27. 2. 2020

KYBERNETICKÉ OPERAČNÍ CENTRUM

Analýza incidentu v nemocnici Benešov

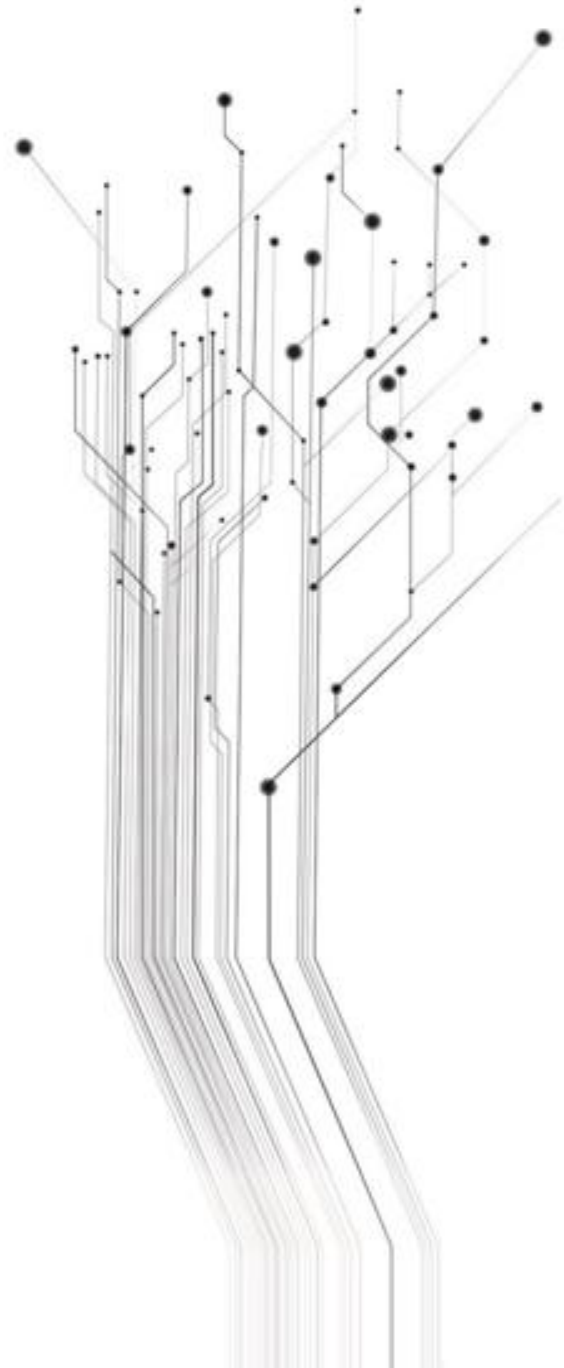
Aleš Staněk - vedoucí oddělení KOC

Incident v nemocnici Benešov

- „RANSOMWARE RYUK & NEMOCNICE BENEŠOV 12/2019“

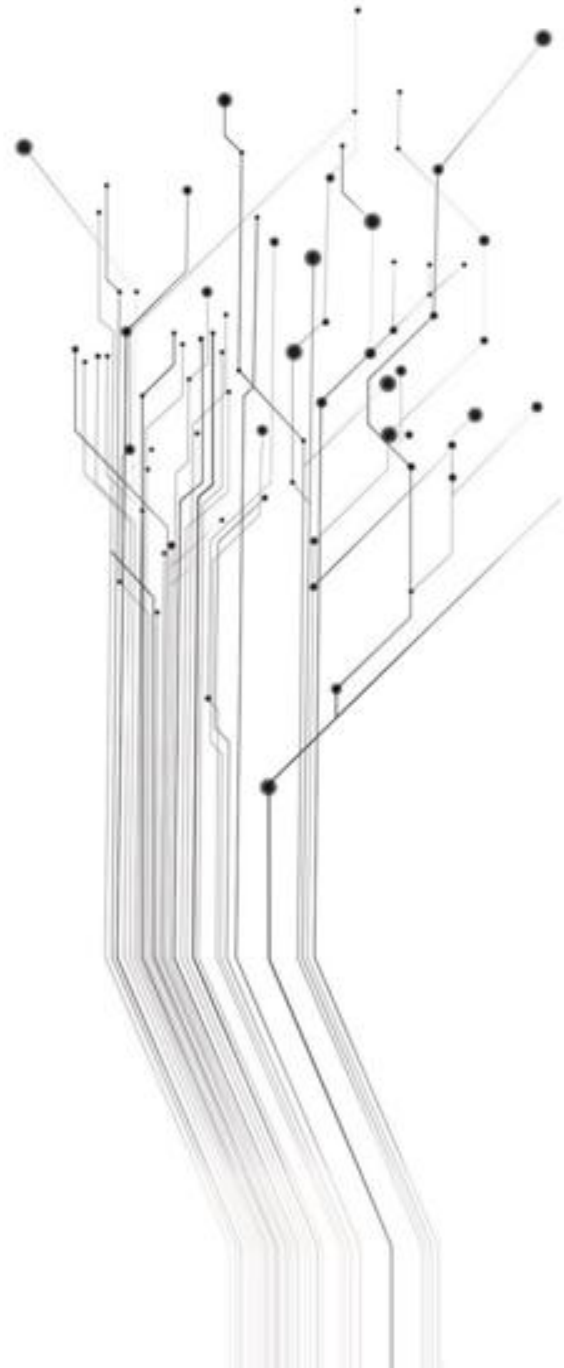
Chronologie útoku

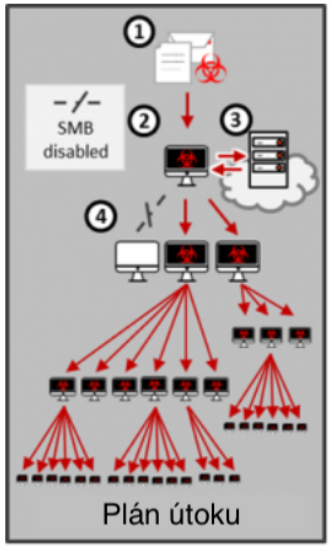
- Infiltrace virem - není známo
- Nahlášení problému - 11. 12. 2019 ve 2:50
- Detekce útoku - 3:20
- Vypnutí sítě IT oddělením nemocnice - 3:30
- Odstraňování následků útoku
- Poslední oddělení plně v provozu od 15.1.2020



Vektor útoku

- Necílená phishingová kampaň
- Otevření závadné přílohy
- Instalace malware **Emotet**
- Scan systémů a následné stažení trojan **TrickBot**
- Scan účtů, prolomení hesel administrátorů
- Rozšíření po síti
- Stažení ransomware **RYUK** - šifrování systémů





Plán útoku

1 PHISHING

Masivní e-mailová kampaň např. s fakturou, upozorněním na platbu daně a možným linkem

Uživatel otevírá závadnou přílohu e-mailu

PowerShell script stahuje malware Emotet

2 OBSAZENÍ POZIC

Emotet upravuje registry pro automatické spuštění a infiltruje se do běžících procesů

3 INSTRUKTÁŽNÍ FÁZE

Emotet informuje o nové infekci své odesílatele a přijímá instrukce. Následuje stažení TrickBot

4 PROPAGACE DO SÍTĚ

Infiltrace do předešlé komunikace

Hesla v internerových prohlížečích

Kompromitace hesel v počítači

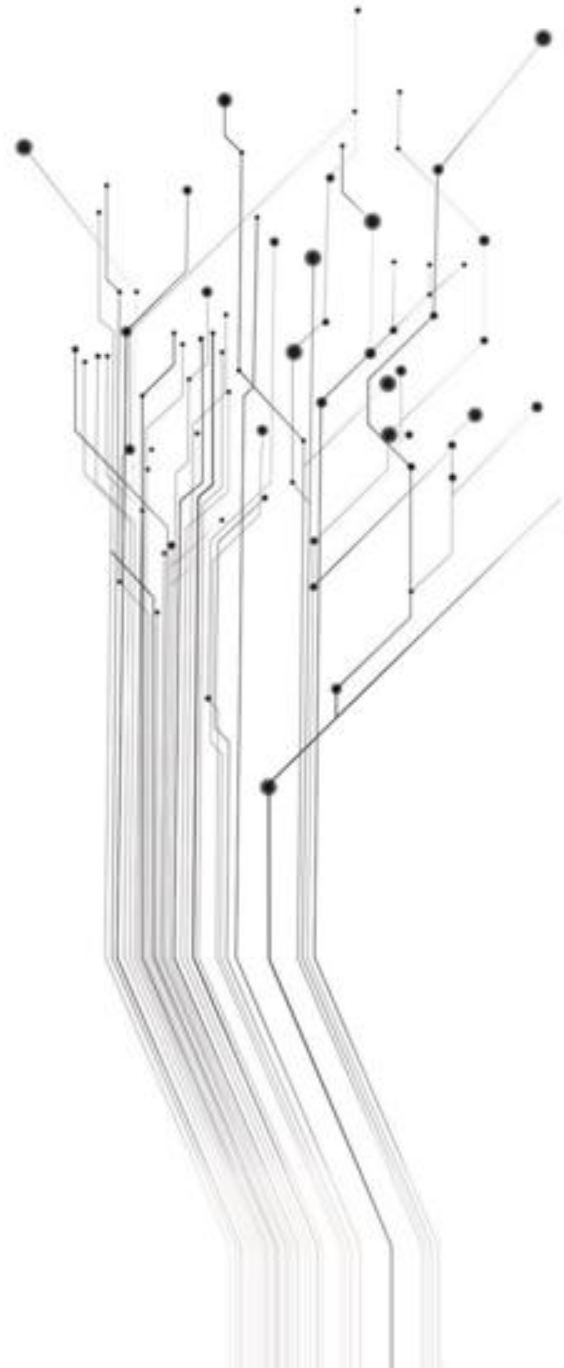
Kompromitace hesel v emailových účtech

SMB

Kompromitace hesel v síti

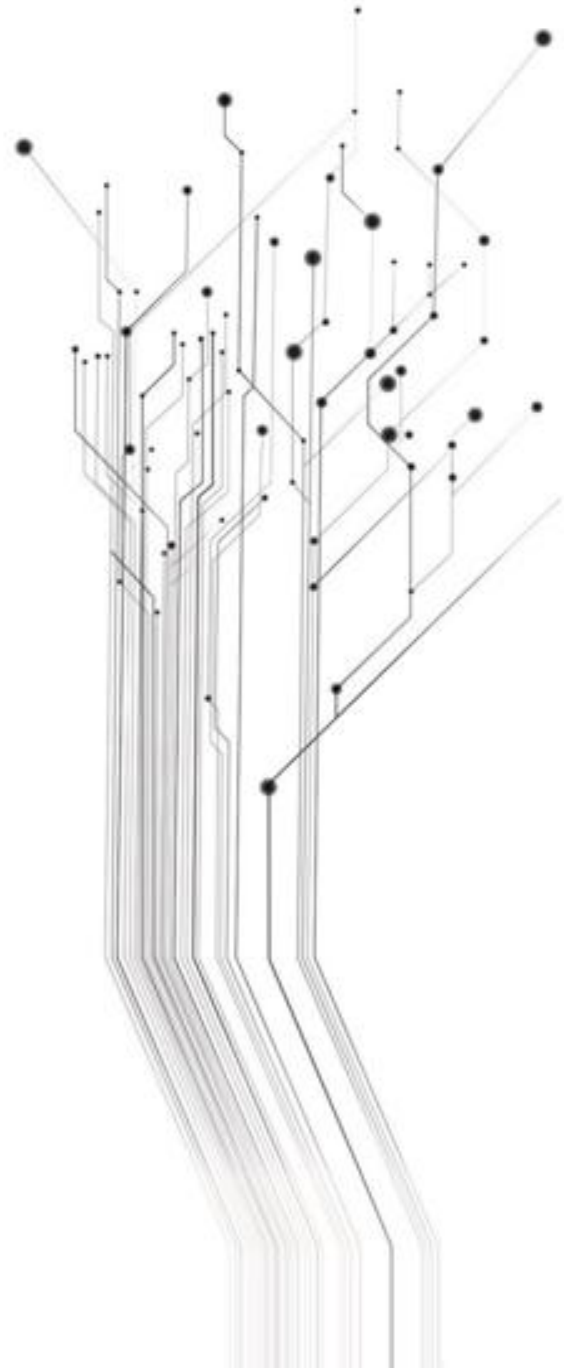
Provoz nemocnice po napadení

- ▪ Z počátku systém „Papír-Tužka“
- ▪ Po týdnu zprovozněn ekonomický a personální systém, lékárenský systém a zdravotnická dokumentace
- ▪ 19. 12. 2019 - fungují zobrazovací techniky, tedy RTG, CT a magnetická rezonance
- ▪ 14 dní bez připojení k internetu
- ▪ 30. 12. 2019 - provoz nemocnice se dostal do normálu
- ▪ 7. 1. 2020 - upozornění pacientů na delší dobu čekání



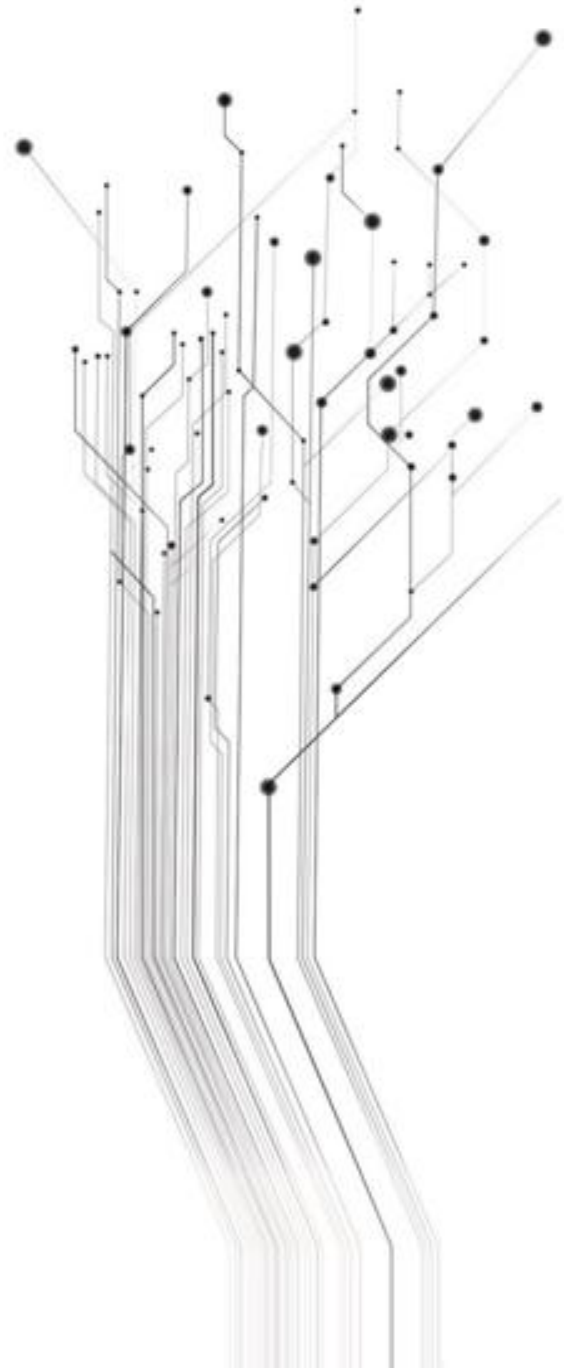
Stav infrastruktury před incidentem

- FW - výkonnostně nedostačuje
- Antivirus na koncových stanicích i serverech
- Většina serverů běží na starém virtualizačním prostředí
- Nedostatečná segmentace sítě
- Stanice mix OS od Win XP po Win 10
- „Black box“ - zařízení pro specializovaná vyšetření (rentgen, ultrazvuk, CT)
- Neomezený přístup na internet všem
- Otevřené RDP do internetu



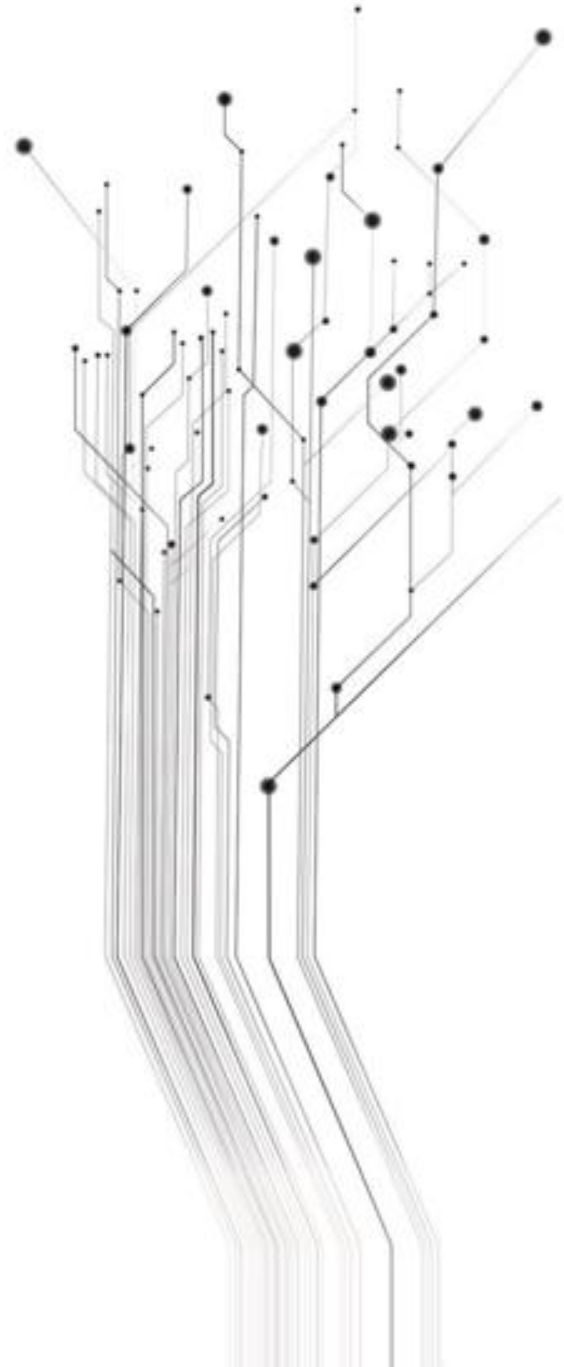
Stav infrastruktury po incidentu

- Nový FW - blokující politika, důraz na vyšší segmentaci
- Všechna vzdálená připojení striktně přes FW
- IT infrastruktura na aktuálních verzích OS
- Zapnuta technologie DLP
- Pro přístup na internet uplatňovány restrikce
- Dohodnuty penetrační testy
- Nastaveno dvoufázové zálohování (offline, online)
- VPN

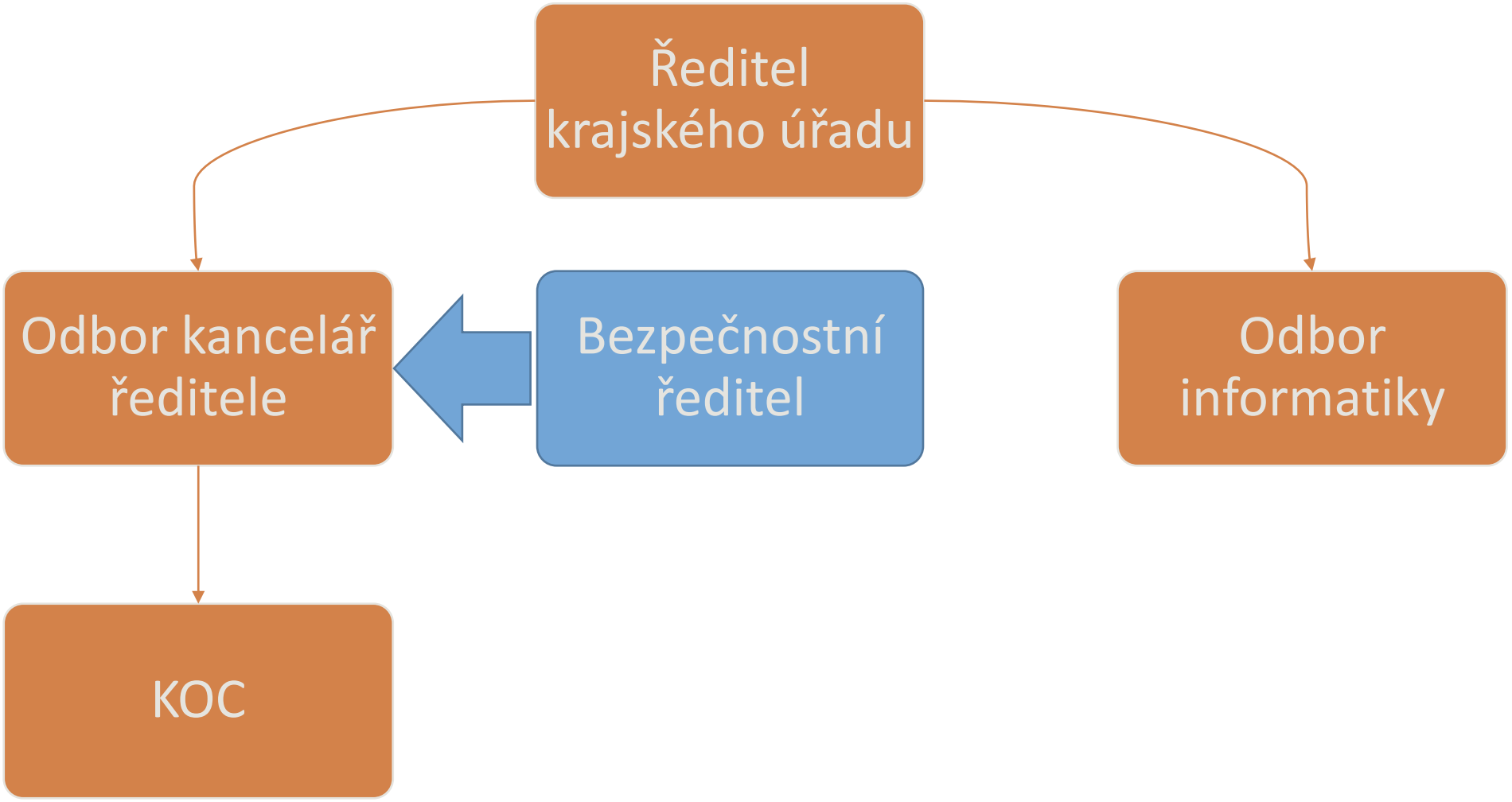


Vzniklá škoda

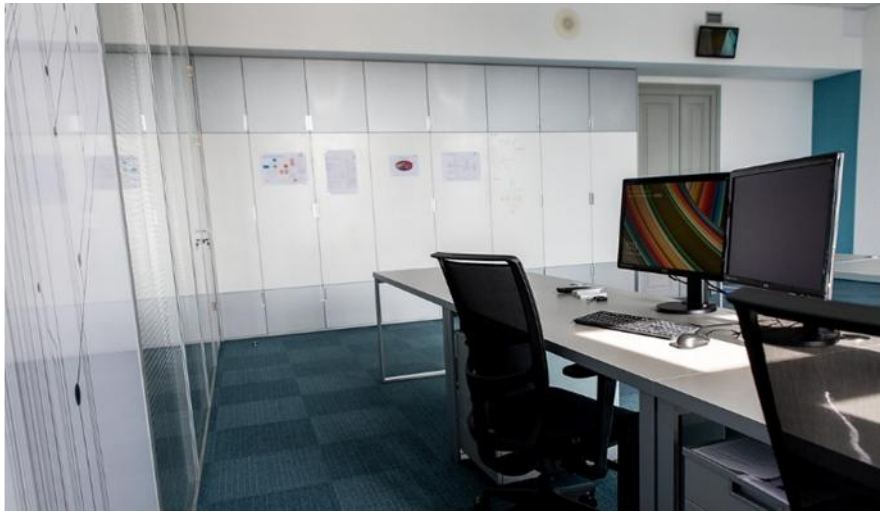
- 30 mil. Kč poskytl Středočeský kraj
- Celková výše bude vyčíslena do polovinu roku 2020
- Škoda přesáhne 50 mil. Kč
- Odhad dle PhDr. Jana Kolbaby (technický ředitel Nemocnice Benešov)

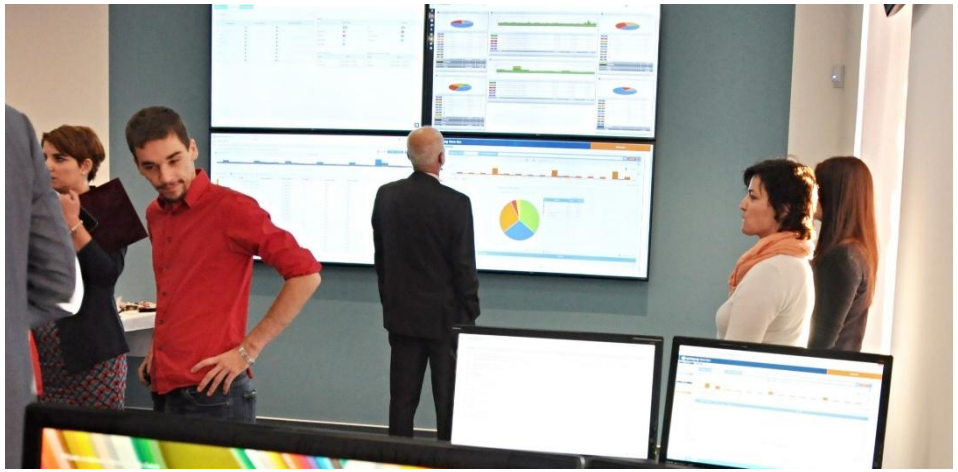


Organizační začlenění



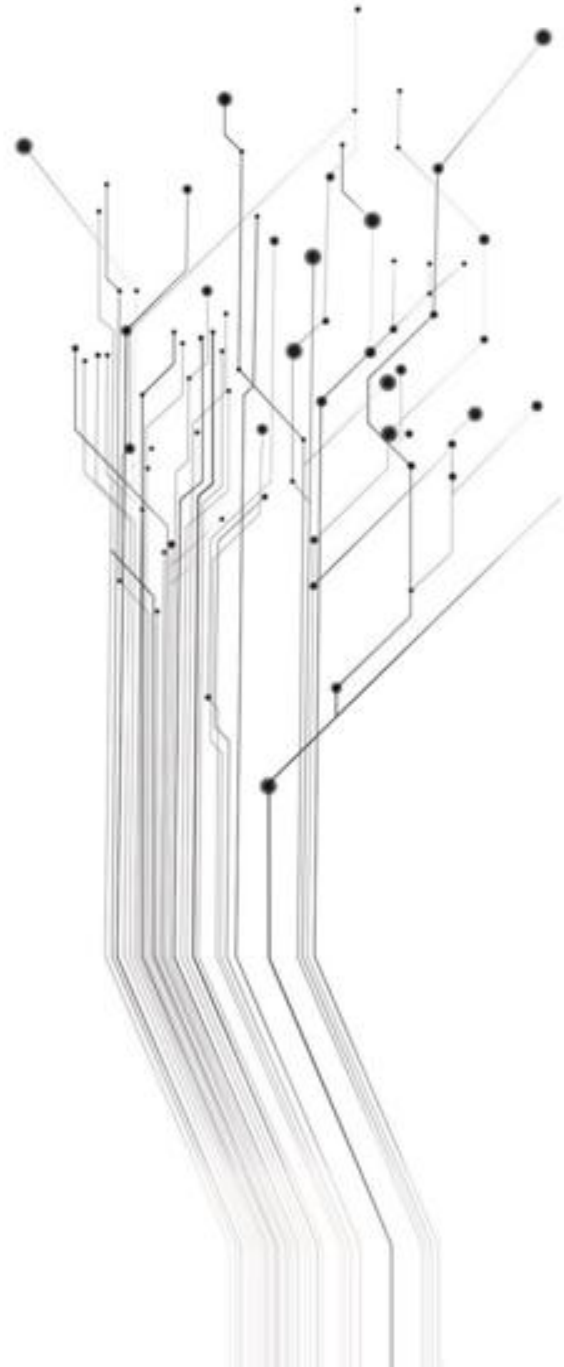
Uvedení dohledového centra do provozu 09/2016





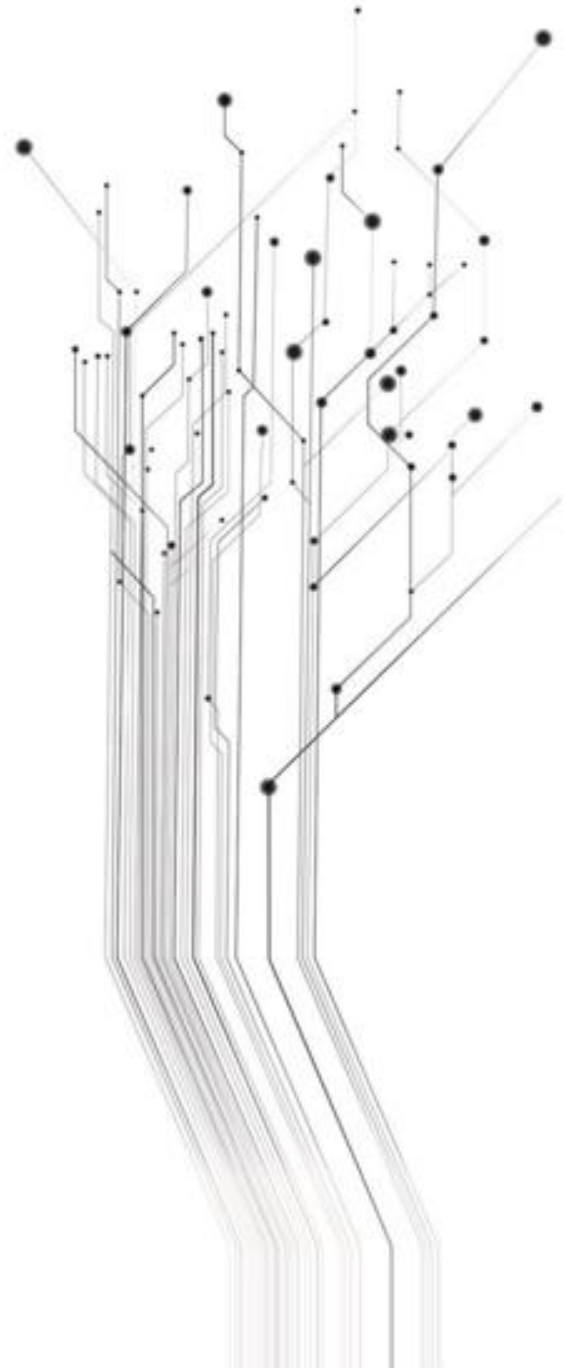
Současný stav KOC JMK

- Je spuštěn monitoring 17 samostatných oddělených sítí: KOC, JMK, SÚS, zatím 4 vybrané střední školy a 9 krajem zřízených nemocnic
- Hlásíme dle zákona všechny vzniklé KBI
- Poskytujeme součinnost při šetřeních NÚKIB a Policie ČR
- Za den vyhodnotíme cca 80 milionů událostí



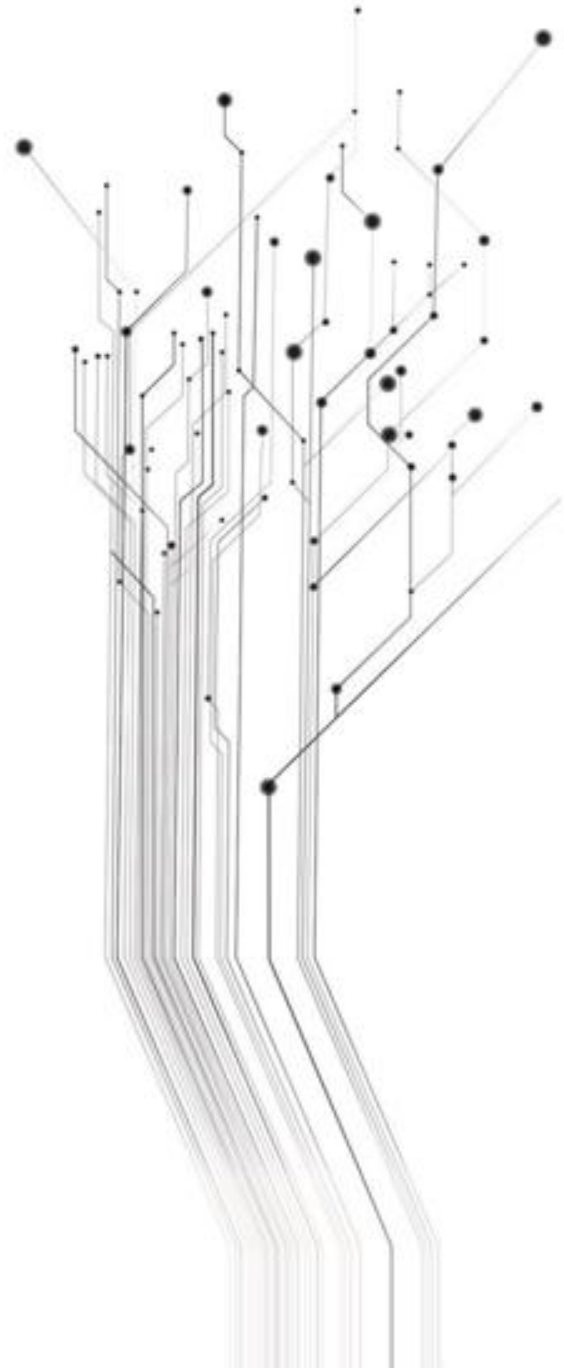
Příspěvkové organizace kraje

- Jihomoravský kraj je zřizovatelem 230 příspěvkových organizací
- Mají různou velikost 3 – 608 zaměstnanců
- Pracují s různými rozpočty 1,5 – 600 milonů Kč za rok
- Starají se o majetek v rozmezí 0,9 – 963 milonů Kč
- Působí v různých oborech – zdravotnictví, školství, dopravě, sociálních službách, kultuře



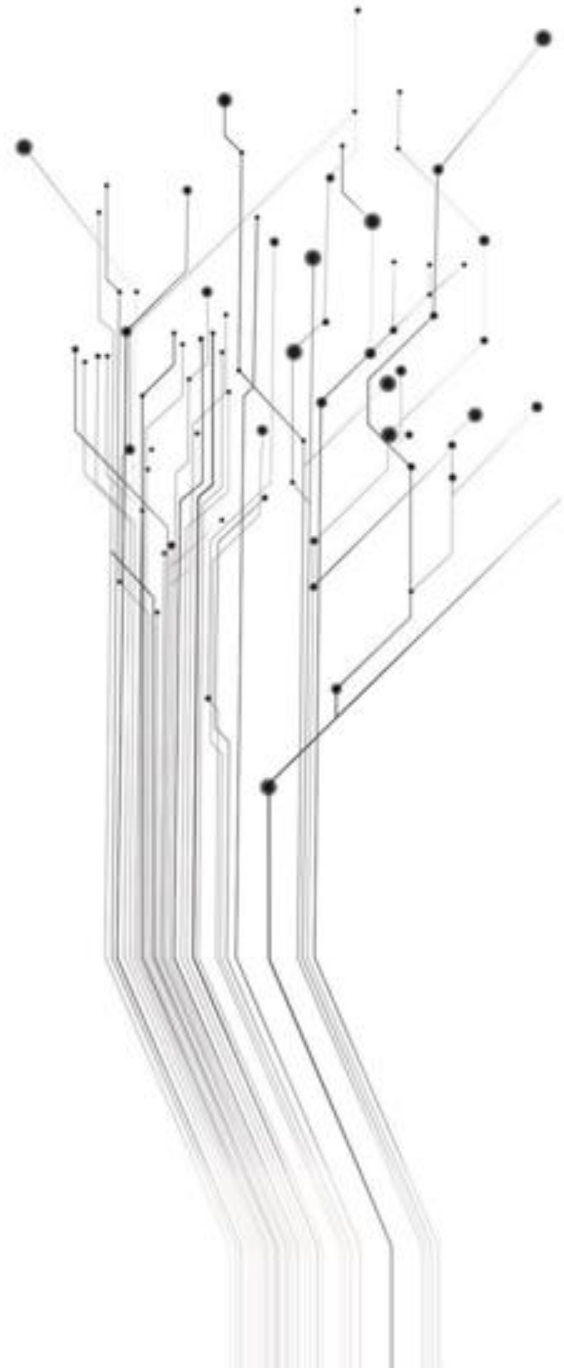
Co děláme?

- Sběr logů ze zařízení
- Analýza a vyhodnocení
- Upozornění na nedostatky v zabezpečení
- Podpora při vzniku bezpečnostní události
- Tvorba znalostní databáze událostí
- Aktivní monitoring provozu
- Testování aplikací, penetrační testování
- **Aktivně se snažíme zlepšovat úroveň KB připojených organizací**



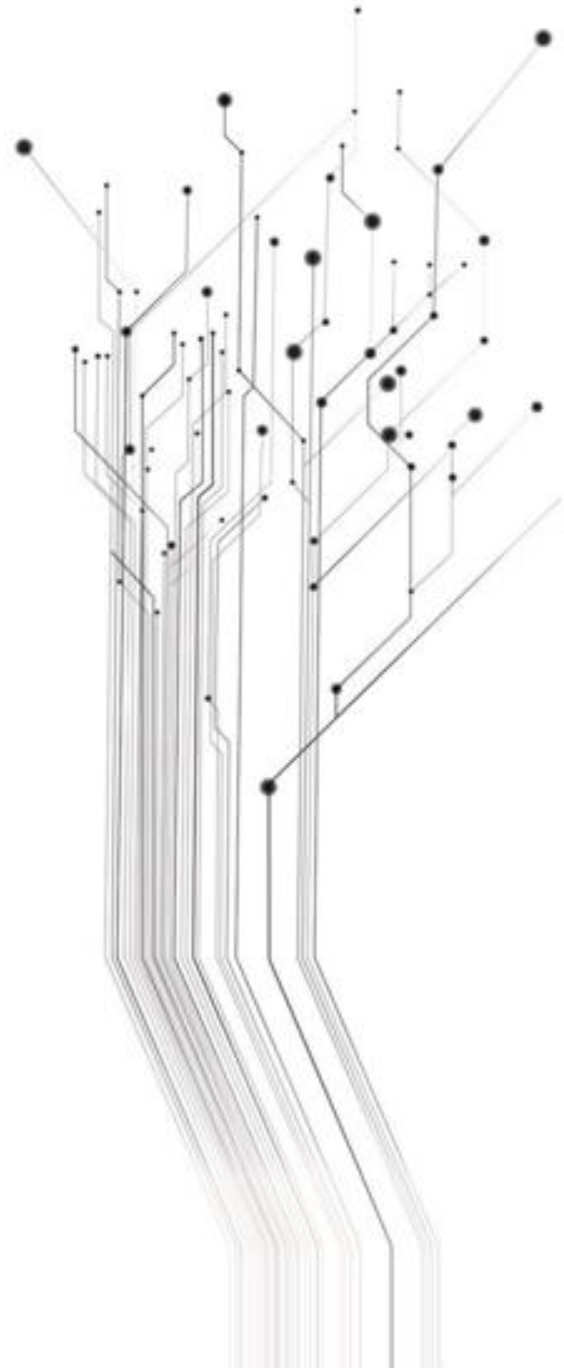
Používané technologie

- Log management - Syslog-ng Store Box (SSB)
- Security Information and Event Management - ArcSight
- Monitoring vlastní sítě - Flowmon
- Provozní monitoring - Centreon
- Ticketovací systém - Request Tracker (RT)
- Zákaznický portál - CyberCopter



Události z nedávné minulosti

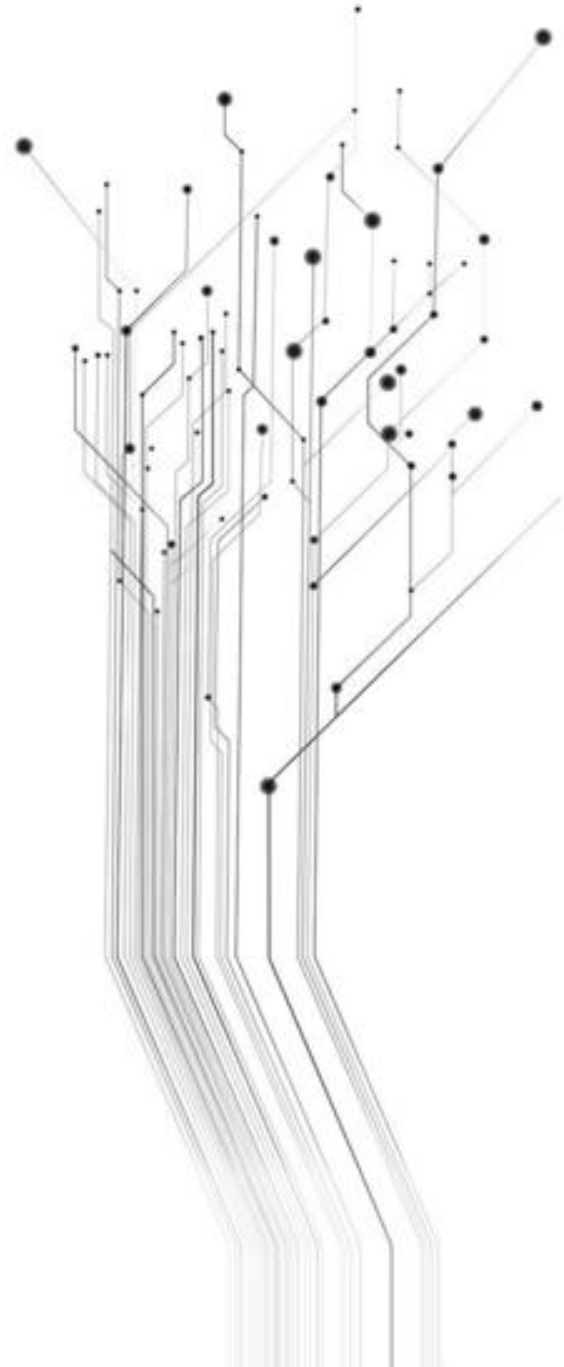
- Otevřené SSH do internetu
- Přístupná web administrace FW z internetu
- Konfigurace politik - ukončení pracovního vztahu
- Stejné phisingové kampaně u několika zákazníků
- Objevení SQL injection zranitelností v aplikacích
- Phishingová kampaň proti JMK



Výsledky phishingové kampaně

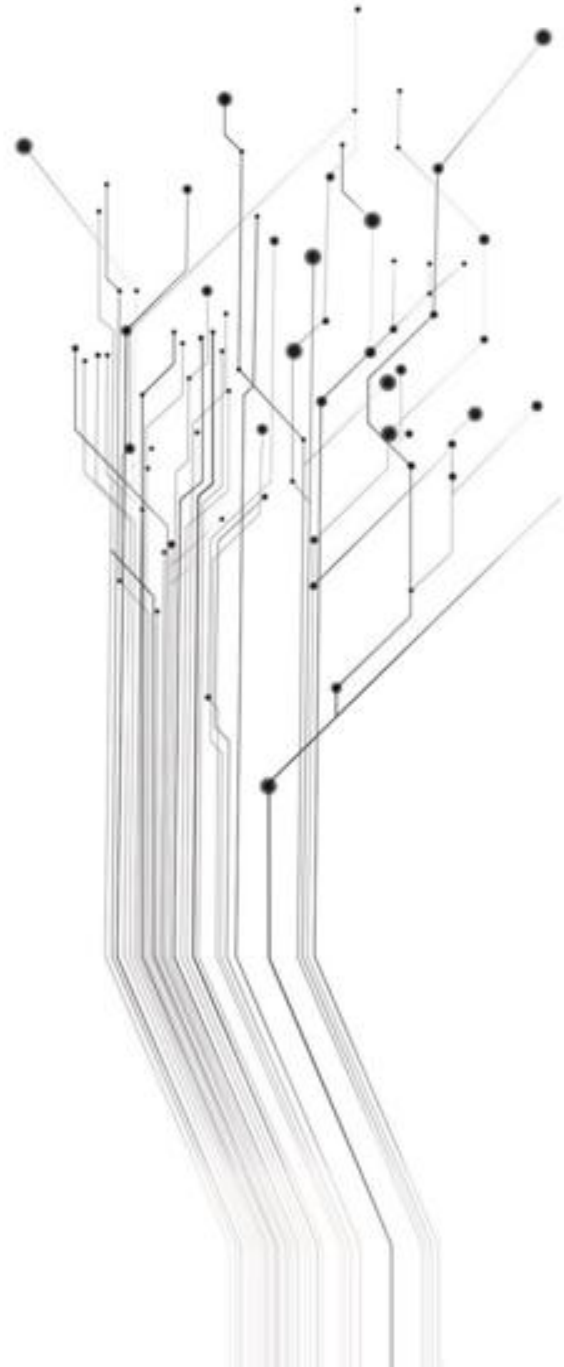
Kampaň v číslech (období od spuštění do reakce OI v 8:09)	
Počet odeslaných e-mailů	114
Počet prokliků z e-mailů	107 z toho 44 unikátních
Počet prokliků na přihlašovací stránku	80 z toho 40 unikátních
Počet pokusů o odeslání přihlašovacích údajů	45 z toho 31 unikátních

Kampaň v číslech po odhalení	
Počet odeslaných e-mailů	715
Datum a čas odeslání prvního e-mailu	07:13:02 - 13. 02. 2020
Datum a čas odeslání posledního e-mailu:	13:10:02 - 13. 02. 2020
Počet prokliků z e-mailů	151 z toho 69 unikátních
Počet prokliků na přihlašovací stránku	119 z toho 60 unikátních
Počet pokusů o odeslání přihlašovacích údajů	73 z toho 47 unikátních

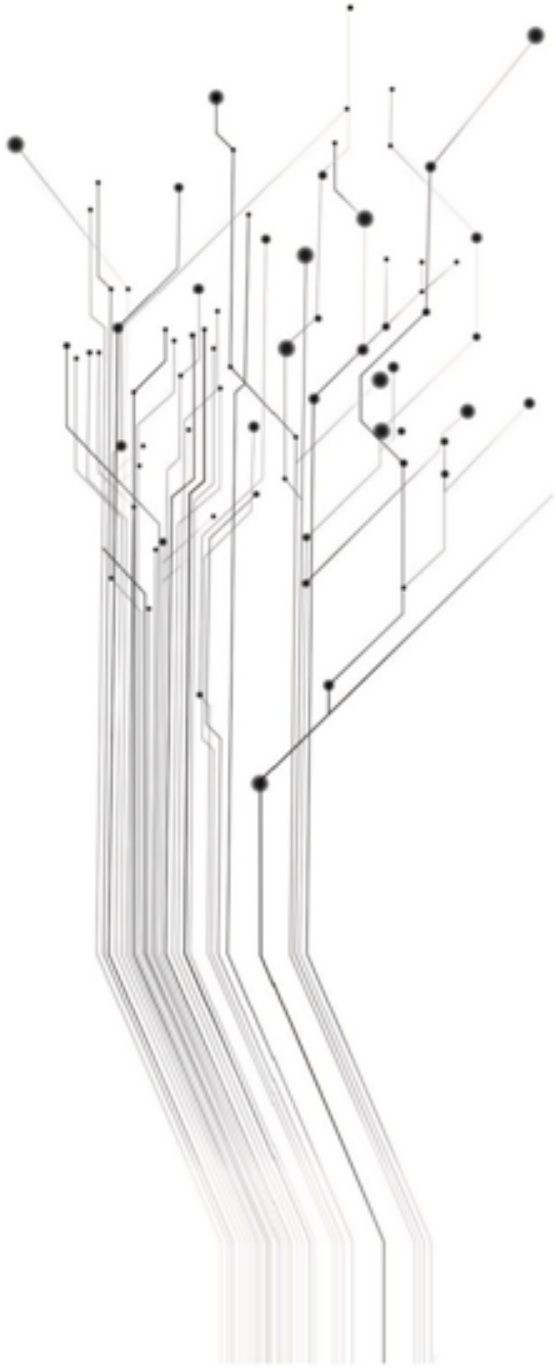


Co neděláme?

- Sledování mailové či jiné formy komunikace
- Nahlížení či přístup do dokumentů nebo složek
- Nahlížení do konfigurací FW či jiných zařízení organizace
- Sledování aktivních činností uživatelů
- Nejsme IT dodavatel
- Nejsme správci systému



27. 2. 2020



KYBERNETICKÉ OPERAČNÍ CENTRUM

Případné dotazy
Aleš Staněk - vedoucí oddělení
Kybernetické operační centrum
stanek.ales@jmk.cz
Telefon: 541 658 903