wunder

IT drošības izaicinājumi mazā/vidējā uzņēmumā

06.10.2018

wunder

GERMANY

Munich
Berlin

FINLAND

Helsinki
Turku

LATVIA

Riga
Valmiera
Rezekne

ESTONIA

Tallinn

SATURS

Izaicinā-jumi

- Darba un privātās IT vides saplūšana
  - Datorus atļauts izmantot privātām vajadzībām
  - Personīgie telefoni tiek izmantoti darbam
  - Administratīvas tiesības uz iekārtām
- Augsts darbinieku/uzņēmuma uzticēšanās līmenis
- Vēsturiski veidojušās piekļuves tiesības
- Neformālas informācijas plūsmas
- Vāja hierarhija, 'nē muļķībām'
- Netērējam resursus iespējamām (nākotnes) problēmām
- Normatīvo aktu un citas 'ārējas' prasības

Ko mēs darām

- Modrība un atbildība (cilvēki nav 'vājais ķēdes posms')
- 'Hack your friends' (nmap, **openvas,** Nessus, ...)
- 'Security in-depth'
- Riski, IAAC, Continuous security
- IT aktīvi un atbildīgie
- 'Least privilege'

Kā mēs darām

- Modrība: Drošības sadaļa Intranet, #security, 'security team bi-monthly'
- Prasības iekārtu (datori, telefoni) iestatījumiem un paš-kontrole
- CyberEssentials+
- Autentifikācija, paroļu un atslēgu pārvaldība, MFA
- Šifrēšana ('data at rest', 'data in transit': VPN, SSL)
- Pret-ļaunatūras kontrole
- Programmatūras atjaunojumi, notifikācijas (IFTTT, #security)
- Security As A Code / iekšējā 'labā prakse'


wunder
Paldies!