MĚSTSKÁ ČÁST PRAHA 5

Kyberbezpečnost

Praktické příklady pro ochranu před hrozbou útoku

Odborný seminář v rámci projektu

„Realizace SMART Česko v praxi obcí a měst“ (SMART ČESKO)

Nesuchyně 27.- 28.4.2023

Reg. č.: *CZ.03.4.74/0.0/0.0/15_025/0016927*

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- V pondělí 14.3.2022 ve večerních hodinách bylo detekováno správcem ICT úřadu nestandardní výkonové zatížení jednoho z poštovních serverů.
- V průběhu noční analýzy stavu a provádění bezpečnostních opatření byla zjištěna nedostupnost dvou serverů úřadu využívaných k testovacím účelům.
- U dvou poštovních serverů byla zjištěna ztráta mailové komunikace od 10:00 hodin ráno dne 14.3.2022.
- Pokračující diagnostikou bylo zjištěno, že se jedná o šifrovací útok.

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- V úterý 15.3.2022 v 7:30 byly na základě rozhodnutí vedoucího Odboru informatiky a manažera kybernetické bezpečnosti vypnuty síťové aktivní prvky – úřad přestal poskytovat služby.
- Všichni vedoucí odborů a členové zastupitelstva byli prostřednictvím nástrojů WhatsApp či SMS informováni o nastalé situaci a o zákazu zapnout či vypnout PC a služební notebooky.
- Protože při útoku byl využit nástroj BitLocker, nativní součást operačního systému MS Windows, tak uživatelé neměli „vůbec sahat na počítač“, aby se zamezilo další eskalaci problému.

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- Bezpečnostní incident byl nahlášen na:
  - Policii České republiky
  - NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost
  - ÚOOÚ – Úřad pro ochranu osobních údajů
  - Řediteli Odboru bezpečnosti Magistrátu hlavního města Prahy
- Na Policii ČR bylo starostkou Prahy 5 podáno trestní oznámení na neznámého pachatele.
- Byl sestaven expertní tým, složený z pracovníků úřadu, pracovníků outsourcingové společnosti a externích specialistů se zkušenostmi s touto problematikou.

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- Webový server Prahy 5 nebyl útokem dotčen, takže na něm byly sdělovány aktuální informace občanům.
- Telefonní ústředna úřadu nebyla v provozu, takže pro příchozí hovory byla operátorem nastavena omluvná informace s odkazem na web Prahy 5.
- Vedoucím odborů byly poskytnuty služební mobilní telefony a informace o kontaktech byly doplněny na web Prahy 5.
- Následně byly na webu uvedeny služby, které byl úřad i přes nepříznivou situaci schopen poskytovat.

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- Expertní tým zahájil svou činnost a každý člen byl za něco zodpovědný
  - Řízení obnovy systémů a koordinace rekonstrukčních prací
  - Kontrola komponent ICT infrastruktury (servery, zálohování, Firewally, …)
  - Zkopírování dat a serverů na zapůjčené datové úložiště
  - Kopírování a předání dat Policii ČR a NÚKIB
  - Kontrola stanic a serverů zapůjčeným nástrojem Bitdefender
  - Jednání s dodavateli provozovaných IS a koordinace jejich činností
  - Komunikace s vedením MČ, vedoucími odborů a tiskem
  - Projektové řízení – vedení jednání a dohled nad plněním úkolů
  - Nastavování bezpečnostních opatření a analýzy rizik
  - Ověřování možného zneužití identit a kontrola přístupů do registrů a bank
- Jednání se konaly i dvakrát denně.

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- Pro odstraňování následků incidentu byly zapůjčeny technologie
  - **Bitdefender** – pro kontrolu stanic a serverů na výskyt škodlivého kódu.
  - **Fidelis** - pro detekci a ochranu před další exfiltrací ICT prostředí.
- Pronajato bylo datové úložiště (na 3 měsíce).
- Zakoupeno bylo 100 licencí **Forticlient VPN** – pro dvoufaktorové ověřování uživatelů pro vzdálený přístup (členů ZMČ a VO).

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- **V průběhu řešení následků incidentu bylo potřeba zajistit:**
  - Přístup do IS Datové schránky
  - Výdej hotových OP a CD
  - Zaplatit včas DPH
  - Zapsat do matriky děti do tří dnů od jejich narození
  - Pravidelně poskytovat informaci občanům (web, sociální sítě, …)
  - Konání jednání Rady MČ byť s menším komfortem
  - Hodně asertivity a pochopení pro požadavky občanů

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- **Pro obnovu systémů** byl použit DRP – **Plánu obnovy po havárii**, který byl zpracován půl roku před incidentem
- Úřad neměl zpracován **Plán kontinuity činností**, popisující činnosti, které je potřeba zajistit při výpadku fungování úřadu
- Před vstupem uživatelů do obnoveného prostředí museli všichni podepsat velmi **striktní pravidla pro práci s ICT**
- **Byl zamezen přístup na Internet** a byly povolovány pouze nezbytné domény schvalované manažerem kybernetické bezpečnosti, uvedené na „whitelistu“
- Bylo nasazeno **dvoufaktorové ověřování** uživatelů, kteří přistupují vzdáleně, ale jen ze služebních notebooků

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- **A jak to vše dopadlo?**
  - Úřad 9 pracovních dnů neposkytoval služby v plném rozsahu
  - Nepřišli jsme o žádná data v na serverech, v databázích ani v zálohách
  - Došlo k zašifrován cca 40 PC, které se nepodařilo odšifrovat
  - Systémy a databáze byly obnoveny na původním, ale vyčištěném prostředí
  - Zakázal se vzdálený přístup k mailům přes OWA (Outlook Web Access)

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- Přestože vyčištěné původní prostředí se tváří, že je v pořádku, tak se v současné době staví čisté ICT prostředí tzv. „na zelené louce“.
- Bez souvislosti s tímto incidentem byl v únoru 2022 připraven podnět k realizaci projektu „**Zvýšení kybernetické bezpečnosti Úřadu městské části Praha 5 a právních subjektů zřizovaných a založených městkou částí**“, na nějž MČ Praha 5 podat žádost o dotaci z IROP 2021 – 2027 a čekáme na vydání právního aktu.

Informace o bezpečnostním incidentu na ÚMČ Praha 5

Co to přineslo?

- Díky tomuto incidentu si všichni zastupitelé MČ a zaměstnanci ÚMČ Praha 5 uvědomili, jak jsou takovéto situace nebezpečné a že je potřeba se při využívání ICT technologií chovat zodpovědně.
- Kybernetické bezpečnosti je věnována podstatně větší pozornost, nežli tomu bylo v minulosti.
- Je dbáno na vzdělávání uživatelů ICT ÚMČ Praha 5 v oblasti kybernetické bezpečnosti

Informace o bezpečnostním incidentu na ÚMČ Praha 5

Vytvořená vnitřní legislativa:

- Směrnice č. 1/2022 **Politika bezpečnosti informací** Úřadu městské části Praha 5.
- **Závazná pravidla práce s ICT** pro pracovníky ÚMČ a pro zastupitele MČ.
- Nařízení č. 7/2022 **Politika organizačních a technických opatření kybernetické bezpečnosti** ÚMČ Praha 5.
- **Základní povinnosti uživatele informačních a komunikačních systémů** MČ Praha 5 v oblasti informační bezpečnosti (jsou součástí vstupního vzdělávání).

Praktické příklady pro ochranu před hrozbou útoku

Vzdělávání a testování znalostí?

- **Jsou využívány bezplatné kurzy na vzdělávacím portálu NÚKIB - https://osveta.nukib.cz**

https://osveta.nukib.cz/dk-22-24

Praktické příklady pro ochranu před hrozbou útoku

Co minimálně zajistit dle zákona 181/2014 Sb. o kybernetické bezpečnosti:

- Zpracovat vnitřní bezpečnostní legislativu a minimum bezpečnostních opatření.
- Veškerá dokumentace musí existovat i v listinné formě.
- Mít definované služby, které je nezbytné i v krizových situacích zajistit (plnění zákonných povinností, … platby DPH, DS apod.).
- Mít popsanou a dokumentovanou informační a komunikační infrastrukturu.
- Mít vytvořenou komunikační matici kontaktů na servisní organizace, techniky, externí správce apod.

Praktické příklady pro ochranu před hrozbou útoku

Jaké technické činnosti je potřeba pravidelně zajistit:

- Řádné fungování antivirových programů.
- Instalovat opravné záplaty operačních systémů PC a serverů.
- Instalovat upgrady provozovaných IS.
- Vyhodnocovat hlášení (logy).
- Provádět pravidelné zálohy dat do jiné geograficky a infrastrukturně oddělené lokality.
- Rozdělit (segmentovat) datovou síť.

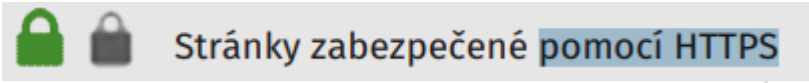
Praktické příklady pro ochranu před hrozbou útoku

Jak řešit bezpečnost s uživateli:

- Vytvořit bezpečnostní desatero a prokazatelně s ním seznámit všechny zaměstnance a použít jej i jako vstupní školení pro nové zaměstnance.
- Pravidelně školit pracovníky na problematiku kybernetické bezpečnosti.
- Provádět penetrační testy (minimálně 1x ročně).
- Reagovat na bezpečnostní informace NÚKIB (ať už ve spolupráci s odbornou firmou či vlastními silami).

Praktické příklady pro ochranu před hrozbou útoku

Desatero kybernetické bezpečnosti

1. Omezit přístup dalším osobám k pracovnímu zařízení
2. Chránit data pro případ odcizení či ztráty zařízení silným heslem
3. Hesla obsahující minimálně 12 znaků se mění po 3 měsících
4. Nepsat a neukládat hesla v blízkosti zařízení či pracovního stolu
5. Zajistit aby nikdo neodezřel vkládané heslo
6. Zamknout zařízení pokaždé, když od něj odcházím
7. Na webu preferovat zabezpečené stránky 

8. Nezveřejňovat své a svých blízkých osobní a citlivé informace
9. Vždy se zamyslet před otevřením mailu a přílohy
10. Nikdy s nikým nesdílet svá přihlašovací hesla a PIN

Praktické příklady pro ochranu před hrozbou útoku

Převzato z časopisu
Veřejná správa č.1/2023

Praktické příklady pro ochranu před hrozbou útoku

Jak řešit bezpečnost s uživateli:

1. **Být připraven = mít plán včetně komunikační matice**
2. **Mít vytisknutou a uloženou potřebnou dokumentaci**
3. **Mít připraven tým a jejich role**
4. **Tvořit průběžnou dokumentaci a přistupovat k řešení incidentu jako k projektu**

Praktické příklady pro ochranu před hrozbou útoku

Děkuji za pozornost

Ing. Pavel Rous
Městský část Praha 5
Referent kvality a eGovernmentu
a
Starosta obce Žilina

Tel: 606 770 173, mail pavel.rous21@gmail.com