Kybernetická bezpečnost

… to je to, oč tu běží

Jaroslav Hloušek, ředitel divize ICT a eGovernmentu

9.ročník konference INFORMAČNÍ A KOMUNIKAČNÍ BEZPEČNOST ČR

21.5.2019

Česká pošta

Česká pošta v číslech

- 32.000 zaměstnanců
- 3.200 poboček
- 22.000 end points
- 70.000 všech koncových zařízení
- 350 serverů MS Windows
- 700 serverů UNIX (Linux)
- 100 serverů SAP
- Obrat cc 20mld Kč

… provozujeme ICT služby

- 60% infrastruktury je KII
- ISDS
- PostSignum
- Bankovní služby
- Služby datových center
- Vývoj
- Interní ICT provoz

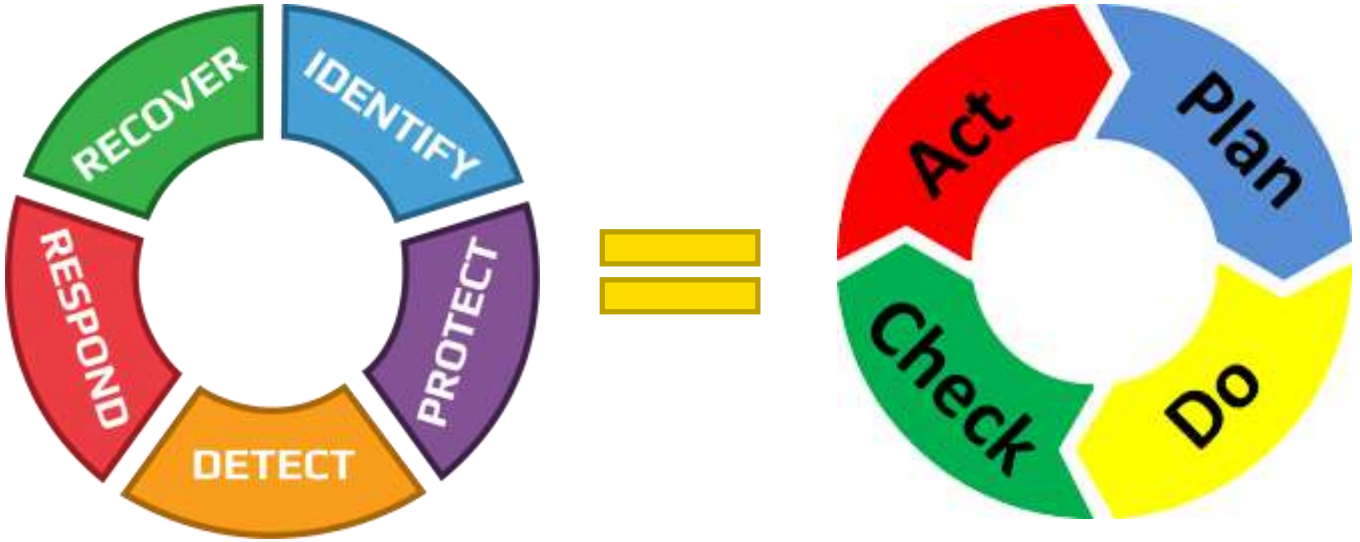
Kyberbezpečnost na České poště

- Monitoring provozu ICT
  - SIEM (log management) - RSA
  - Monitorování síťových toků a nastavení - GreyCortex, FlowMon
  - Skener technických zranitelností – NESUS (Tenable)
  - PIM (Ekran)
- Pasivní ochrana komunikace
  - Antivir s centrální správou - ESET
  - Filtrování komunikace – F5
  - Firewall - CheckPoint
  - VPN, kryptování - Cisco

… dále

- Centrální řízení uživatelů
  - IDM – MidPoint (OpenSource)
  - MDM - Microsoft
- Správa licencí – AVE Caesar
- Řízení bezpečnosti
  - Řízení rizik, řízení kontinuity – Verinice (jen pro ISDS)
- Dokumentace
  - Politiky, směrnice, metodiky, ...
- Zvyšování bezpečnostního povědomí
  - Školení, příručky

Koncept fungování kyberbezpečnosti ČP



CYBERSECURITY FRAMEWORK **PDCA – DENINGŮV CYKLUS**

Team kyberbezpečnosti pro ČP / BICT

- 12 lidí
- IT náklady na kybernetickou bezpečnost za rok činí asi 43,5mio Kč
- Pracoviště ve 4 lokalitách
- Základní činnost
  - Interní kyberbezpečnost (organizační i technická)
  - Dohledy a řešení incidentů
  - Edukace uživatelů všech úrovní
  - Interní projekty
  - … a bohatá administrativa ☺

Máme reálné zkušenosti ...

- Úspěšný fishing (finanční ztráta v řádech 100tis.)
- Požár DC (zastaralá el.instalace, díky nezávislé záloze nedošlo k fatálním škodám)
- Zneužití loga ČP pro fishing (facebook, WhatsUp)
- Kompromitace osobních údajů (úmyslná i neúmyslná)
- Zneužití přístupových údajů uživatelů (nedbalost uživatelů)
- Vloupání a krádeže výpočetní techniky
- Velkoplošné výpadky
- Virová pandemie

Je důležité VČAS a RYCHLE reagovat, postupovat dle krizových scénářů, události následně analyzovat (příčiny a důsledky) a vždy se POUČIT!

Naše priority ...

- Zvyšovat naši odbornost v oblasti kyberbezpečnosti a zároveň i úroveň našich uživatelů (projekty, vývoj, provoz …)
- Neustále zvyšovat podíl automatizace na monitorování provozu ICT a tím zajišťovat zvyšování efektivity bezpečnostního dohledu
- Být efektivním partnerem při budování eGovernmentu (ISDS, CzechPOINT)
- Aktivně se podílet na realizaci nových elektronických služeb klientům ČP
- Bezezbytku naplnit povinnosti uložené státem (legislativou)

… a plány do blízké budoucnosti?

Integrace nástrojů bezpečnostního dohledu a vybudování SOC (security operation center) na vysoké úrovni.

Vznik POST CSIRT (Computer Security Incident Response Team).

Česká pošta

Najdete nás na