systém Úřadu městské části Brno-střed kvalitní bezpečnostní úrovně a odolnosti vůči v tomto dokumentu pojmenovaným hrozbám. Zde připomínáme: předstírání identity uživatele, zneužití softwaru neautorizovanými uživateli, selhání hardware, poškození paměťového média, selhání dodávky energie, krádež a škodlivý software.

Dále jsou ohrožena aktiva provozovaná na lokálních stanicích uživatelů, jež mohou být zničena poškozením hardwaru (nebo paměťového média), jsou-li opomíjena pravidla zálohování - např. na server.