NÚKIB

Jakub Veselý ředitel odboru vládní CERT

Adam Kučínský ředitel odboru regulace

Co dělá NÚKIB

- NÚKIB je regulátor
- Nastavuje standardy v oblasti kybernetické bezpečnosti (vyhlášky a zákon)
- Analyzuje a vyhodnocuje kybernetickou bezpečností situaci
- Dohlíží na kybernetickou bezpečnost povinných osob ze ZKB
  - Ve zdravotnictví je to aktuálně 16 nemocnic

- **NÚKIB není IT dodavatel, nemůže suplovat úlohu správce systému!**
- **Za dopad incidentu i za jeho vyřešení je vždy odpovědný správce systému!**

Události z našeho pohledu

- Zpráva v médiích
- Snaha kontaktovat nemocnici v Benešově
- Rozhodnutí o pomoci a vyslání response týmu
- Vyslán response tým
  - Analyzuje
  - Doporučuje
  - Navrhuje opatření
- Vydání upozornění na hrozbu **Emotet-Trickbot-Ryuk**
- Naplánováno penetrační testování

Naše činnost v Benešově

- 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

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 je často špatně

- Technické nedostatky
  - Nedostatečná segmentace sítě
  - Nikdo se nestará o zranitelnosti
  - Nedochází k aktualizaci systémů
  - 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

Co můžeme nabídnout?

- Všechny vzdělávací materiály najdete na stránkách
  - https://nukib.cz/cs/vzdelavani/
- Informace o hrozbách
  - https://www.govcert.cz/
- Bezpečnostní doporučení NÚKIB pro administrátory 3.0
  - https://www.govcert.cz/download/doporuceni/NUKIB_doporuceni_admin_3.0_barva.pdf
- Scan zranitelností
  - Žádost na e-mail: nckb@nukib.cz
  - Předmět „Žádost o scan zranitelností *nemocniceXY*“
  - V odpovědi na e-mail dostanete informace o dalším postupu