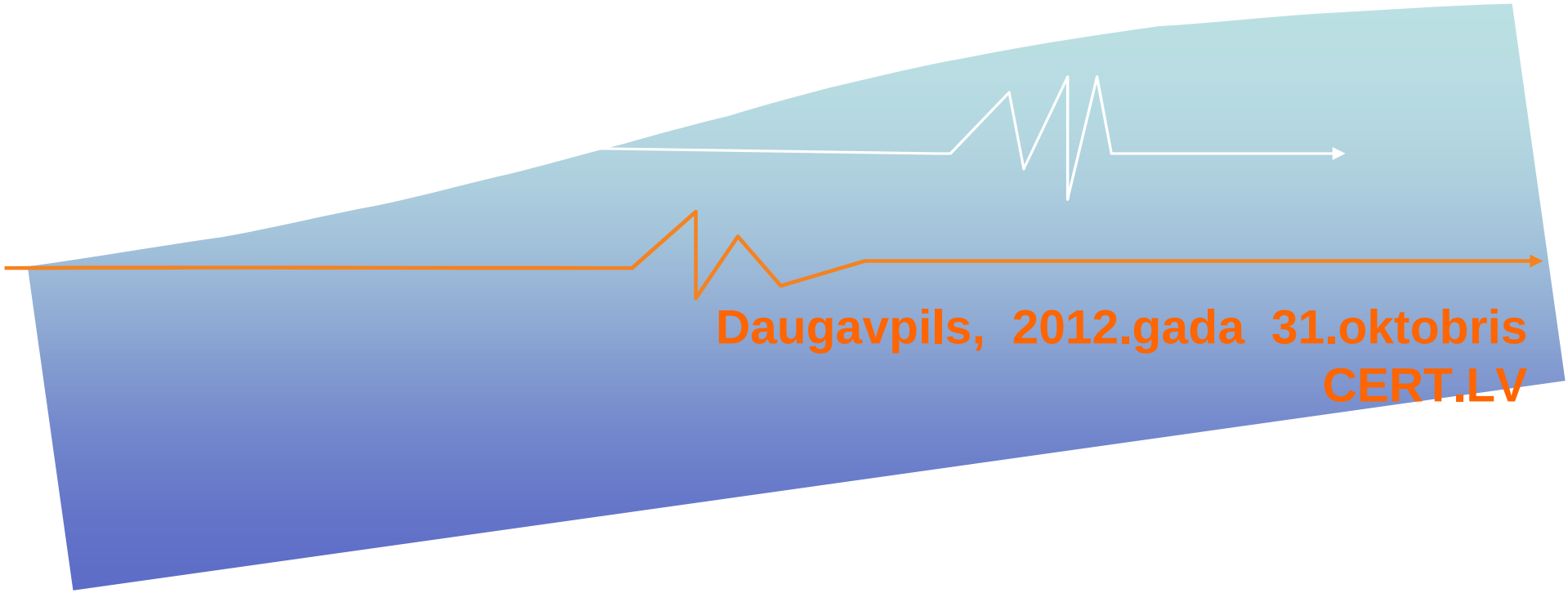
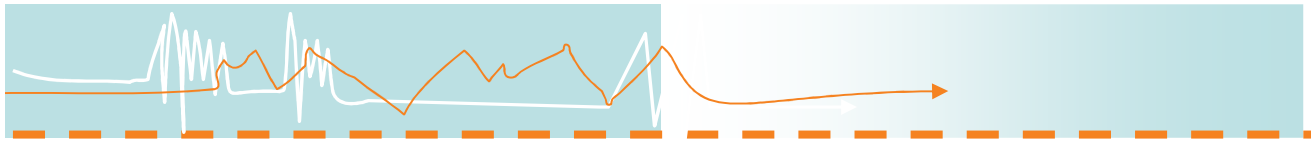
“Kā pamanīt drošības incidentu?”

Gints Mālkalnietis, CERT.LV



Daugavpils, 2012.gada 31.oktobris
CERT.LV



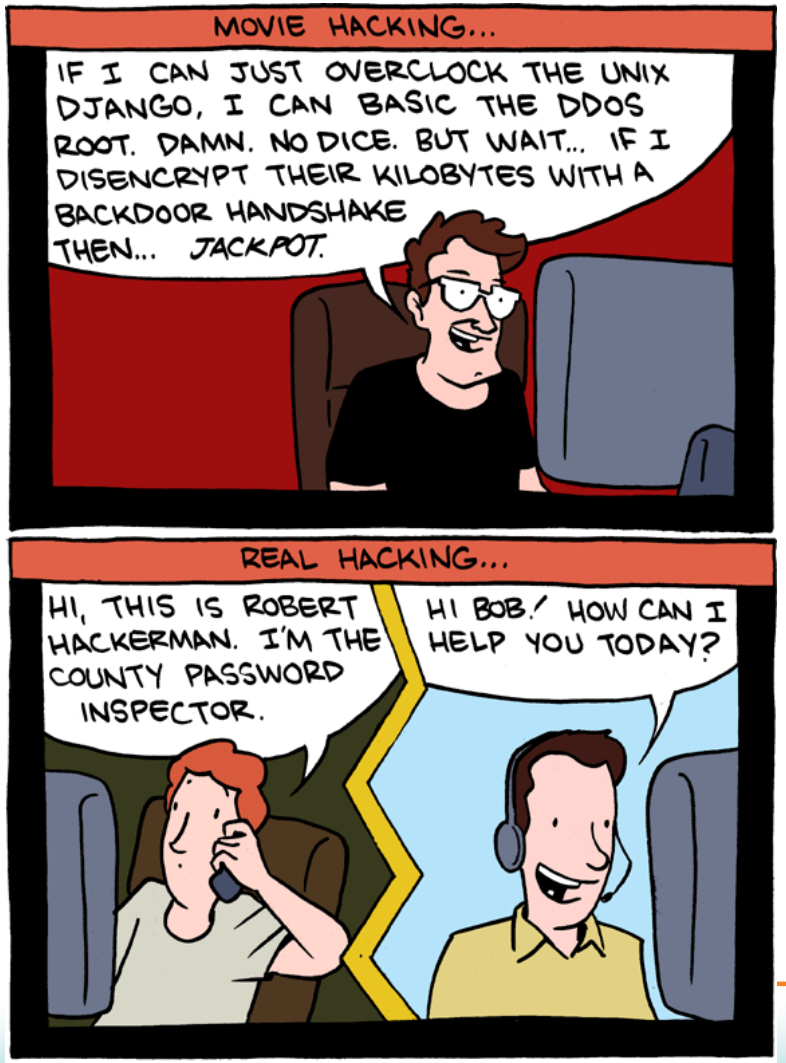
CERT.LV

Saturs

- Riski mūsdienu tehnoloģijām
- Nedaudz par datorvīrusiem
- Īsi par robotu tīkliem
- Dažas noderīgas lapas

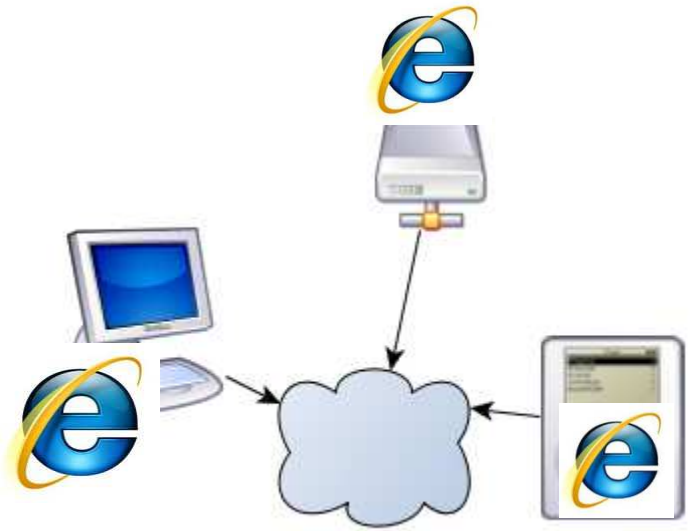
Riski mūsdienu tehnoloģijās

- Neviens drošības tehniskais risinājums nav 100% drošs!



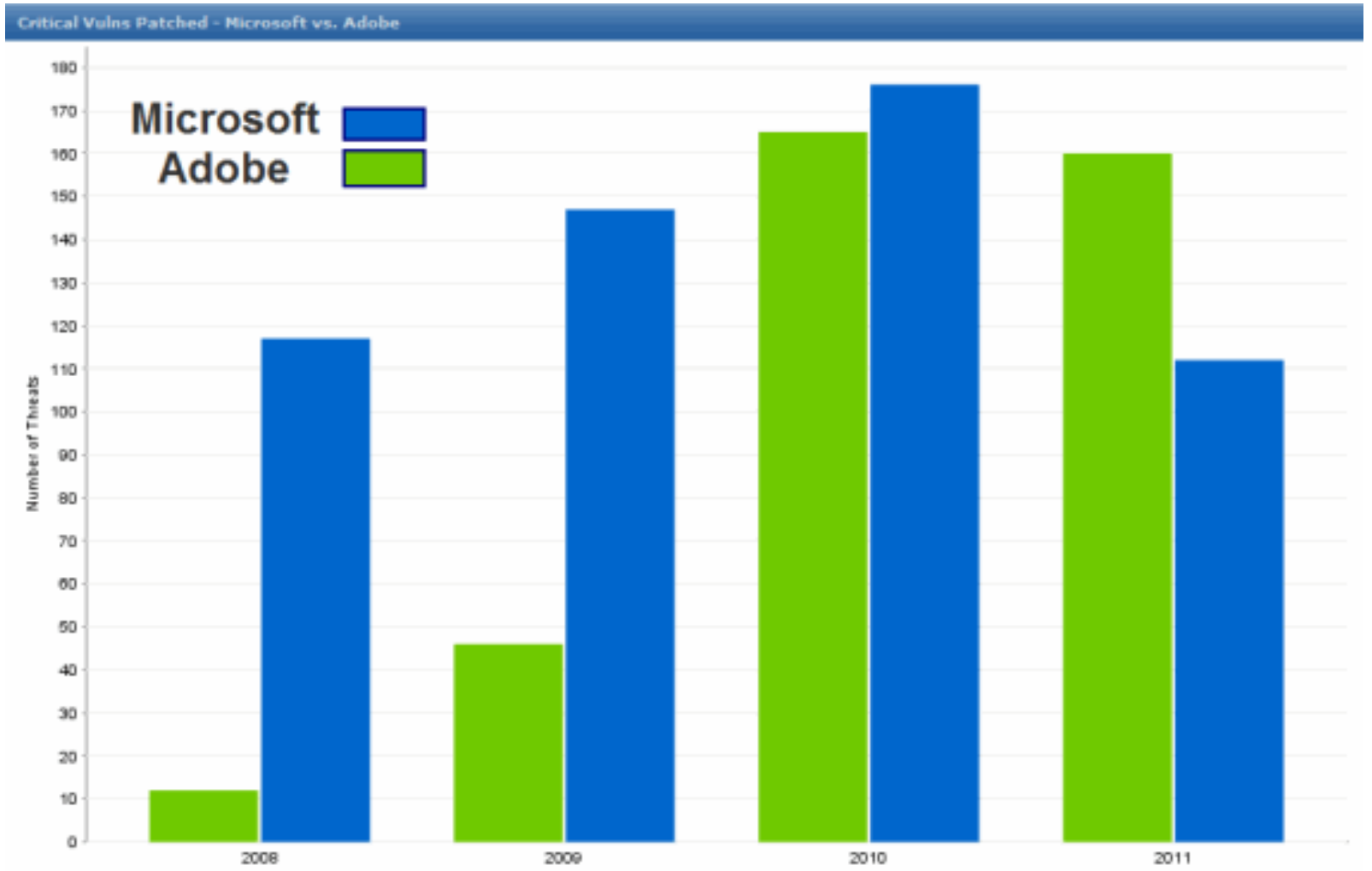
Interneta pārlūks = dators (OS + aplikācija)

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



Jebkurš dators = serveris

- Veiktspēja > kā 5 gadus vecam serverim
- 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

Jebkurš tīkls => internets?

- Jānodala publiski izmantojamie datortīkli no iekšējiem tīkliem
- Ne visiem datoriem ir nepieciešama piekļuve internetam
- Publisks WiFi – piekļuve tikai internetam, ne iekšējam organizācijas tīklam!
- Nomainiet rūpnīcu noklusētos uzstādījumus!

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!**

Datu “mākonis” – neglābj no vecām kļūdām!

• 2009 – Vairāk kā 300 dokumentu par TWITTER biznesa plāniem tika nozagti no Google Apps. Iemesls – vāja parole.
• 2010 – Izveidota programma WiFi paroļu uzlaušanai, izmantojot Amazon E2 Cloud
• 2011 – Amazon E2 Cloud tiek izmantot uzbrukumā Sony PSN
• 2011 – Dropbox kļūdas pēc uz vairākām stundām atslēdz autentifikācijas pārbaudi = iespējams lejuplādēt jebkuru failu

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

Antivirus	Result	Update
AhnLab-V3	-	20120410
AntiVir	-	20120411
Antiy-AVL	-	20120411
Avast	-	20120411
AVG	-	20120411
BitDefender	-	20120411
ByteHero	-	20120407
CAT-QuickHeal	-	20120411
ClamAV	-	20120411
Commtouch	-	20120411
Comodo	-	20120411
DrWeb	-	20120411
Emsisoft	-	20120411
eSafe	-	20120408
eTrust-Vet	-	20120411
F-Prot	-	20120410
F-Secure	-	20120411
Fortinet	-	20120411
GData	-	20120411
Ikarus	-	20120411
Jiangmin	-	20120411
K7AntiVirus	-	20120410
Kaspersky	-	20120411
McAfee	-	20120411
McAfee-GW-Edition	-	20120410
Microsoft	-	20120411
NOD32	-	20120411
Norman	-	20120411
nProtect	-	20120411
Panda	-	20120410
PCTools	-	20120411
Rising	-	20120411
Sophos	-	20120411
SUPERAntiSpyware	-	20120402

SHA256: b0c4b0379402045512a9b

File name: x.docx

Detection ratio: 0 / 42

Analysis date: 2012-04-11 11:41:05 UTC

- Programmēšanas laiks < 30 minūtes
- Profesionāli kaitīgā koda veidotāji izmanto automatizētus rīkus sava koda slēpšanai
- “Svaiga” datorvīrusa variācija katru dienu

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 noņemamajiem datu nesējiem
5. Izmantojiet centralizētu antivīrusu vadību

Kur slēpjas datorvīrusi? (1)

1. Ļaundabīgu kodu saturošās interneta vietnēs
   - ✓Izveidotas apzināti
   - ✓Apmeklētāji tiek pievilināti caur SEO
   - ✓Saites forumos, komentāros, Twitter
2. Uzlauztās, labdabīgās interneta vietnēs
   - ✓ SQL injekcijas
   - ✓Novecojušas satura vadības sistēmas
   - ✓Kļūdas lapas kodā
   - ✓Kļūdas reklāmas plūsmu sistēmās
3. Noņemamajos datu nesējos:
   - ✓USB zibatmiņa
   - ✓Nezināms izcelsmes CD
   - ✓Navigācijas iekārtas (TomTom, Garmin utt.)
   - ✓Citas iekārtas ar iebūvētu datu krātuvi – GSM modemi, mobilie telefoni, mūzikas atskaņotāji

Kur slēpjas datorvīrusi? (2)

1. E-pastā saņemtajos dokumentos un saitēs
2. Tīkla iekārtās
3. Biroja tehnikā
   - ✓ Printeri – satur operētājsistēmu Windows 2000 vai Linux speciālas versijas
   - ✓ “Smart TV” – gandrīz pilnvērtīgs dators ar Linux OS
   - ✓ Dažādas specializētas mēriekārtas, medicīnas aparatūra

Robotu tīkls

- Robotu tīkls = standarta lietotāja mājas/ofisa dators + uzlauztie serveri
- Lietotāja datori visbiežāk tiek inficēti, apmeklējot kaitīgu kodu saturošas mājas lapas
- Tiek izmantotas interneta pārlūkprogrammu un to papildinājumu ievainojamības
- Skaits nepārtraukti svārstās
- Tiek izmantoti “application layer” uzbrukumiem citām sistēmām, mēstuļu izsūtīšanai
- Var vākt dažādus lietotāja datus

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 antivīrusu programmatūra
   ✓ Ļaundabīgas programmatūras pieejamība no organizācijas IT resursiem

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

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

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