Kybernetický útok na FN Brno 12.-13.3.2020

Téma zpracoval: Petr Čačík, CI Oddělení systémů FN Brno

Popis instituce

- druhá největší nemocnice v republice (1889 lůžek, obložnost 54%, průměr 65%)
- spádovost pro více jak 1 mil. obyvatel
- rozkládá se ve třech geograficky oddělených areálech
- cca 6 000 zaměstnanců (v COVID cca 8000 uživatelských účtů),
- IT oddělení 70 zaměstnanců (včetně administrativy a spojovatelek z TU

Technologické zázemí

- dvě geograficky oddělená datová centra
- 24 fyzických serverů - *12 pro virtuální desktopy a 12 pro virtuální servery*
- provozováno přes 350 virtuálních serverů
- 4 datová úložiště pro systémy a data, PACS archiv 2 datová úložiště
- 23 informačních systémů základní služby identifikovaných dle ZKB

Koncová zařízení

- 2500 PC
- 1200 virtuálních desktopů
- 10 routerů, 300 switchů a 750 wifi AP
- cca 8000 přidělených IP adres
- cca 600 individuálně síťově propojených modalit a přístrojů (ZP)

Instituce v době útoku

- **Střídání vrcholového managementu**
  - *organizační změny, rozvojové IT projekty pozastaveny,..*
- **Dlouhodobé škrty nebo odklad investic do ICT včetně kybernetické bezpečnosti**
  - *počítáno s modernizacemi z IROP prostředků (V10)*
- **Nedostatečný výkon datových center utáhnout v odpovídající kvalitě provoz**
  - *latence systémů, drobné výpadky, snižování bezpečnosti*
- **Nasazeny všechny bezpečnostní prvky dle aktuálních licencí a možností ICT**
- *antivir, firewall, vzdálené přístupy, segmentace sítě*
  - *vyšší bezpečnosti bylo ustoupeno pro udržení výkonu provozních systémů (antivir na serverech pouze v provedení agentless)*
- **Datová síť segmetována do VLAN**
  - *z důvodu velkého provozu na stávající síťové prvky nešlo nasadit ACL*
- **První vlna COVID 19**
  - *příprava nových provozů a úprava stávajících*
  - *minimum zaměstnanců i pacientům, omezení provozu většiny nemocnice. Obložnost lůžek stažena na cca 40%)*

Zaznamenání útoku

- Útok začal 12.3.2020 po 22:00 hod
- Nahlášeno uživateli na podporu IT 13.3.2020 v 1:00 hod - nejede prohlížeč obrazové dokumentace
- 2:00-3:00 potvrzeno napadení aplikačních serverů prohlížeče obrazové dokumentace
- 3:00 – 5:00 administrátoři provedly kontrolu provozních serverů pro vyhodnocení stávající situace a zřejmý rozsah škod, předběžné informace předány zastupujícímu náměstkovi (zajistil kontaktování vedení nemocnice, PČR, NÚKIB)
- 5:00 – 7:00 tlumení provozu koncových stanic a kritických pracovišť, vypínání kritických systémů a shazování datové sítě
- Od 7:00 rozhodování o dalších krocích převzal NÚKIB.

Pozn: Čas je relativní ☺

Rozsah škod

- **Napadeny Windows aplikační servery**

Ø *nutná nová instalace provozních systémů bez využití záloh*

- **Zakryptován VIS SharePoint Online**

Ø *instituce přišla o 6 let vývoje aplikací podporující informovanost a pracovní workflow*

- **Zakryptování připravovaných systémů**

Ø *včetně dat, kde ještě nebyla nastavena politika zálohování*

- **Zakryptovány některé nestandardně provozované a nezabezpečené systémy a úložiště ve správě dodavatelů**

➢ primárně zálohy z přístrojů

Útok nezpůsobil

Ztrátu pacientských dat a databází primárních systémů (KIS, PACS, TIS, LIS, ERP,…) díky preciznímu zabezpečení záloh.

Doporučení NÚKIB

- **Okamžitě odpojit instituci od internetu**

- **Odstavit datovou síť beze zbytku**
  - *prověřit veškerou infrastrukturu*

- **Odstavit koncové stanice**
  - *prověřit na vzorcích stanic kam se útočník dostal*

- **Odstavit veškeré servery a úložiště**
  - *zpracovat seznam všech serverů a plán jejich kontroly*

- **Připravit za úseky IT plán obnovy jednotlivých technologií**
  - *datová centra, pořadí kritických provozů, rozdělit efektivně kolektiv a úkoly na ně kladené*
  - *pro obnovu produkční systémů nepoužívat zálohy (možnost dlouhodobé infekce)*
  - *doporučena reinstalace všech koncových stanic*

Náprava

- **14 dnů** - infrastruktura a datová centra
- **1-3 měsíce** - obnova primárních systémů (dalších několik měsíců obnova IS bez podpory nebo servisního zajištění)
- **1-2 měsíce** - obnova koncových stanic (výměna cca 2500 HDD, konfigurace OS a specializovaných aplikací)
- **Pro udržení provozu laboratoří**, bylo nutné provést prioritní kontrolu a izolovat jejich datovou síť (VLAN) od zbytku provozu.
- **Radiodiagnostika** - nutné připravit a zprovoznit záložní řešení pro prohlížení obrazových dat (PACS byl zařazen až za KIS)
- Prioritně uváděny do provozu systémy na LINUX distribuci (KIS, TIS, PACS archiv a záložní prohlížeč)
- Provozní systémy na OS Windows Server řešeny čistou reinstalací s nasazením nejnovějších verzí klientů.

Náprava

Operativně se FN Brno podařilo získat z havarijních zdrojů:

- core switche pro lepší segmentaci datové sítě a nasazení ACL
- přechod do Cloudu Microsoft - Windows 10 Enterprise, Serverové licence User Cal, Office 365,…

S odstupem + 1rok se teprve podařilo:

- hraniční firewall
- připojení na SOC (24/7 dohled síťového provozu)
- antivirová ochrana koncových stanic (v řešení)

Postřehy

- Úvodní týdny zájem ze strany uživatelů (upadalo postupně s nabíhajícími systémy)
- Nemocnice neměla vytvořen krizový plán pro obnovu ICT ve smyslu priorit uvádění jednotlivých systémů do provozu

➢ *nutné z důvodu rozložení lidských zdrojů, v průběhu obnovy byly měněny priority*

➢ *nebyly krizové havarijní plány v tištěné podobě*

➢ *při obnově pomohla dlouhodobá znalost prostředí IT pracovníků*

- První vlna COVID a lockdown pomohl při obnově provozu

➢ *minimum lidí v zaměstnání, minimum pacientů a prováděných výkonů*

- Krizový štáb FN se primárně zajímal o COVID, obnova ICT plně v rukou IT oddělení
- Do obnovy se zapojila drtivá většina IT zaměstnanců nad rámec běžné pracovní doby
- Různý přístup dodavatelů a nutné jednání s nimi, aby pomoc nebyla kontraproduktivní
- Mnoho firem nabízelo pomoc - nutno filtrovat co je kalkul a co je přínos
- Poradci, kteří na určitou dobu zpomalili tempo uvedení ICT do provozu

➢ *opakované vysvětlování naplánovaných úkolů vedoucích k obnově provozu*

Postřehy

- Zdroje - nedostatečný výkon a zastarání stávající technologie opět omezoval nastavení bezpečnosti best practice (nutné dělat kompromisy)
- Po náběhu základních systémů, bylo již nutné řešit i standardní agendu.
- Enormní zápřah kolegů z datových sítí
  - *minimum lidí se znalostmi a možnostmi pomoci*
- Centralizace ICT řešení, začleněných v doméně poskytla útočníkovi výhodu rychle se šířit
- S obnovou provozu všech systémů práce nekončí
  - *náprava je řešena do dnes, i když není mezi uživateli vidět.*
- Několik útvarů napadlo, že by nám mohli dát najíst (závodní jídelna uzavřena, tak jako hospody v okolí) :)
- Zaměstnanci nemocnice stále vnímají kybernetické hrozby jako problém IT a ne i jako svou vlastní odpovědnost

Umíme se bránit kybernetickým útokům

- **Neumíme**

➢ Můžeme klást pouze složitější překážky útočníkům do cesty.

- **Můžeme se maximálně připravit**

➢ Velmi záleží na funkčnosti organizace a jeho koordinaci během a po útoku
➢ Znalost prostředí a provázání na krizový tým
➢ Bodově v papírové podobě mít veden plán obnovy ICT (záleží kterou část měsíce útok na organizaci přijde - změny priorit)
➢ Nutno přijmout zodpovědnost všemi zaměstnanci
➢ Edukace a testování zaměstnanců v oblasti kybernetických hrozeb
➢ Důležité je umět co nejdříve zamezit přístup z internetu a omezit provoz LAN
➢ Zajistit offline zálohu dat
➢ Zvyšování kvalifikace IT správců

Poděkování

- ***NÚKIB*** *- nastavil pravidla, doporučil postup obnovy, edukoval vedení nemocnice, pomohl s kontrolou serverů..*
- ***Dodavatelé -*** *všem kteří automaticky a naprosto profesionálně přistoupili na požadavky a termíny s pomocí, které od nás byly vzneseny*
- ***Zaměstnanci*** *- všichni co přiložili ruku k dílu a vzpomněli si na nás*
- ***A hlavně všem zaměstnancům na IT oddělení FN Brno, kteří nad rámec svých povinností několik měsíců vydrželi v enormním zápřahu a pomohli s nápravou.***

Děkuji za pozornost.