Postřehy z pilotního provozu služby „Penetrační testy"

Dominik Marek, Kraj Vysočina

Kraj Vysočina

Kraj Vysočina

- zkušenosti s penetračními testy
- zavedená bezpečnostní opatření
  - nejen na základě první zkušenosti z pentestů
- oblasti
  - Autentizace
  - Networking
  - WWW
  - Soubory
  - Monitoring

Autentizace

- zavedení tierového modelu administrace
- Interactive logon: Number of previous logons to cache
  - stanice 1
  - servery 0
- přeheslování účtu typu Administrator
- nasazení 2FA pro VPN a VDI

Networking

- registrace kr-vysocina.com, kr-vysocina.net, kr-vysocina.org, kr-vysocina.info, kr-vysocina.eu
- vypnutí SMBv1
- zákaz všeobecné dostupnosti zdrojů z Internetu pro serverový segment
  - včetně zavedení serverové webové proxy

Web služby

- eliminace wildcard certifikátů
- smluvní podmínky s dodavateli - opravy zranitelností

Soubory

- zakázáno spouštění nepodepsaných maker
- zakázáno spouštění javascriptu z PDF souborů
- soubory typu .js(e) a .iqy - výchozí program na spouštění je notepad

Monitoring

- Flow based monitoring sítě
- SIEM

Děkuji za pozornost!

Dominik Marek

Kraj Vysočina

Marek.Dominik@kr-vysocina.cz