Tak nás zašifrovali...

Tomáš Hilmar
Vedoucí odboru informatiky MČ Praha 3

Praha

Co se stalo?

→ Došlo ke kompletnímu zašifrování serverové infrastruktury na bázi MS Windows, NAS úložišť a primárního zálohovacího serveru včetně úložiště záloh.

→ Částečně zašifrováno síťové úložiště s uživatelskými profily

→ Funkce AD a DB MS Exchange útok „přežily”

→ Servery na bázi OS Linux nepostiženy, management infrastruktury (virtual appliance) také

Jak?

→ Podceněním zachyceného předchozího útoku, kdy nedošlo k odhalení veškerých následků

→ Útočník získal na jednom stroji kontrolu nad účtem local system, následně pomocí lokálních politik zajistil spuštění scriptů vedoucích k získání hesla administrátorského účtu

→ Neúspěšný pokus o spuštění ransomware, prostřednictvím VSS zastavení rezidentního štítu antiviru

→ Spuštění souboru s ransomware = zahájení šifrování obsahu disků (pondělí 3:00 – 6:00)

→ Odstranění veškerých system restore point z OS

Co s tím?

→ Odstavení informačního systému, zabránění dalšímu šíření
→ Zjištění příčiny a rozsahu škody
→ Informace (nejen) uživatelům
→ Stanovení plánu obnovy, konzultace s NÚKIB a NAKIT
→ Zajištění nezbytných zdrojů pro obnovu
→ Zahájení obnovy

Obnova

→ Migrace funkcí AD do nového prostředí, vynucení změny hesel
→ Obnovení infrastruktury ze sekundárních záloh v odděleného prostoru
→ Export dat z jednotlivých systémů, čistá instalace v novém prostředí, import dat
→ Implementace nových bezpečnostních opatření
→ Čistá instalace veškerých uživatelských stanic, povolení přístupu k síťovým službám
→ Vyřešení problematiky integračních vazeb
→ Ověření produktivního provozu

Změny

→ Implementace dalších bezpečnostních opatření přijmutích vedením na základě doporučení NÚKIB a NAKIT např.:
  → Implementace technologií O365 E5
  → Zavedení MFA
  → Migrace MS Exchange, Sharepoint aj. do prostředí O365
  → Kompletní redesign pravidel na firewallu
  → Revize GPO
  → Změny ve způsobu ukládání záloh, pořízení fyzického hw pro zpracování záloh
  → aj.

Děkuji za pozornost

Praha