MĚSTSKÁ ČÁST PRAHA 5

Zkušenosti z pohledu tajemnice ÚMČ Praha 5 týkající se bezpečnostního incidentu

14. - 15.6.2022 Olomouc

MODERNÍ VEŘEJNÁ SPRÁVA

Ministerstvo vnitra České republiky

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- V pondělí 14.3.2022 ve večerních hodinách bylo detekováno nestandardní výkonové zatížení jednoho z poštovních serverů a byla zjištěna ztráta mailové komunikace.
- Pokračující diagnostikou bylo zjištěno, že se jedná o šifrovací útok na servery úřadu.
- Byly zahájeny práce na serverech pro zastavení útoku. Servery byly odpojeny od sítě úřadu.

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, který koordinoval procesy se zpravodajskými službami
  - **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 vzhledem k vypnutí sítě 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
  - Kontrola stanic a serverů nástrojem Bitdefender
  - Kopírování a předání dat Policii ČR a NÚKIB
  - 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 konala i dvakrát denně a vše bylo pečlivě dokumentováno.

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
- Pro vzdálený přístup administrátorů a uživatelů nastaven **Forticlient VPN.** K němu zakoupeno 100 licencí **FortiToken** pro dvoufaktorové ověřování uživatelů (členů ZMČ a VO).
- Nyní se bude řešit nákup technologií **Bitdefender** a **Fidelis** dalších licencí **FortiToken**.

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- **Co jsme se naučili** ???
- Kromě DRP – **Plánu obnovy po havárii**, je potřeba mít zpracován i **Plán kontinuity činností**, pro zajištění činností při výpadku fungování úřadu
  - 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
  - Mít hodně asertivity a pochopení pro občany
- Dokumentaci je potřeba mít uloženu i v tištěné podobě!

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- Úřad má zřízeny pozice
  - Manažer kybernetické bezpečnosti
  - Architekt kybernetické bezpečnosti
  - Architekt e-governmentu
- V oblasti kybernetické bezpečnosti má úřad zpracovanou vnitřní legislativu zahrnující
  - Politiku bezpečnosti informací
  - Politiky organizačních opatření

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 na serverech, v databázích, v elektronické poště, ani v zálohách
  - Došlo k zašifrován cca 40 PC, které se ještě nepodařilo dešifrovat
  - Systémy a databáze byly obnoveny na původním, ale vyčištěném prostředí
  - Byl zakázán vzdálený přístup k mailům přes OWA (Outlook Web Access)
  - Přístup na internet se řídí cíleně dle potřeb uživatelů
  - Bylo nasazeno dvoufaktorové ověřování uživatelů při vzdáleném přístupu, ale jen ze služebních notebooků
  - Po obnově provozu všichni uživatelé podepsali striktní pravidla pro práci s ICT

Informace o bezpečnostním incidentu na ÚMČ Praha 5

- Přestože vyčištěné původní prostředí se tváří, že je v pořádku, i tak se připravujeme ICT infrastrukturu postavit nově 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 chce MČ Praha 5 podat žádost o dotaci z IROP 2021 – 2027.
- Díky tomuto incidentu si všichni zastupitelé MČ a pracovníci ÚMČ Praha 5 uvědomili, jak jsou takovéto situace nebezpečné a že je potřeba se při využívání ICT technologií chovat zodpovědně.

Informace o bezpečnostním incidentu na ÚMČ Praha 5

Poděkování za zvládnutí této nepříjemné situace patří jednak celému expertnímu týmu, ale i vedení MČ Praha 5 a všem pracovníkům, za jejich trpělivost a pochopení.

Děkuji za pozornost

JUDr. Kateřina Černá

tajemnice ÚMČ Praha 5