DOHLEDOVÉ CENTRUM SOCCR

(Security Operation Center for Cyber Reliability)

31/3/2015

Česká pošta
odštěpný závod ICT služby

AFCEA: Seminář CERT & SOC

SOCCR

DOHLEDUJE BEZPEČNOST ICT SYSTÉMŮ RESORTU MV

PODPORUJE ŘÍZENÍ RIZIK A KONTINUITY

IDENTIFIKUJE, VYHODNOCUJE A HLÁSÍ INCIDENTY DO NCKB (NBÚ)

ŘÍDÍ BEZPEČNOST

24x7

TÝM SOCCR = CIRT MV

POSKYTUJE PROVOZNÍ A BEZPEČNOSTNÍ REPORTING

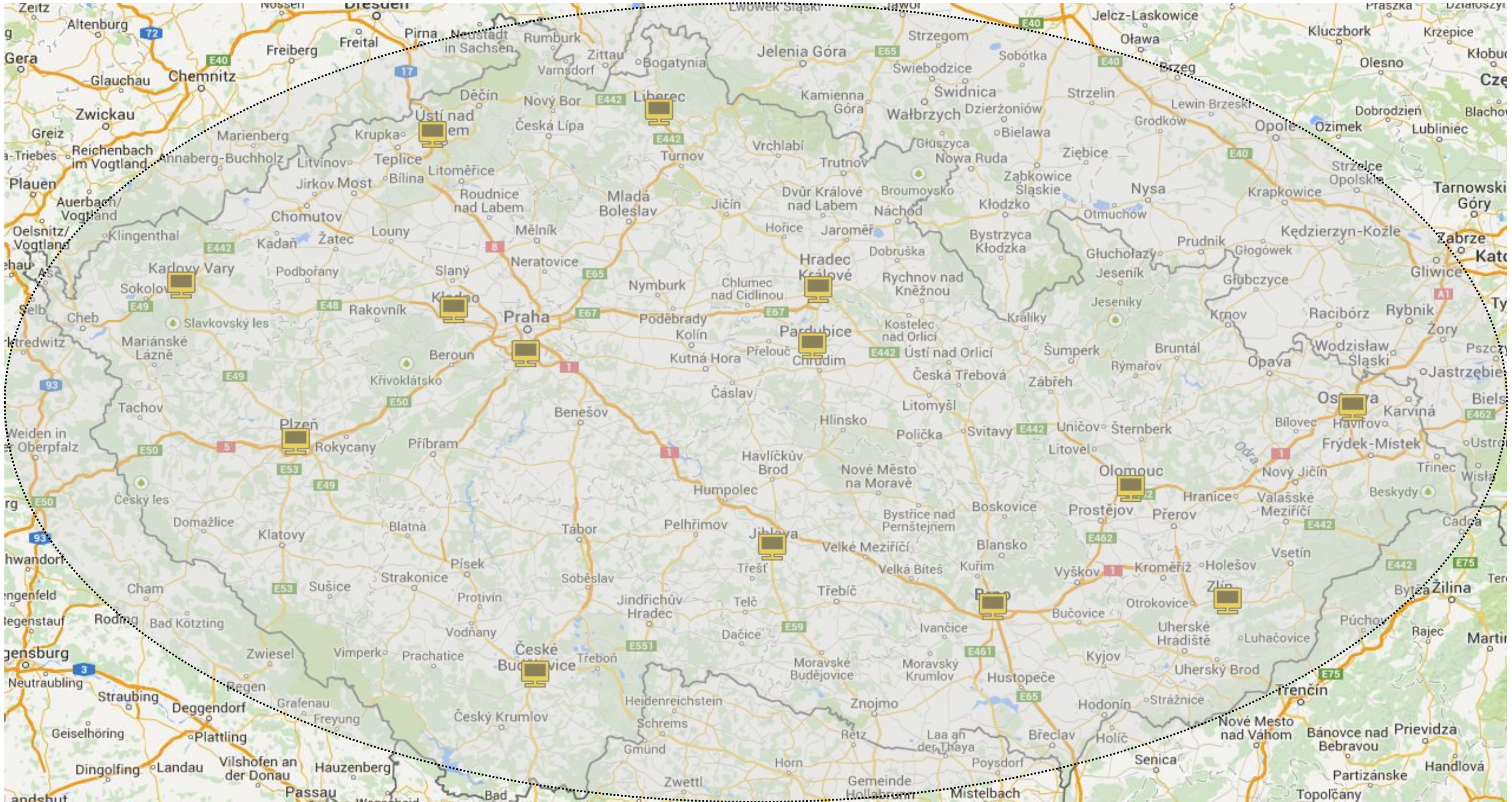
JE V SOULADU ISO 27001 ISO 22301 ISO 20000

JE MODULÁRNÍ A PŘIPRAVEN NA DALŠÍ ROZVOJ

SKENUJE ZRANITELNOSTI

PROVOZUJE ČPOZ

Geografie SOCCR



SOCCR dohleduje až 10 000 aktivních prvků po celém Česku (stav 2016)

Aktivní vs. pasivní mód

AKTIVNÍ MÓD – ŘÍDÍ BEZPEČNOST	PASIVNÍ MÓD – DOHLÍŽÍ BEZPEČNOST
SOCCR je bezpečnostní administrátor systému	SOCCR je dohlížitel - pouze dostává informace ze systému
SOCCR analyzuje, vyhodnocuje a dává informace zpět do systému, aktivně řeší incident (technicky, procesně), ve spolupráci s administrátory zasahuje do konfigurace	SOCCR analyzuje, vyhodnocuje a dává informace zpět do systému, dává doporučení na reakci
SIEM – v systému je implementována sonda/agent, sbírá události, vyhodnocuje, do SOCCR zasílá agregované údaje	SIEM – získává agregované události z koncového systému pomocí systémového účtu, logy se analyzují až v SOCCR
SOCCR vyžaduje plný přístup do systému, implementaci nástroje PIM/PAM + 2FA (administrátorské přístupy)	N/A – SOCCR má pouze přístup „pro čtení“
SOCCR provádí automatizované skenování zranitelností s autentizací	SOCCR (ne-)pravidelně skenuje zranitelnosti bez autentizace (s povolením správce systému)
Honeypot – implementován v (interní) síti, aktivně dohleduje technologií IPS/IDS	N/A
Podpora procesů řízení rizik a kontinuity (SOCCR má nástroj)	SOCCR neřeší procesy RM a BCM, pouze jednoduchá metodická podpora zdarma

Kompetenční centrum doplňuje SOCCR

SLUŽBY
ŘEŠENÍ
TECHNOLOGIE
PRODUKTY

DOHLEDOVÉ CENTRUM SOCCR

ZNALOSTI

LIDI

ZKUŠENOS

TI

Další kroky 2015

- Definovat rozhraní pro připojené systémy
  (detail aktivního a pasivního módu)
- Připravit typové projekty pro konektory na SOCCR
- Implementovat technologie a procesy v rámci MV
- Zahájit provoz dohledového centra SOCCR

Rozvoj SOCCR 2016+

- Rozšířit tým a nástroje pro **skenování veřejných fór, medií, sociálních sítí** pro korelaci interních událostí v systémech MV
  s podezřelými událostmi v externím prostředí
- Získávat informace o všech hrozbách z různých zdrojů a koncentrovat úsilí na relevantní nebezpečné případy
- Vytvořit SOCCR Intelligence Database – shromažďuje a **koreluje** všechny události v systémech MV
- Automatizovat procesy řízení rizik a kontinuity systémů MV
- Rozšířit bezpečnostní reporting o stavu systémů (Big Data)

Dohledové centrum SOCCR

Děkuji za pozornost