Zkušenosti z kybernetických útoků na sektor zdravotnictví

e-government 20:10

Adam Kučínský

Národní úřad pro kybernetickou a informační bezpečnost
Odbor regulace

9. září. 2020

Vybrané činnosti NÚKIB v souvislosti s útoky na nemocnice

- 11.12. 2019 – Incident v nemocnici v Benešově
- 12. 3. 2020 – Incident ve FN Brno
- 17. 3. 2020 – Vydáno reaktivní opatření (RO) pro nemocnice
- 18. 3. 2020 – vydána metodika k RO
- 18. 3. 2020 – vydáno a rozesláno doporučení pro poskytovatele zdravotních služeb vč. metodiky
- 27. 3. 2020 - Nabídka služeb nemocnicím – e-learning, sken zranitelností, Turris Mox (ve spolupráci s CZ.NIC)
- 16. 4. 2020 – Varování
- 17. 4. 2020 – Doporučení k varování

Průběžně:

- **Řešení větších či menších incidentů a událostí – konzultace, výměna informací, pomoc s vyšetřováním**

Incident v nemocnici Benešov

- 11. 12. 2019 – Nemocnice v Benešově
- Co se stalo: Emotet-Trickbot-Ryuk - zašifrování dat
- Dopad: Výrazné omezení provozu nemocnice
- Finanční dopad: 40-50 milionů Kč
- Doba trvání narušení: Nemocnice obnovila provoz koncem prosince 2019, proces obnovy infrastruktury pokračoval dále i v lednu 2020

Incident ve FN Brno

- 12. 3. 2020 – FN Brno
- Co se stalo: Kolem 01:00 AM útočník získal práva doménového admina a začal šířit ransomware, IT odd. situaci zachytilo a začalo odpojovat systémy
- Dopad: Odložení plávaných úkonů, nemožnost ukládat data, celkové výrazné omezení všech činností
- Finanční dopad: odhadem řádově stovky milionů
- Některé části nemocnice byly více jak týden po útoku stále odstaveny

Události z našeho pohledu – průběh incidentu

- Hlášení incidentu/Zpráva v médiích
- Snaha kontaktovat napadenou organizaci
- Zjištění základního přehledu o situaci
- Rozhodnutí o pomoci a vyslání response týmu
- Vyslán response tým
  - Analyzuje
  - Doporučuje
  - Navrhuje opatření
- Zajištění stop, indikátorů kompromitace a jejich vyhodnocení
- Rozhodnutí o případném dalším postupu – sdílení informací o incidentu, vydání opatření, upozornění ostatních apod.

Činnost NÚKIB v zasažené organizaci

- Analýza stavu
- Určení časového i věcného rozsahu kompromitace systémů
- Návrh **možných** postupů při procesu obnovy dat
- Výpomoc při odstraňování a analýze škodlivého kódu
- Doporučení pro zabezpečení systémů a sítě

- **NÚKIB nemůže suplovat správce či dodavatele systémů!**

Dopady podobných incidentů

- ICT dopady
  - Kompletní ovládnutí systému
  - Krádež důležitých dat
  - Záměna dat
  - Znepřístupnění dat
  - Napadnutí HW zdravotnických zařízení

- Reálné dopady
  - Organizace přestává fungovat
  - Fyzické škody na majetku a zdraví
  - Ohrožení života a zdraví
  - Reputační dopady
  - Finanční dopady

Nejčastější cesty útočníka

- Phisingový e-mail
- Veřejně dostupné služby z internetu
  - Remote desktop protocol (RDP)
  - Secure Shell (SSH)
  - Webový e-mailový klient
  - Informační systémy
- Neautorizovaný přístup k vnitřní síti
  - Špatně zabezpečené Wifi
  - Ethernet přípojky
- Osobní zařízení, notebooky

Základní bezpečnostní pravidla
co bylo/je špatně

- Technické nedostatky
  - Nedostatečná segmentace sítě
  - Nejsou řešeny a vyhodnocovány zranitelnosti, nedochází k aktualizacím systémů
  - Nedostatečně řešené zálohování
  - Vystavování služeb do internetu bez řádného důvodu
  - Ignorace „best practices“
- Manažerské nedostatky
  - Pravidlo minimálního nutného přístupu
  - Provoz šéfuje bezpečnosti
  - Management nejde příkladem
  - Ignorace „best practices“
- Školení uživatelů
  - Uživatelé bez proškolení jsou bezpečnostní hrozbou
- Monitoring
  - Nedochází k analýze provozu – nedostatečný síťový monitoring

Vybrané činnosti NÚKIB v souvislosti s útoky na nemocnice

- 11.12. 2019 – Incident v nemocnici v Benešově
- 12. 3. 2020 – Incident ve FN Brno
- 17. 3. 2020 – Vydáno reaktivní opatření (RO) pro nemocnice
- 18. 3. 2020 – vydána metodika k RO
- 18. 3. 2020 – vydáno a rozesláno doporučení pro poskytovatele zdravotních služeb vč. metodiky
- 27. 3. 2020 - Nabídka služeb nemocnicím – e-learning, sken zranitelností, Turris Mox (ve spolupráci s CZ.NIC)
- 16. 4. 2020 – Varování
- 17. 4. 2020 – Doporučení k varování

Průběžně:

- **Řešení větších či menších incidentů a událostí – konzultace, výměna informací, pomoc s vyšetřováním**

Reaktivní opatření pro nemocnice a metodika I.

- 17. 3. 2020 – Vydáno reaktivní opatření (RO) pro nemocnice
- Postup podle § 13 odst. 1 zákona č. 181/2014 Sb.
- Závazné pro adrésáty - nemocnice pod ZKB
- **Důvod vydání**: Na základě proběhnuvšího incidentu
- **Cíl**: Minimalizace rizika vzniku podobných incidentů – zabezpečení systémů před incidentem
- **Náplň**: Provést 4 sady úkonů, celkem 20 konkrétních opatření
- **Legitimizace neprovedení úkonu**: Pokud by provedení úkonu způsobilo větší dopad než incident samotný
- K RO byla vydána metodika, která jej konkretizovala, uváděla cíle jednotlivých úkonů a doporučení k provedení

Reaktivní opatření pro nemocnice a metodika II.

- 1. sada úkonů – provést bezodkladně
  - Zamezit propojování systémů navzájem mimo nezbytné případy
  - Zamezit komunikaci do internetu vyjma nezbytných případů
  - Vyčlenit síť lékařských přístrojů od zbytku sítě
  - Změnit hesla privilegovaných účtů
  - Nahlásit Úřadu aktuální IP rozsahy
  - **Subjekty provedly částečně či zcela všechna opatření**
- 2. sada úkonů – provést do dvou dnů
  - Přesun záloh do off-line, zkontrolovat funkčnost záloh
  - Prověřit BCM plány a přesunout je mimo systémy
  - Nemazat data o KBI, prověřit zaslané indikátory kompromitace
  - Upozornit zaměstnance o riziku phishingu
  - **4 subjekty jedno nebo více opatření neprovedly**

Reaktivní opatření pro nemocnice a metodika III.

- 3. sada úkonů – provést do týdne
  - Ověřit, že zálohy jsou odděleny tak, aby je ani privileg. admin nemohl smazat
  - Zakázat použití nepodepsaných maker, pokud je to možné
  - Zkontrolovat segmentaci sítě a řízení mezi segmenty
  - Zpřísnit bezpečnostní politiky koncových stanic (zákaz spouštění neschválených aplikací, nepodepsaných PowerShell, ...)
  - Pokud není BCM – zpracovat alespoň pro klíčové systémy
  - Zajistit sken zranitelností – k realizaci možno využít Úřad
  - **4 subjekty jedno z opatření neprovedly**
- 4. sada úkonů – provést do 2 týdnů
  - Nasadit antiviry na všechna relevantní zařízení
  - Zvážit aktualizaci, otestovat, nasadit
  - **Subjekty provedly částečně či zcela všechna opatření**

Doporučení pro poskytovatele zdravotních služeb vč. metodiky

- 18. 3. 2020 – vydáno a rozesláno doporučení pro poskytovatele zdravotních služeb vč. metodiky
- Velmi podobné RO
  - vypuštěny některé body
  - nezávazné
- Rozesláno na 85 zdravotnických zařízení, které byly označeny ze strany MZD jako „páteřní“

Nabídka služeb nemocnicím

- 27. 3. 2020 - Nabídka služeb nemocnicím

1. Sdružení CZ.NIC nabídlo nemocnicím pod ZKB bezplatně routery TURRIS MOX vč. zaškolení a asistence – umožnění splnění segmentace sítě z RO
   - Využila jen jedna nemocnice (konkrétně žádost o 1 ks) z 16 oslovených
2. NÚKIB nabídl monitoring zranitelností
   - Využilo cca 40 z 200 oslovených
3. NÚKIB nabídl školení uživatelů pomocí e-learnigu – s možností zajištění „na klíč“ nebo k nasazení na vlastní infrastruktuře
   - Nevyužila žádná nemocnice z 16 oslovených

Varování ze dne 16. 4. 2020 a doporučení k němu

- 16. 4. 2020 – Varování
- 17. 4. 2020 – Doporučení k varování
- Varování před hrozbou spočívající v realizaci **rozsáhlé kampaně závažných kybernetických útoků** na informační a komunikační systémy v České republice, zejména pak na systémy zdravotnických zařízení
- Obsahovalo doporučení
  - Varovat uživatele před spear phisingem
  - Zabránit spouštění maker
  - Zablokovat zbytné přístupy z vnějšku
  - Offline zálohy vč. kontroly funkčnosti
- K tomu vydáno další doporučení s dalšími opatřeními

Co z toho plyne?

- Ukázalo se, že:
  - Narušení informačních systémů nemocnic na reálné dopady
    - Není to o tom, že doktoři operují/léčí a nepotřebují IT
  - Některé nemocnice pod ZKB nemají zavedena některá opaření podle ZKB
    - To vyplývá z reportů o RO
  - Nemocnic pod ZKB je málo
    - V ČR cca 250 zdravotnických zařízení – pod ZKB je 16
  - Lidí, kteří v nemocnicích dělají bezpečnost je málo
    - Obecně je oblast mimo zájem managementu
  - NÚKIB nemá efektivní komunikační nástroj směrem k nemocnicím
    - Nemáme kontakty na jiné subjekty, než na ty pod ZKB
  - Nemocnice nemají zájem/čas to řešit?
    - Nabídky na elearnig, turrisy, pentesty, monitoring hrozeb nebyly moc využity

Co s tím?

- Koordinace a standardizace v KB pro nemocnice:
  - Vzhledem k diverzitě systémů je téměř nemožné centrálně nastavit účinné řešení a mít je okamžitě, jde o dlouhodobý proces
  - Standard musí být obecný – v tuto chvíli na něm pracujeme - doporučení
- NÚKIB je „dimenzován“ na povinné osoby
  - Nelze ze strany NÚKIB okamžitě začít řešit všechny nemocnice
  - V případě více současně probíhajících útoků nastane problém s kapacitami
  - NÚKIB ani nemůže sám zabezpečení nemocnic vyřešit – může jej koordinovat, ale realizaci musí zajistit nemocnice samotné
  - V případě více útoků současně se bude prioritizovat
- Oborový CERT pro zdravotnictví
  - Měl by existovat?
  - Kde by měl být zařazen?
- Chce se to vůbec řešit?

Co aktuálně můžeme nabídnout?

- Všechny vzdělávací materiály najdete na stránkách
  - https://nukib.cz/cs/vzdelavani/
- Informace o hrozbách
  - https://nukib.cz/cs/infoservis/hrozby/
- Bezpečnostní doporučení NÚKIB pro administrátory 4.0
  - https://www.nukib.cz/download/vzdelavani/doporuceni/Admin4CB.pdf
- Scan zranitelností pro nemocnice
  - Žádost na e-mail: nckb@nukib.cz
  - Předmět „Žádost o **scan** zranitelností *nemocniceXY*“
  - V odpovědi na e-mail dostanete informace o dalším postupu
- Monitoring zranitelnosti
  - Žádost na e-mail: nckb@nukib.cz
  - Předmět „Žádost o **monitoring** zranitelností *nemocniceXY*“
  - V odpovědi na e-mail dostanete informace o dalším postupu
- E-learning
  - Žádost na e-mail: nckb@nukib.cz
  - Předmět „Žádost o **e-learning -** *nemocniceXY*“
  - V odpovědi na e-mail dostanete informace o dalším postupu

Co aktuálně můžeme nabídnout?

- Podpůrné materiály k implementaci ZKB a vyhlášek zde.
  - https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/
- Minimální bezpečnostní standard
  - Cílem je nastavit elementární požadavky na bezpečnost systémů/organizací, které nespadají do ZKB
  - Vyvěšeno na webu NÚKIB
  - Nezávazný dokument

DĚKUJI ZA POZORNOST

regulace@nukib.cz
nckb@nukib.cz