Kiberdrošības incidentu pārvaldība

Tet pieredze

Uldis Lībietis

IT drošības pārvaldnieks

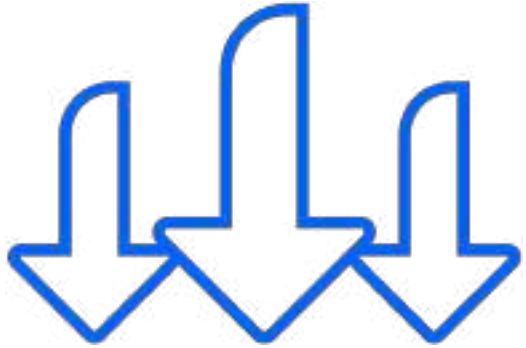
Lai nepieļautu IT drošības incidentus

- Aizsardzības risinājumi:
  - darbinieku izglītošana
  - pretvīrusu aizsardzība
  - regulāri atjauninājumi
  - konfigurāciju pārvaldība
  - ievainojamību diagnostika
  - ielaušanās testi
- Uzraudzības risinājumi
- Reakcija uz incidentu

Kibernoziedznieki neguļ un brīvdienas neņem

Par **50%** vairāk nobloķēto e-pastu ar **vīrusiem**

Jauna veida izplatīšana **-.edoc failiem**



Gandrīz **2400** DDoS uzbrukumi: lielāki, agresīvāki, ilgāki

Arī mēs strādājam 24/7/365

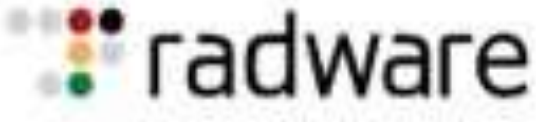
Uzraugām sevi

Sniedzam drošības pakalpojumus klientiem

Informējam par nepilnībām

~3 miljardi apstrādātu auditācijas pierakstu

Tehniskie palīglīdzekļi



Ievainojamās un uzlauztās mājas iekārtas

- Simptomi:
  - sūdzības – slikts internets
  - neizskaidrojami iekārtu restarti
  - dalībnieki DDoS uzbrukumos
  - Cert.lv sarakstos
  - Botnet dalībnieku sarakstos
  - SPAM izsūtītāju sarakstos
  - iekārtu «bojāeja»
  - VoIP zvani uz ārzemēm

48 300 brīdinājuma vēstules klientiem – arī par apkures katliem, kamerām, mājas automātiku

Pakalpojumu atteices uzbrukumi

- Simptomi:
  - sūdzības – slikts internets
  - pārslogotas iekārtas
  - lēcienveida slodzes pieaugums
  - izspiedēja vēstules
- Upuri:
  - azartspēļu spēlētāji
  - mācību/eksāmenu vides
  - bankas, internetveikali, lielie uzņēmumi

Novērst klienta paša spēkiem nav iespējams

Nu, protams – atjauninājumi

- Gadā **~17 000** drošības caurumu
  - Ne visi aktuāli
  - Ne visi bīstami
- Tomēr:
  - Ne viss tiek pateikts
  - Reizēm – samazināts vērtējums
  - Kombinācija ar citiem caurumiem
  - Riska vērtējums pieaugošs
  - Izmantošanas laiks no publicēšanas sarūk

Atjauninājumu instalēšana kā nepārtraukts process


ENDPOINTS
REALTIME THREATS
DDOS
THREATS
VULNERABILITIES
ATTENTION