IT riski un kiberdraudi valsts iestādēm un pašvaldībām

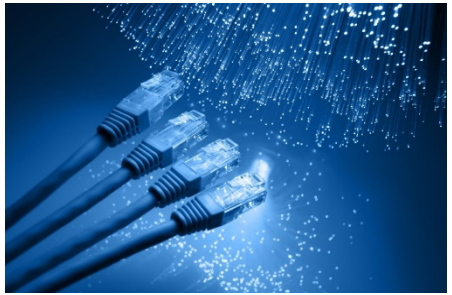
Uldis Lībietis

IT drošības pārvaldnieks

Datu aizsardzības speciālists

Pakalpojumi valsts un privātajam sektoram

Nodrošinām 54% Latvijas interneta plūsmas



Savienojamība

Čatbots, 24/7 zvanu centri, pieteikumu sistēmas

Komunikācijas un sadarbības iespējas

Apkalpojam vairāk nekā 5800 darbstacijas un 2200 serverus

Datoru apkalpošana un speciālistu īre

Pakalpojumi valsts un privātajam sektoram

5 datu centri Latvijā (ISO27001, PCI-DSS LV1, Tier III)

Datu centri un mākoņpakalpojumi

250+ industrijas tehnoloģiju eksperti

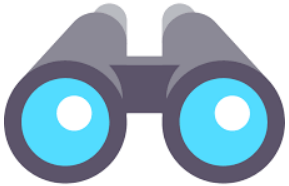
Informācijas tehnoloģiju konsultācijas

24/7 SOC (650 milj. logi dienā), drošības auditi, u.c.

IT drošības pakalpojumi

Tet pieredze IT drošībā

Tet infrastruktūras aizsardzība - informācijas avots par Jūsu IT drošības līmeni



- **DDoS uzbrukumu aizsardzība**
- **E-pasta aizsardzība:**
  - mēstules
  - antivīruss
- **Drošības notikumu uzraudzības sistēmas (SIEM)**
- **Citas drošības sistēmas:**
  - ugunsmūri
  - IDS/IPS
  - u.c.

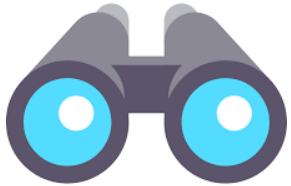
Sadarbība ar CERT.LV

- **Sniedzam CERT.LV informāciju par drošības incidentiem**
- **Saņemam informāciju par ievainojamām IP adresēm**
- **Reizi nedēļā veicam IP adrešu lietotāju apziņošanu:**
  - nedēļā tiek izsūtīti 700-900 brīdinājuma e-pasti
  - tajā skaitā valsts, pašvaldības iestādēm (~ 40)
  - lielākajai daļai apziņošana ir atkārtota
  - ievainojamības ir aktīvas 4-8 nedēļas
- **Sniedzam atbalstu visiem, kas to vēlās**

tet

Sniedzot interneta pakalpojumus Tet arī novēro

- **Pieejamības pārtraukumus:**
  - Jūsu elektroapgādes pārrāvumus
  - Jūsu telpu mikroklimata neatbilstību
  - DDoS uzbrukumus



- **IT drošības problēmu pieteikumus:**
  - zvanus
  - e-pastus
  - pieteikumu apstrādes sistēmas pieteikumus

Veicam IT drošības novērtēšanas darbības

- **IT un VDAR auditi, lai atbilstu**
  - Ministru kabineta noteikumiem 442
  - VDAR prasībām
  - Industrijas labajai praksei
- **Ievainojamību diagnostika**
  - Web aplikācijām
  - Datoriem/serveriem/mobilajām iekārtām/IoT
- **Ielaušanās testēšana**

Veicam IT vides uzturēšanas ārpakalpojuma sniegšanu

- IT drošības pārvaldnieks
- Datu aizsardzības speciālists
- Datortehnikas apkalpotājs

- 24/7 Drošības vadības centrs

Atziņas no IT auditiem 12.2017-11.2019

Biežāk identificētās IT drošības nepilnības valsts un pašvaldību iestādēs (1/3)

- **IT drošības organizācija/ IT drošības pārvaldnieks (16/30)**
  - Pienākumu atdalīšana
  - Netiek pildīti darba pienākumi
  - Formāla nozīmēšana – IT administrators, teh. resursu turētājs, IT vadītājs, Juridiskās nodaļas vadītājs
- **Netiek apzināti visi IT resursi un netiek veikta sistēmu klasifikācija (29/30)**
- **Netiek ierobežota fiziskā piekļuve (9/30)**
- **Netiek uzstādīti atjauninājumi (Software/Firmware) (29/30)**
- **Netiek atspējoti nevajadzīgi servisi (18/30)**

Biežāk identificētās IT drošības nepilnības valsts un pašvaldību iestādēs (2/3)

- **Tiek izmantota nedroša attālinātā piekļuve resursiem (29/30)**
- **Netiek izmantots vai nepareizi konfigurēts Ugunsmūris (14/30)**
- **Netiek veikta korekta rezerves kopiju veidošana, glabāšana un atjaunošana (28/30)**
- **Nepilnības lietotāju kontu pārvaldībā (30/30):**
  - Centralizācijas trūkums
  - Paroļu politikas pārkāpumi
  - Paroļu saglabāšana interneta pārlūkprogrammās
  - Koplietošanas kontu izmantošana
  - Pārmērīgu pieejas tiesību piešķiršana
- **Web analītikas neatbilstoša lietošana (10/30)**

Biežāk identificētās IT drošības nepilnības valsts un pašvaldību iestādēs (3/3)

- **Auditācijas pieraksti (30/30):**
  - Netiek veidoti
  - Netiek uzglabāti ārpus avota noteikto laika periodu
  - Netiek sinhronizēts laiks (NTP)
  - Netiek veikta analīze un reakcija uz incidentiem
- **Neaizmirstam par IoT iekārtām!**

MK 442 prasības bieži netiek ievērotas, jo trūkst kontroles mehānisma

Paldies par uzmanību!

Uldis Lībietis

IT drošības pārvaldnieks

Datu aizsardzības speciālists