“Kā pamanīt drošības incidentus?”

Gints Mālkalnietis, CERT.LV

Seminārs Jelgavas un Dobeles pilsētu un rajonu informātikas skolotājiem

Jelgava, 2012.gada 22.februāris

CERT.LV

Analizējiet ilgtermiņa aktivitātes datortīklā!

Vērojiet skolas ikdienas datu plūsmas!

Savāciet informāciju no iekārtām, kas to spēj dot!

- **Tīkla iekārtas**
  - ✓ Maršrutētāji (router)
  - ✓ Gateway
  - ✓ Switch

Ziniet kas notiek datoros!

- **Programmu un servisu žurnālfaili**
  - ✓ Datubāžu žurnālfaili
  - ✓ Serveru žurnālfaili
  - ✓ Darbstaciju žurnālfaili

Antivīrusu programmas – ne tik drošas kā solīts!

- Efektivitāte pret jauniem vīrusiem - 10-20%
- Nav laicīgi atjaunotas
- Traucē un bremzē ikdienas darbus
- Nereaģē uz ārējo “spiegošanas” aparatūru

Droši glabājiet savāktos pierakstus!!

- **Svarīgus žurnālfailus neglabājiet tikai iekārtā, kas tos rada!**
  - ✓Saglabājiet žurnālfailus atsevišķā serverī!
  - ✓Izmantojiet protokolos SNMP, SSH, SFTP
  - ✓Ja iekārta šos protokolus neatbalsta – pārsūtiet tos citā veidā (e-mail utt.)

Nepazaudējiet pierakstus!!

- **Ierobežojiet piekļuvi žurnālfailu glabāšanas serverim!**
  - ✓Piekļuves tiesību kontrole
  - ✓Rakstošā iekārta nedrīkst pārrakstīt, dzēst, vai labot savus vai citus ierakstus!
- **Nodrošiniet pietiekami daudz vietas, lai varētu pārbaudīt datus arī pēc ilgāka laika!**

Par ko ziņot CERT.LV??

1. **Nesankcionēta piekļuve**:
   - ✓Fiziska vai loģiska, iepriekš nesaskaņota piekļuve pie organizācijas IT resursiem vai datiem
2. **Darbības**, kuru mērķis vai rezultāts ir IT resursu pieejamības traucēšana:
   - ✓ **DoS/DDoS**
   - ✓Nesankcionēta IT resursu pārslogošana, vai jebkuru citu metožu pielietošana, kas rezultējas servisa nepieejamībā.
3. **Ļaundabīga** programmatūra:
   - ✓Ļaundabīgas programmatūras sekmīgi uzstādīšanas gadījumi, kurus nav spējusi novērst pretvīrusu programmatūra
   - ✓ Ļaundabīgas programmātūras pieejamība no organizācijas IT resursiem

Par ko ziņot CERT.LV??

4. **Sociālā Inženierija (Social Engineering)**:
   - ✓Manipulācija ar mērķi izvilināt sensitīvu informāciju; bieži nemaz neiesaistot sarežģītas tehnoloģijas, bet gan pielietojot psiholoģijas metodes
   - ✓ Piemēram, uzbrucējs telefonsarunā izliekas par kādu personu, kurai upuris varētu uzticēt kādu “neizpaužamu” informāciju
   - ✓Retos gadījumos var būt arī fizisks kontakts

5. **CERT.LV** var ziņot arī par gadījumiem, kas Jums intuitīvi šķiet **aizdomīgi**

Esat piesardzīgi nevis bailīgi!

- Ar IT tehnoloģijām saistītos **riskus** iespējams **apzināt, novērtēt** un **vadīt**

- Laicīgi **sagatavojoties** iepējams **minimizēt** uzbrukuma ietekmi

- **Zināšanas** par savu datorsistēmu ļauj atrast rezerves darba **plānu**

- **Nebaidieties** par savām aizdomām **ziņot** CERT.LV!!

Dažas noderīgas adreses

Failu antivīrusu pārbaude- http://www.virustotal.com/
Pārlūkprogrammas drošības pārbaude - https://browsercheck.qualys.com/
Kaspersku Virus Removal- http://devbuilds.kaspersky-labs.com/devbuilds/AVPTool/
Bitdefender Rescue CD- http://kb.bitdefender.com/site/article/650/

Paldies!!!

Gints Mālkalnietis
E-pasts: gints@cert.lv
Tīmekļa vietne: http://www.cert.lv
Portāla Esi drošs tīmekļa vietne: http://www.esidross.lv
CERT.LV Twitter vietne: http://twitter.com/certlv