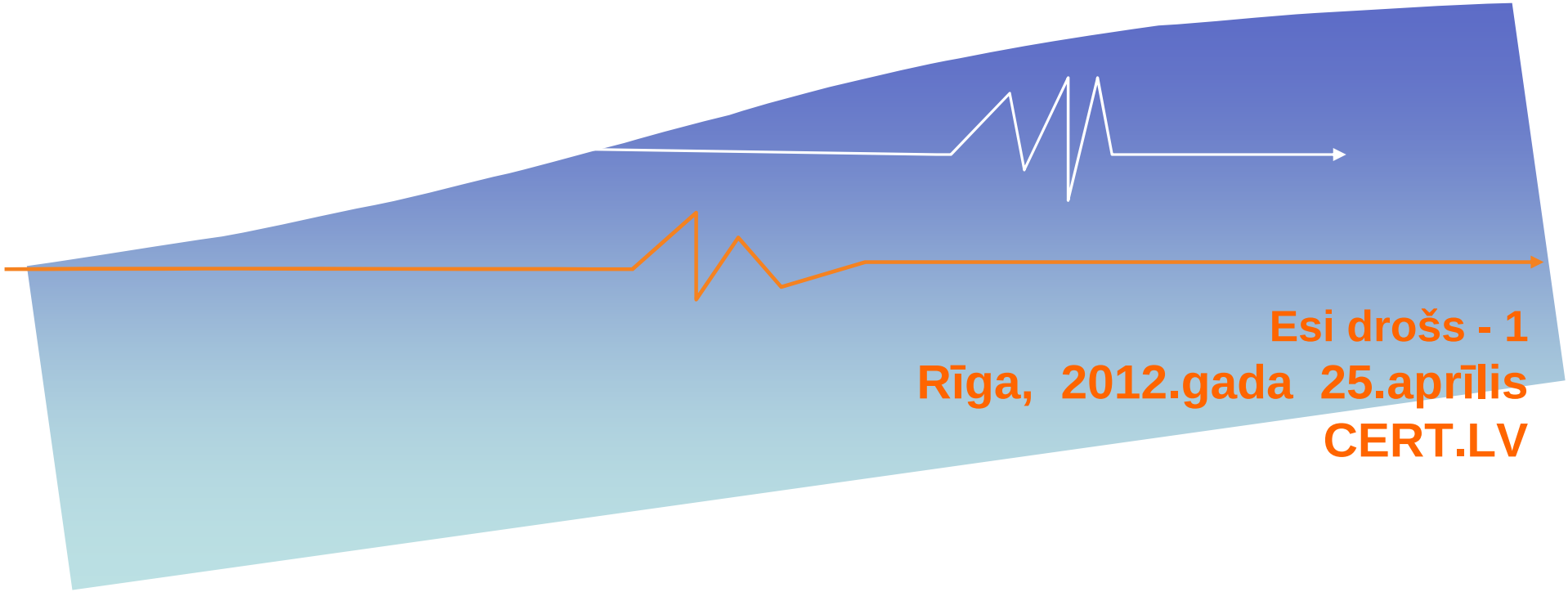
# *“Kā pamanīt drošības incidentus?”*

Gints Mālkalnietis, CERT.LV



**Esi drošs - 1**

**Rīga, 2012.gada 25.aprīlis**

**CERT.LV**

# Analizējiet ilgtermiņa aktivitātes datortīklā!

# Vērojiet 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

# Droši glabājiet savāktos pierakstus!!

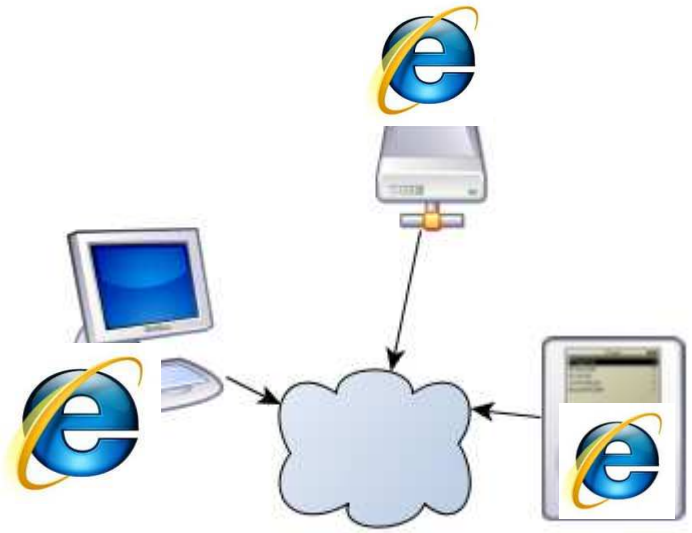
- **Svarīgus žurnālfailus neglabājiet tikai iekārtā, kas tos rada!**
  - ✓Saglabājiet žurnālfailus atsevišķā serverī!
  - ✓Izmantojiet protokolos SNMP, SSH, SFTP
  - ✓Ja iekārta šos protokolus neatbalsta – pārsūtiet tos citā veidā (e-mail utt.)

# 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!**

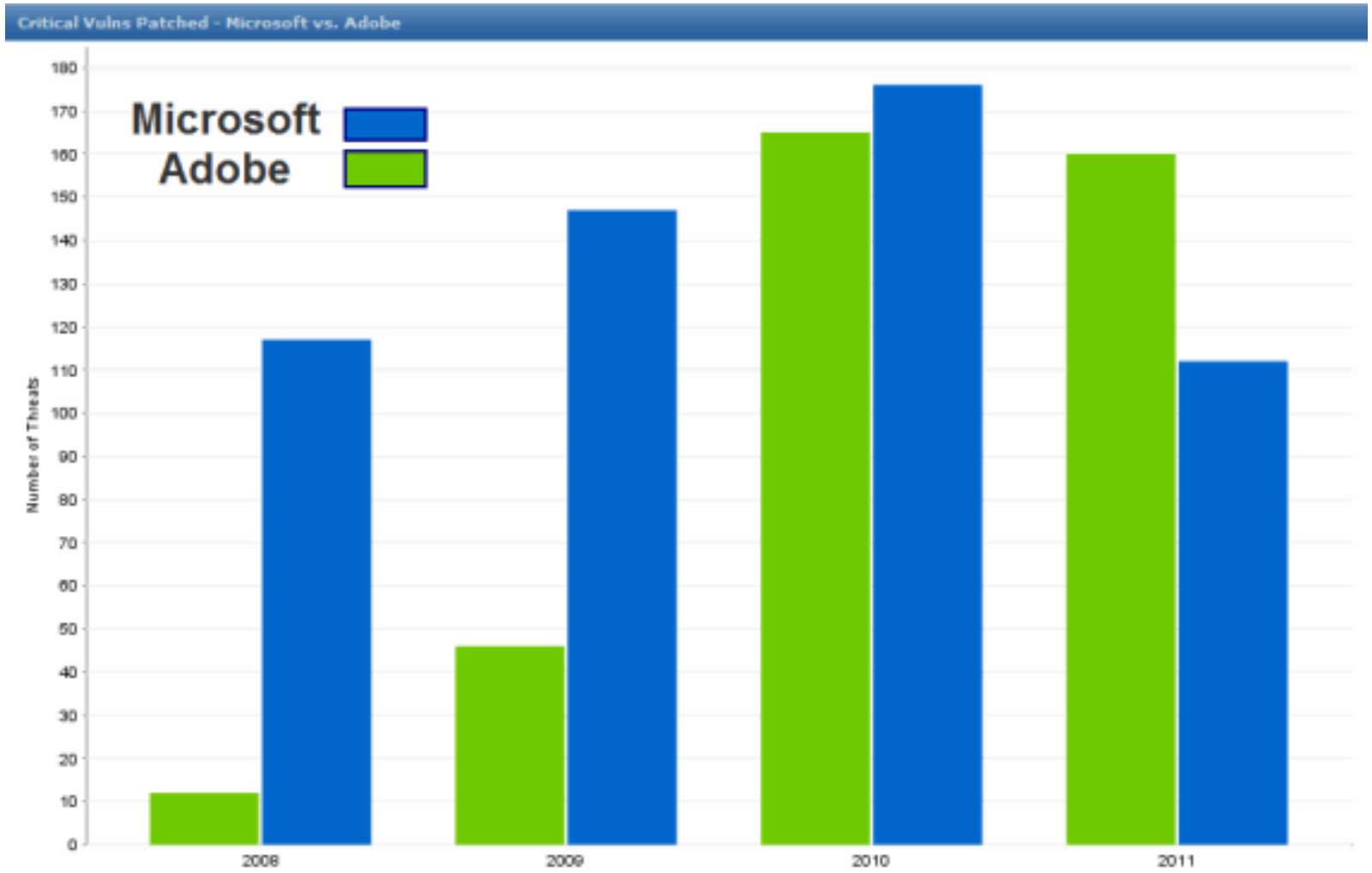
# Tehnoloģijas mainās – riski paliek!!

- Interneta pārlūks – jaunais dators
- Veiksmīgs uzbrukums pārlūkam – pilnīga kontrole pār lietotāja datiem
- Dažādas ierīces – viena ievainojamība



# Tehnoloģijas mainās – riski paliek!!

- Lietotāja dators– jaunais serveris
- Vienmēr – pievienots internetam
- Parasti – ar novecojušām, nelabotām programmām
- Dažreiz – ar pārāk lielām lietotāja pilnvarām veikt tajā izmaiņas



Critical Vulns Patched - Microsoft vs. Adobe
Microsoft
Adobe
Number of Threats
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
2008
2009
2010
2011

# 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

# Antivīrusu programmu efektivitātes pavairošana

1. Antivīrusu programma = pēdējais datora aizsardzības līmenis
2. Atvieglojiet tā darbu ar vispārēju datortīkla drošības uzstādījumu sakārtošanu!
3. Izmantojiet operētājsistēmas iespējas ierobežot nezināmu programmu izpildi
4. Atslēdziet automātisku programmu izpildi no noņemamjiem datu nesējiem
5. Izmantojiet centralizētu antivīrusu vadību

# Kur slēpjas datorvīrusi?

1. Ļaundabīgu kodu saturošas interneta vietnes
   - ✓Izveidotas apzināti
   - ✓Apmeklētāji tiek pievilināti caur SEO
   - ✓Saites forumos, komentāros, Twitter
2. Uzlauztas labdabīgas interneta vietnes
   - ✓ SQL injekcijas
   - ✓Novecojušas satura vadības sistēmas
   - ✓Kļūdas lapas kodā
   - ✓Kļūdas reklāmas plūsmu sistēmās
3. Noņemamie datu nesēji:
   - ✓USB zibatmiņa
   - ✓Nezināms izcelmes CD
   - ✓Navigācijas iekārtas (TomTom, Garmin utt.)
   - ✓Citas iekārtas ar iebūvētu datu krātuvi – GSM modēmi, mobilie telefoni, mūzikas atskaņotāji

# Kur slēpjas datorvīrusi?

4. E-pastā saņemti dokumenti un saites
5. Tīkla iekārtas
6. Biroja tehnika
   - ✓Printeri – satur operētājsistēmu Windows 2000 vai Linux speciālas versijas
   - ✓“Smart TV” – gandrīz pilnvērtīgs dators ar Linux OS
   - ✓Dažādas specializētas mēriekārtas, medicīnas aparatūra

# 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)**
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** iespējams **minimizēt** uzbrukuma ietekmi

•**Zināšanas** par savu datorsistēmu ļauj operatīvi veidot rezerves darba plūsmu

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

# Dažas noderīgas adreses

Failu antivīrusu pārbaude-
http://www.virustotal.com/
Pārlūkprogrammas drošības pārbaude -
https://browsercheck.qualys.com/
F-Secure Rescue CD
http://www.f-secure.com/en/web/labs_global/removal/rescue-cd
Atvērtā koda programmatūra:
http://atveries.lv

# 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