STATUTÁRNÍ MĚSTO LIBEREC

Poznámka: *Zveřejněna je pouze upravená verze dokumentu z důvodu dodržení přiměřenosti rozsahu zveřejňovaných osobních údajů podle nařízení Evropského parlamentu a rady (EU) 2016/679 , 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 a aplikačních zákonů ČR).*
Nejsou dotčena práva podle § 16 odst. 2 písm. e) zákona č. 128/2000 Sb., o obcích (obecní zřízení) oprávněných osob uvedených v § 16 a § 17 téhož zákona.

20. schůze rady města dne: 19.11.2019

Bod pořadu jednání: 47

Strategie bezpečnosti IS MML na roky 2020 až 2022

Stručný obsah: Schválení strategie bezpečnosti IS MML na roky 2020 až 2022.

MML, Odbor informatiky a řízení procesů

Důvod předložení: Schválení strategie bezpečnosti IS MML

Zpracoval: Vavřina Zbyněk, Ing. - vedoucí odboru informatiky a řízení procesů

Projednáno s: Ing. Martinem Čechem, tajemníkem

Mgr. Jiřím Šolcem, náměstkem primátora pro technickou správu města a informační technologie

Ing. Jaroslavem Burešem, MBA, statutárním ředitelem Liberecká IS, a.s.

Předkládá: Vavřina Zbyněk, Ing. - vedoucí odboru informatiky a řízení procesů

K projednání v radě přizván(a):

Předpokládaná doba projednání (min): 5

Po schválení předložit na jednání:

Návrh usnesení

Rada města po projednání

schvaluje

strategii bezpečnosti IS MML na roky 2020 až 2022, dle přílohy č. 1.

ukládá

zajistit plnění schválené strategie IS MML.

P: Vavřina Zbyněk, Ing. - vedoucí odboru informatiky a řízení procesů
T: 31.01.2023

Důvodová zpráva

Východiska pro stanovení strategie

Zpracování strategie bezpečnosti IS MML je výsledkem pravidelné roční analýzy rizik, která probíhá v IS MML, a na jejímž základě jsou formulovány bezpečnostní cíle pro konkrétní rok a z nich vyplývající investice a zásahy. Poprvé však vzniknul dokument, který definuje cíle v oblasti bezpečnosti na delší období a který je předkládán radě města ke schválení. Hlavními důvody jsou:

a) Rostoucí důležitost bezpečnosti informačních systémů vyplývající z jejich nepostradatelnosti, rostoucí složitosti, rychlosti vývoje technologií, ale i rychlosti vývoje bezpečnostních útoků.

b) Významný vliv, který bezpečnost informačních technologií může mít na běžný život úřadu.

c) Závaznost bezpečnostních opatření pro všechny uživatele informačního systému MML.

Formulace strategie probíhala od dubna 2019 v bezpečnostní skupině tvořené osobami uvedenými v záhlaví této zprávy. Strategie shrnuje rizika vyhodnocená jako neakceptovatelná s nutností reakce. Definované hrozby byly podrobeny opětovné analýze rizik a z ní vyplývající priorite, respektive rozdělení do jednotlivých let.

Vznik této strategie neznamená, že IS MML je nechráněný, naopak je na současnou dobu chráněn velmi dobře, nicméně již zmíněná rychlost vývoje technologií, požadavků na bezpečnost IS a bezpečnostních útoků vyvolává potřebu vyššího stupně ochrany oproti současnému stavu v následujících letech.

Předkládaná strategie byla odsouhlasena také správní radou Liberecké IS a navazuje na Strategii rozvoje skupiny Liberecké IS pro roky 2020 - 2022.

Dále uvedený text je členěn na konkrétní bezpečnostní hrozby, odpovídající cíle, předpoklad doby realizace a předpokládané potřeby finančních zdrojů.

U jednotlivých cílů jsou uvedeny orientační ceny řešení, pokud by mělo být realizováno nákupem HW nebo SW. Tyto údaje jsou pouze informací o běžných cenách na trhu, aby bylo možno plánovat finanční zdroje. Skutečné ceny budou stanoveny výběrem vhodných produktů a dodavatelů, a pokud nedojde k zásadním zvratům na trhu, tak nebudou vyšší než uváděné orientační.

Strategie bezpečnosti IS MML na roky 2020 – 2022 – stručný přehled

1) Pokročilá ochrana před hrozbami z internetu

Cíl: Nahrazení stávajícího zařízení firewall s zařízením s pokročilými funkcemi ochrany pro zajištění datového provozu

Termín realizace: rok 2020

Očekávané výdaje na pořízení: 2500 tis. Kč

Očekávané roční náklady provozu: 1150 tis. Kč

2) Evidence a kontrola přístupů uživatelů k aplikacím a jejich oprávněním, Řešení DLP

Cíl 1: Vývoj a nasazení aplikace pro evidenci přístupových oprávnění

Termín realizace: rok 2020

Očekávané výdaje na pořízení: 100 tis. Kč

Očekávané roční náklady provozu: 20 tis. Kč

Cíl 2: Nasazení systému DLP („Data Loss Prevention“)

Termín realizace: rok 2022

Očekávané výdaje na pořízení: 200 tis. Kč

Očekávané roční náklady provozu: 330 tis. Kč

3) Řízení přístupu uživatelů a zařízení k „drátové“ síti

Cíl: Výměna aktivních prvků sítě za nové s tzv. technologií 802.1x. umožňující naprogramování systému pro zabezpečení (řízení a kontrolu) přístupu k síti,

Termín realizace: dokončení v roce 2022, postupně v letech 2020 a 2021

Očekávané výdaje na pořízení: celkem 4000 tis. Kč, postupně v letech 2020 a 2021

Očekávané roční náklady provozu: cílově 670 tis. Kč

4) Pokročilá antimalware ochrana stanic uživatelů a serverů

Cíl: Nasazení antimalware sytému s centrální správou, nastavitelnými politikami a cloudovými službami na stanice uživatelů a servery

Termín realizace: dokončení v roce 2022, postupně v letech 2020 a 2021

Očekávané výdaje na pořízení: 0

Očekávané roční náklady provozu: cílově 55 tis. Kč

5) Vyšší stupeň zabezpečení vzdálených přístupů do sítě přes VPN a VDI

Cíl: Nasazení řešení dvoufaktorové autentizace pro přihlášení k VPN a VDI

Termín realizace: rok 2020

Očekávané výdaje na pořízení: 0

Očekávané roční náklady provozu: 45 tis. Kč

6) Zvýšení fyzické bezpečnosti - hasicí zařízení

Cíl: Vybavení významného technologického uzlu – serverovny na nové radnici hasicím zařízením

Termín realizace: rok 2020

Očekávané výdaje na pořízení: 300 tis. Kč

Očekávané roční náklady provozu: 10 tis. Kč

7) Bezpečnost bezdrátových sítí na MML a přenositelných (mobilních) zařízení

Cíl: Nasazení Network Policy Server pro řízení přístupu k síti pomocí certifikátů zařízení.

Termín realizace: rok 2020

Očekávané výdaje na pořízení: 150 tis. Kč

Očekávané roční náklady provozu: 0

8) Monitoring a analýza chování sítě

Cíl 1: Specifikace požadovaného rozsahu monitorování sítě

Termín realizace: rok 2021

Očekávané výdaje na pořízení: 0

Očekávané roční náklady provozu: 0

Cíl 2: Nasazení produktu pro monitoring a analýzu chování sítě.
Termín realizace: rok 2022

Očekávané výdaje na pořízení: 1400 tis. Kč

Očekávané roční náklady provozu: 460 tis. Kč

9) Nasazení informačního systému pro evidenci požadavků bezpečnosti a GDPR

Cíl: Vlastními zdroji LIS dovyvinout systém centrální evidence obecných bezpečnostních prvků aplikací včetně bezpečnostních prvků pro zajištění ochrany osobních údajů fyzických osob.

Termín realizace: rok 2020

Očekávané výdaje na pořízení: 0

Očekávané roční náklady provozu: 0

10) Problematika bezpečnosti mobilních zařízení MP

Cíl: Nasazení Mobile Device Managementu (MDM) na mobilní telefony MP

Termín realizace: rok 2020

Očekávané výdaje na pořízení: 0

Očekávané roční náklady provozu: 100 tis. Kč

11) Zabezpečení ochrany mailbox email serveru

Cíl: Pořízení email security gateway s funkcemi antimalware, antispam

Termín realizace: rok 2020

Očekávané výdaje na pořízení: 150 ti. Kč

Očekávané roční náklady provozu: 50 tis. Kč

12) Nastavení striktních komunikačních pravidel mezi sítěmi

Cíl: Rekognoskace síťového chování jednotlivých aplikací, redefinice požadavků minimální potřebné povolené komunikace, vytvoření a nasazení nových pravidel na firewall

Termín realizace: rok 2021

Očekávané výdaje na pořízení: 300 tis. Kč

Očekávané roční náklady provozu: 0

13) Zajištění auditu logů

Cíl 1: Analýza rozsahu potřeb logování

Termín realizace: rok 2021

Očekávané výdaje na pořízení: 0

Očekávané roční náklady provozu: 0

Cíl 2: Nasazení systému centrálního sběru a vyhodnocování logování pro systémy a aplikace

Termín realizace: rok 2022

Očekávané výdaje na pořízení: 200 tis. Kč

Očekávané roční náklady provozu: 30 tis. Kč

14) Šifrování úložiště na úrovni databáze a komunikace mezi aplikací a databází

Cíl: Bez cíle - podmíněně akceptovatelné riziko do vyřešení bodu 17.

15) Bezpečnost hesel pro přístupy do systémů

Cíl: Stále prosazovat v IS MML vynucenou politiku bezpečnosti hesel dle doporučení, ověřit možnost uplatnění politiky u těch aplikací, kde to není autorem umožněno.

Termín realizace: rok 2021

Očekávané výdaje na pořízení: 0

Očekávané roční náklady provozu: 0

16) <u>Standardy pro nasazování nových aplikací</u>

Cíl: Vynutit v procesech MML standardy pro nasazování nových aplikací

Termín realizace: rok 2020

Očekávané výdaje na pořízení: 0

Očekávané roční náklady provozu: 0

17) <u>Velikost databází v IS MML</u>

Cíl: Vypracování dílčí strategie pro řešení databázového prostředí pro IS MML, implementace zvoleného řešení

Termín realizace: dokončení v roce 2022, postupně v letech 2020 a 2021

Očekávané výdaje na pořízení: celkem 2000 tis. Kč, postupně v letech 2021 a 2022

Očekávané roční náklady provozu: cílově 670 tis. Kč

18) <u>IP hlasové služby</u>

Cíl: Vypracování studie pro náhradu technologie VOIP pro MML, implementace zvoleného řešení

Termín realizace: dokončení v roce 2022, postupně v letech 2021 a 2022

Očekávané výdaje na pořízení: celkem 2500 tis. Kč v roce 2022

Očekávané roční náklady provozu: cílově 670 tis. Kč.

Úplný text Strategie bezpečnosti IS MML na roky 2020 – 2022 je v příloze č. 1 této důvodové zprávy. Dokument strategie bezpečnosti IS MML je dokumentem neveřejným, důvodem je podrobný popis zranitelností IS MML.

<u>Přílohy:</u> *materiál neobsahuje žádné přílohy.*