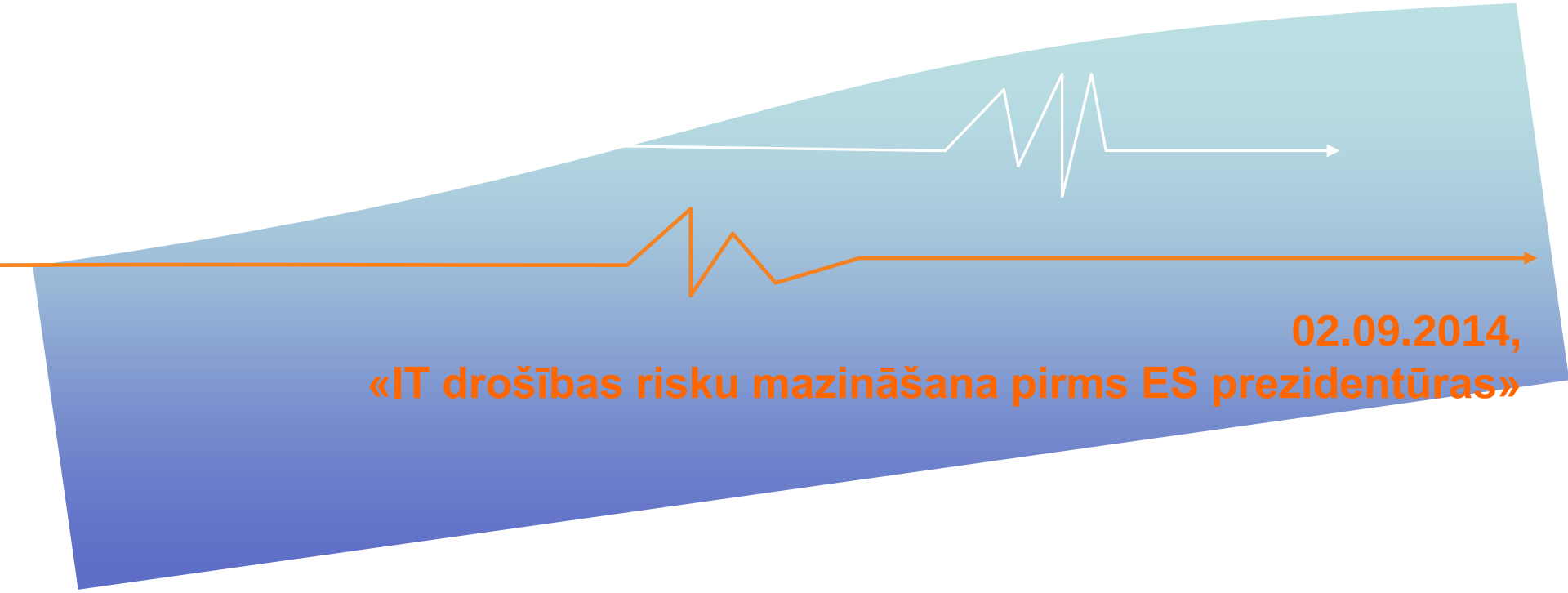
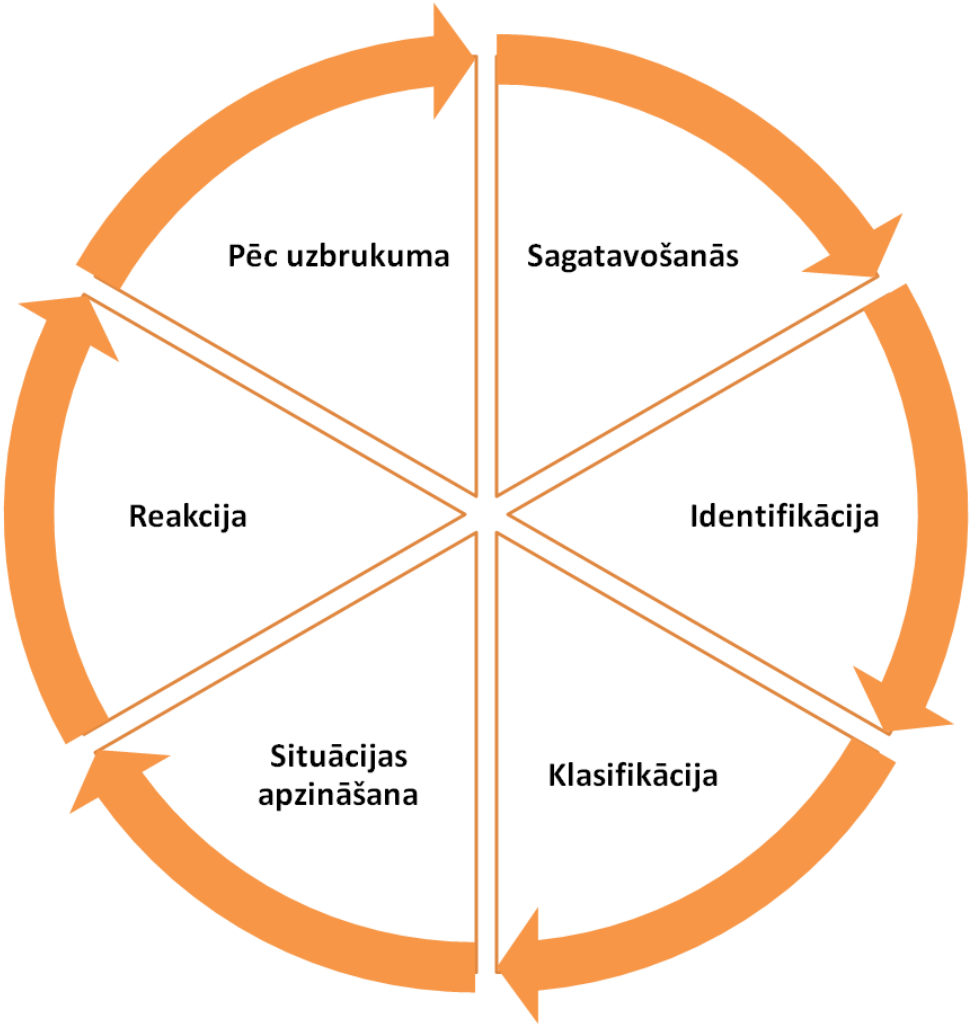
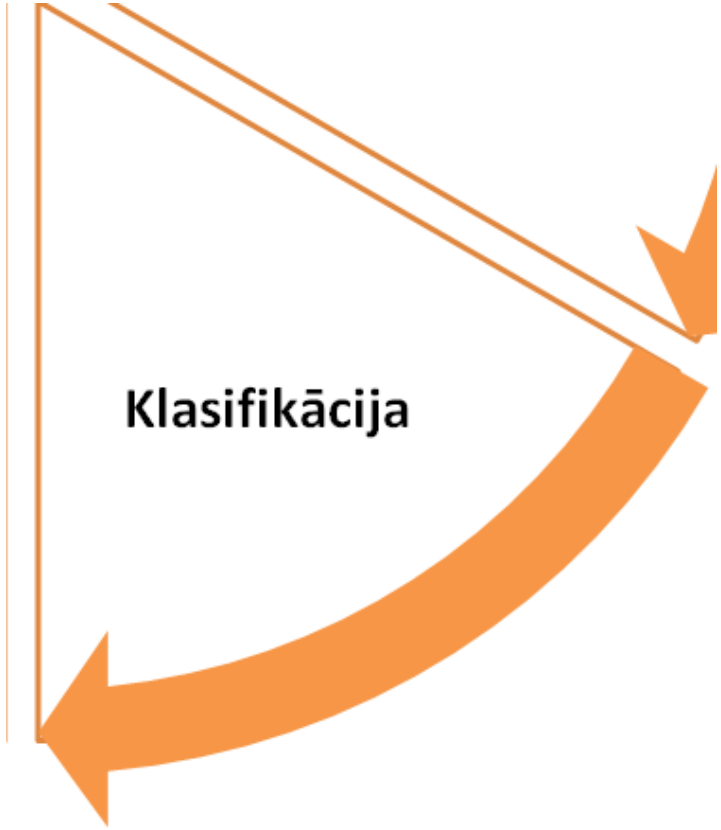
# *Uzbrukumu klasifikācija*

Gints Mālkalnietis, CERT.LV



**02.09.2014,**
**«IT drošības risku mazināšana pirms ES prezidentūras»**


Pēc uzbrukuma
Sagatavošanās
Identifikācija
Klasifikācija
Situācijas apzināšana
Reakcija


Klasifikācija

# Uzbrukumu veidi

- Kompromitētas iekārtas
- Pikšķerēšana
- Ļaundabīgs kods
- Piekļuves lieguma uzbrukumi

# Uzbrukumu veidi

- Kompromitētas iekārtas

➢ **Cēloņi:**

✓ Novecojušas, nedrošas programmatūras versijas
✓ Konfigurācijas kļūdas (standarta paroles, ieslēgti nevajadzīgi servisi)
✓ Piekļuves datu zādzība (bieži – paroles nozagtas no administratora datora)
✓ Vairākkārt izmantotas paroles
✓ Jaunatklātas ievainojamības

➢ **Risinājumi:**

✓ Iekārtu regulāra atjaunināšana, novecojušu iekārtu izslēgšana no datortīkla
✓ Standartizētu, drošu konfigurāciju izveide un ieviešana
✓ Pārdomāta paroļu izmantošana politika, vairākfaktoru autentifikācijas mehānismu izmantošana

# Uzbrukumu veidi

- Pikšķerēšana

➢ **Cēloņi:**

✓ Nepietiekama lietotāju informētība

✓ Nesakārtota e-pasta sistēma (bez SPF ierakstiem, bez specificētiem atļautajiem SMTP serveriem)

✓ Nedroša programmatūra uz lietotāja datora

➢ **Risinājumi:**

✓ Darbinieku izglītošana

✓ SPF un citu ierobežojošo mehānismu ieviešana

✓ Laicīgi atjaunināt programmatūru, ierobežot lietotāja tiesības izpildīt kodu no interneta vietnēm

# Uzbrukumu veidi

- Ļaundabīga koda izpilde

➢ **Cēloņi:**

✓ Nepietiekama lietotāju informētība
✓ Nedroša programmatūra uz lietotāja datora
✓ Pārāk plašas tiesības izpildīt nezināmu kodu

➢ **Risinājumi:**

✓ Darbinieku izglītošana
✓ Laicīgi atjaunināta programmatūra, ierobežotas lietotāja tiesības
✓ E-pasta pielikumu filtri
✓ Ierobežot programmu izpildi no pārnēsājamiem datu nesējiem

# Sekmīga DOS mērķi

- Uzbrucēju mērķis ir tikai viens – traucēt datorsistēmas darbību, neļaut izmantot tās uzturētos pakalpojumus!
- Visi līdzekļi ir labi, ja tiek panākts vēlamais rezultāts!
  - Uzbrukums ir sekmīgs, ja pakalpojumu sniegšana tiek traucēta “aizsardzības” pasākumu rezultātā
  - Kopējo sistēmas veiktspēju ietekmēs tās vājākais posms
  - Izslēgts serveris = veiksmīgs DOS

# Level7 (aplikāciju) DOS mērķi

**VoIP servisi:**

- ✓ Uzbrukuma mērķi – VoIP kontrolieri un individuāli VoIP termināli
- ✓ Ievainojamības VoIP sistēmās un to konfigurācijās tiek meklētas vairākiem mērķiem:

1)Veikt zvanus uz sveša rēķina
2)Noklausīties sarunas
3)Traucēt pakalpojuma darbību

- **Risinājumi:**
- ✓ Konfigurāciju pārbaude
- ✓ Ugunssiena

# Level7 (aplikāciju) DOS mērķi

**WEB aplikācijas:**

- ✓ Specifiski pieprasījumi  patērē daudz servera resursu
- ✓ Ikdienas darbā lietotāji tos veic ļoti reti, tāpēc veiktspējas zudumi nav pamanīti
- ✓ Pēkšņa, masveidīga, pieprasījumu veikšana traucē sistēmas darbību
- **Risinājumi:**
- ✓ Rūpīga veiktspējas testēšana
- ✓ Pareiza servera konfigurācija

# Level7 (aplikāciju) DOS mērķi

**Autentifikācijas un sesiju pārvaldības mehānismi**

- ✓ Šifrēta informācijas kanāla izveide patērē daudz servera resursu
- ✓ Neveiksmīga sesiju pārvaldības mehānisma izvēle ierobežo to skaitu, pat tad, ja pārējie servera resursi ir pietiekami
- ✓ Tiek bloķēti leģitīmu lietotāju konti
- **Risinājumi:**
- ✓ Vairākfaktoru autentifikācija
- ✓ Pareiza servera konfigurācija

# Level7 (aplikāciju) DOS mērķi

- **GIS serveri**
- ✓ Reti lietoti, daudz jaudas patērējoši serveri
- ✓ Domāti darbinieku ikdienas pienākumu veikšanai, bet dažreiz sasniedzami no interneta
- ✓ Iespējamas SQL injekcijas un datu modifikācijas
- **Risinājumi:**
- ✓ Firewall
- ✓ Pārbaudīt un atjaunot programmatūru

# Noklusētās vērtības

- Standarta konfigurācijā programmām pieejamie resursi var būt stipri limitēti:
  - ✓ Default Ubuntu: ulimit –a = 1024 – noslogotā serverī šis limits ātri tiek pārniegts
  - ✓ MySQL max connections =151 (Linux, Solaris spēj uzturēt 1000-10000 konekcijas, Windows <2048)
  - ✓ Apache: ServerLimit 16 StartServers 2 MaxClients 150 MinSpareThreads 25 MaxSpareThreads 75 ThreadsPerChild 25

- Sistēmas veiktspēju noteiks vājākais elements!
- Viens HTTP pieprasījums webserverim var radīt vairākus desmitus pieprasījumu datubāzei!
- Reti lietotas web aplikācijas var labi strādāt ikdienas režīmā, bet ļoti noslogot serveri, apstrādājot specifiskus pieprasījumus – laba iespēja veikt DOS uzbrukumu

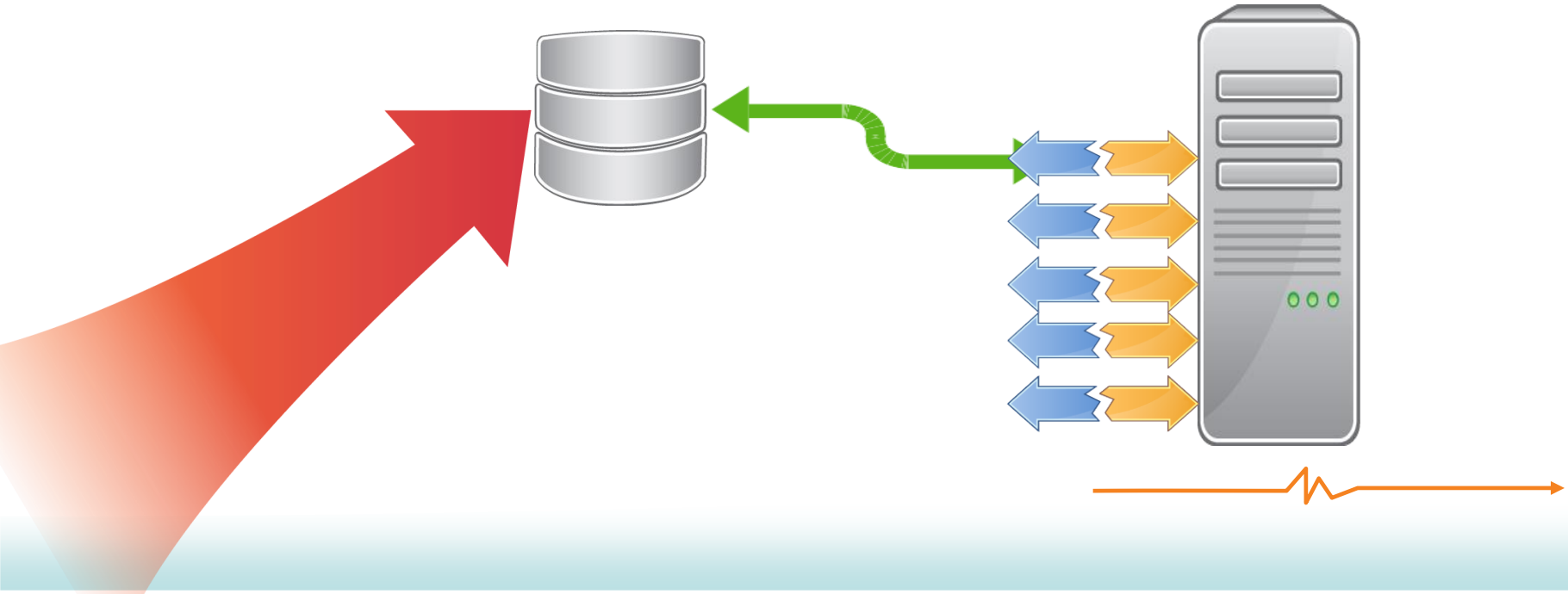
# Aizsardzības iekārtu ietekme

- Iekārtas, kas filtrē un analizē ienākošo datu plūsmu, var būtiski PALIELINĀT DOS risku, jo datu analīzei izmanto daudz resursus.

Pietiekami jaudīgas iekārtas mēdz būt ļoti dārgas.

# Aizsardzības iekārtu ietekme

- Nepareizi konfigurēts HTTP pieprasījumu cache serveris var uzturēt ievērojami mazāk lietotāju pieprasījumu nekā tā “aizsargātais” webserveris.



# Neievainojamu datorsistēmu nav!

- Jebkura reāla datorsistēma satur daudz, dažādu komponenšu
- Jaunatklātu ievainojamību labošanas laiks nav iepriekš zināms
- Nopietnu, bet nesalabotu ievainojamību gadījumā, datorsistēmas īpašniekiem rodas dilemma:
  1. Turpināt izmantot sistēmu ar zināmu ievainojamību
  2. Neizmantot/ierobežot datorsistēmu līdz labojuma ieviešanai

# Pagaidu risinājumi

- Ražotāji piedāvā dažādus risinājumus operatīvai ievainojamību ietekmes novēršanai:
  1. Uzbrukumu ierobežošana, izmantojot ugunsmūru un DPI iekārtas – tiek analizēti ienākošie dati, bloķējot zināmu uzbrukumu indikatorus saturošas paketes.
  2. “Virtual patching” serverī - papildus programmas, kas pārtver/labo ienākošos pieprasījumus pirms nodošanas tālākai apstrādei
  3. Papildinājumi/filtri esošajām programmām

# Ievainojamības ietekmes izvērtēšana

- Kritiskas ievainojamības, kas atklāj sensitīvus datus, ilgtermiņa ietekmi ir sarežģīti izvērtēt:
  1. Bieži nav precīzi zināms ievainojamības atklāšanas laiks (tas var atšķirties no publiski zināmā)
  2. Žurnālfaili var nesaturēt informāciju, kas nepieciešama, lai konstatētu sekmīga uzbrukuma faktu
  3. Sekmīgs uzbrukums var atklāt piekļuves datus citām, neievainotām sistēmām.

# Ievainojamības ietekmes izvērtēšana

- Savstarpēji saistītas datorsistēmas:
  1. Savstarpēji saistītu datorsistēmu ietekme praktiski ir daudz lielāka, nekā plānots, tās veidojot.
  2. “Vienvirziena” komunikāciju modelis būtiski ietekmē nepieciešamo funkciju realizāciju, tāpēc praksē tiek izmantots ļoti reti.
  3. Pilnīga datorsistēmu komunikāciju apzināšana un dokumentēšana ir sarežģīta un laikietilpīga!

# 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