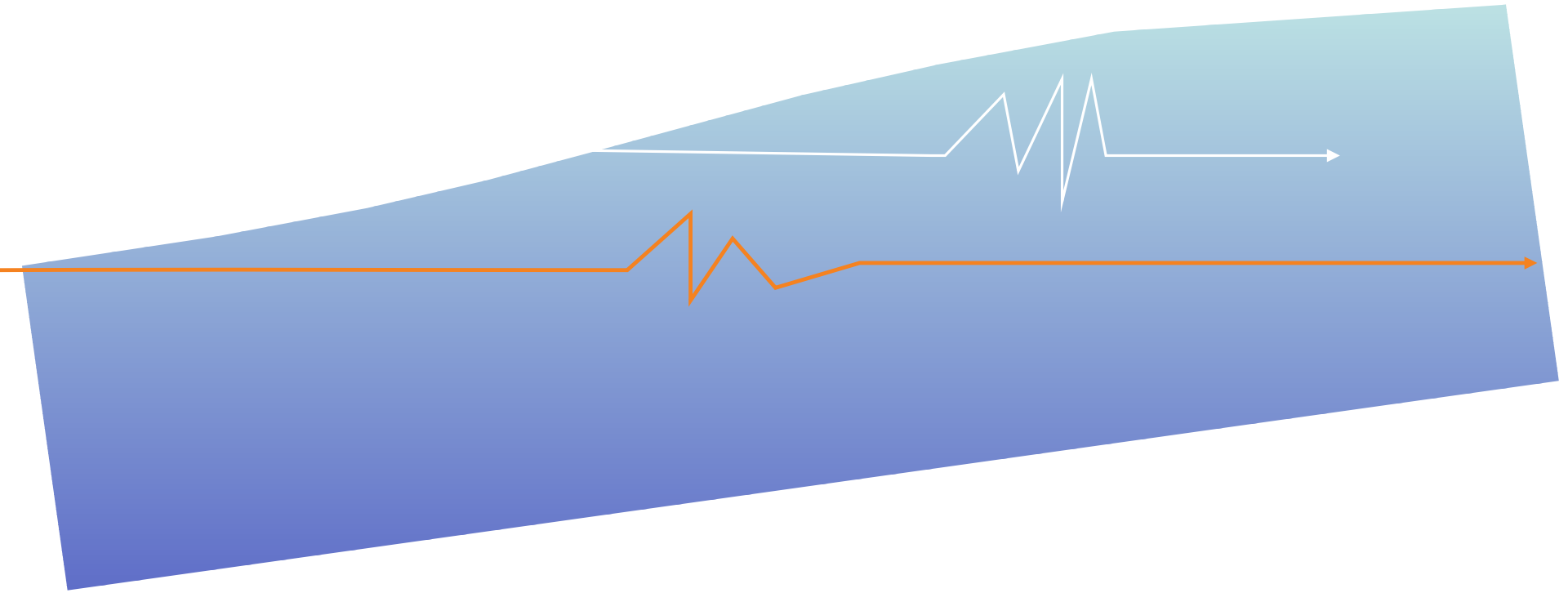
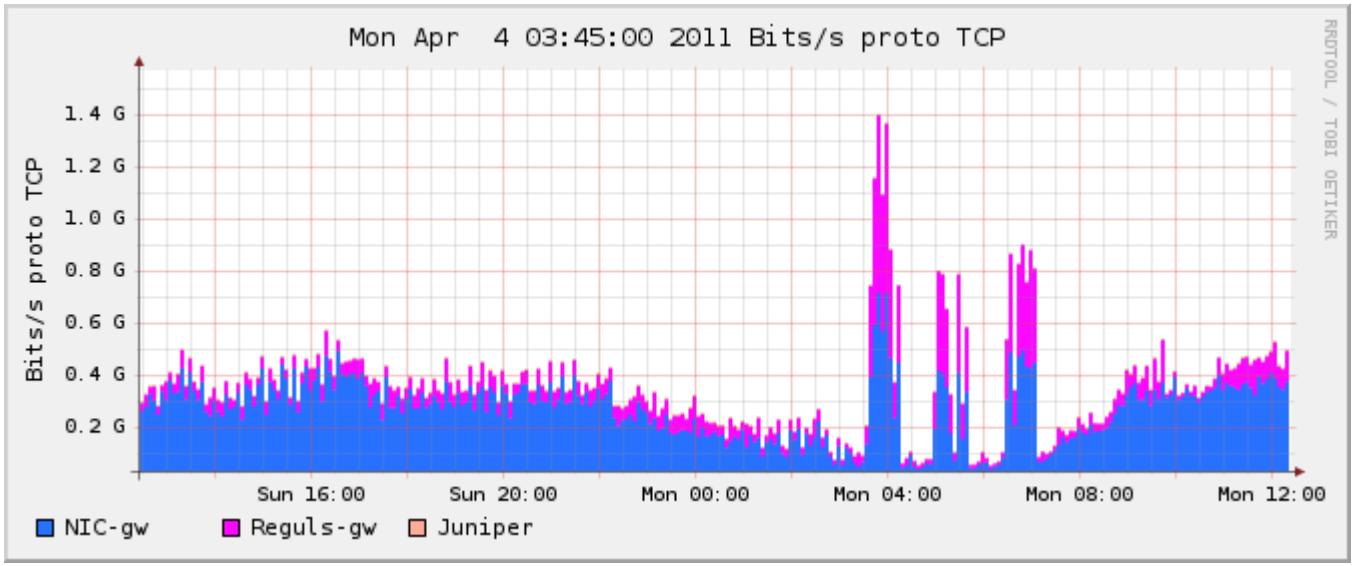
“Kā pamanīt drošības incidentu?”

Gints Mālkalnietis, CERT.LV



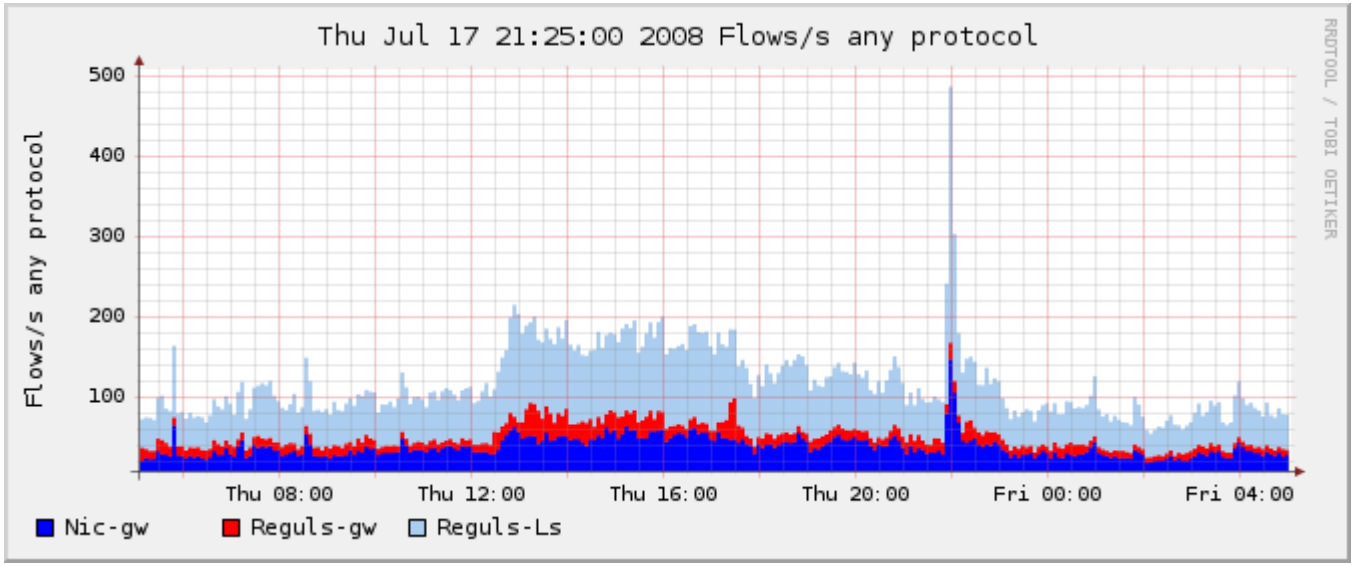
Vai mans datortīkls ir drošībā?

Iepazīstiet sava datortīkla ikdienas datu plūsmas!



Vai ir kādas izmaiņas?

Pievērsiet uzmanību datu plūsmām, kas izceļas



Analizējiet ilgtermiņa aktivitātes datortīklā!

Kāds ir jūsu iestādes datortīkla normāla darba grafiks?

Savāciet informāciju no iekārtām, kas to spēj dot!

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

Vērojiet, kas notiek datoros!

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

Brīdiniet par plānotajiem darbiem!

- Jauna servisa palaišana
- Iekārtu pievienošana
- Publiskas mājas lapas izvietošana
- Iekārtu vai programmu atjauninājumi
- Datortīkla konfigurācijas maiņa

Savāktos pierakstus glabājiet drošībā!

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

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**
- **Pārdomājiet, ko darīsiet, ja tiks pārsniegta servera ietilpība**

Automātiski analizējiet savāktos datus un izsūtiet brīdinājumus

- **Linux programmas:**
  Zabbix, BigBrother, MRTG, Nagios
- **Microsoft:**
  DC + Group Policy + komerciālas programmas (Hyena)

Nenoguliet incidenta sākumu!

- **Automātisko sistēmu sensoriem jābūt noregulētiem atbilstoši datortīkla specifikai**
- **Tie nedrīkst būt arī pārāk jutīgi**
- **Rūpīgi izvēlēties trauksmes līmeni:**

✓**Viltus** trauksmes **notrulina** uzmanību!

✓Iespējams **nepamanīt īsto** uzbrukumu!

✓Visi ir **pieraduši** pie **“sarkanās lampiņas”!**

Personai, kas saņem šos brīdinājumus, uz tiem ir jāreaģē!

- **Nepazaudējiet** brīdinājumus pastkastītē!
- Vienmēr nosakiet **atbildīgo** par brīdinājumu apstrādi!
- Sagatavojiet **dokumentāciju** tā, lai to **izprastu** vairāk kā viens speciālists!
- Ziniet, **kam** ziņot standarta un nestandarta situācijās!

Tomēr tas neatbrīvo administratoru no regulāras savāktās informācijas analīzes!

- Automātiskā analīze pārbauda **tikai** tos notikumus, kas uzstādīti!
- **Jauna veida** uzbrukums var radīt neparedzamus kļūdu pierakstus!
- Uzbrucējs var **maskēties,** neuzkrītoši iekļaujoties pārējā datu plūsmā!

Neuzticieties svešiem failiem!

- Antivīrusi atpazīst **<20% jaunu** vīrusu!
- Tas, ka antivīrusu programma ir palaista, nenozīmē, ka tā **darbojas** kā paredzēts!
- Fails, ko atsūta jūsu kolēģis, varbūt jau ir **inficēts** viņa mājas datorā!
- **ĻOTI** neuzticieties failiem, ko neesat pieprasījuši!
  - ✓ja fails nav sensitīvs – ātrai pārbaudei izmantojiet www.virustotal.com
  - ✓Savlaicīgi atjaunojiet programmas un to komponentes (Adobe Acrobat Reader u.c.)

Par ko ziņot CERT.LV?

1. **Nesankcionēta piekļuve**:
   - ✓Fiziska vai loģiska, iepriekš nesaskaņota piekļuve pie organizācijas IT resursiem vai datiem
1. **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.
1. **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?

1. Nesankcionēti **piekļuves mēģinājumi** resursiem, kas uzskatāmi par īpaši uzraugāmiem:
   - ✓Jebkuri mēģinājumi identificēt IT resursu.
   - ✓ Atvērto portu, protokolu un servisu skenēšana un mēģinājumi piekļūt resursam.
1. **Pikšķerēšana (Phishing)**:
   - ✓Darbības, ar kuru palīdzību tiek veikti mēģinājumi izkrāpt sensitīvus datus, tādus kā paroles, lietotājvārdus, kredītkaršu un kontu inforāciju utt., izliekoties par kādu resursu, kam upuris varētu uzticēt šādu informāciju, piemēram, par internet bankas web lapu vai citu pakalpojumu sniedzēju, kur nepieciešama lietotāja autorizācija/autentifikācija.
   - ✓ Šīs darbības parasti tiek veiktas ar e-pastu vai citu rakstisku elektronisko komunikācijas līdzekļu starpniecību.

Par ko ziņot CERT.LV?

1. **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.
   - ✓ Augstāk minētā pikšķerēšana arī ir viena no sociālās inženierijas tehnikām.
1. CERT.LV var ziņot arī par gadījumiem, kas Jums intuitīvi šķiet **aizdomīgi**

Kāda informācija būtu jāuzrāda ziņojumā par incidentu?

- ✓Organizācijas nosaukums
- ✓Kontaktpersona (vārds un uzvārds, e-pasts, telefons)
- ✓Incidenta tips un īss apraksts
- ✓Indienta laiks un datums, ja nav zināms, tad laiks un datums uz konstatācijas brīdi
- ✓Avota IP adrese, izmantotie protokoli un porti
- ✓Galamērķa IP adrese, izmantotie protokoli un porti
- ✓Log/žurnāl failu fragmenti, kas attiecās uz incidentu, vai pilns žurnālfailu saturs
- ✓Operētājsistēma – versija
- ✓Kompromitētās sistēmas, resursa, programmatūras funkcija (web serveris, FTP serveris, darbstacija, maršrutētājs, utt.)
- ✓Lietotā pretvīrusu programmatūra – nosaukums, versija, kad veikti atjauninājumi
- ✓Sistēmas fiziskā atrašanās vieta
- ✓Kā ir identificēts incidents
- ✓Kādas ir icidenta radītās sekas
- ✓Ja incidents ir jau novērsts/atrisināts, tad kādiem līdzekļiem un kad

Esiet piesardzīgi nevis bailīgi!

- Ar IT tehnoloģijām saistītos **riskus** iespējams **apzināt, novērtēt** un **vadīt**
- Savlaicīgi **sagatavojoties,** iespējams **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-
www.virustotal.com

Pārlūkprogrammas drošības pārbaude -
https://browsercheck.qualys.com/

Kaspersky Virus Removal-
http://devbuilds.kaspersky-labs.com/devbuilds/AVPTool/

Bitdefender Rescue CD-
http://kb.bitdefender.com/site/article/650/

Paldies par uzmanību!

http://ww.cert.lv/

cert@cert.lv

gints@cert.lv