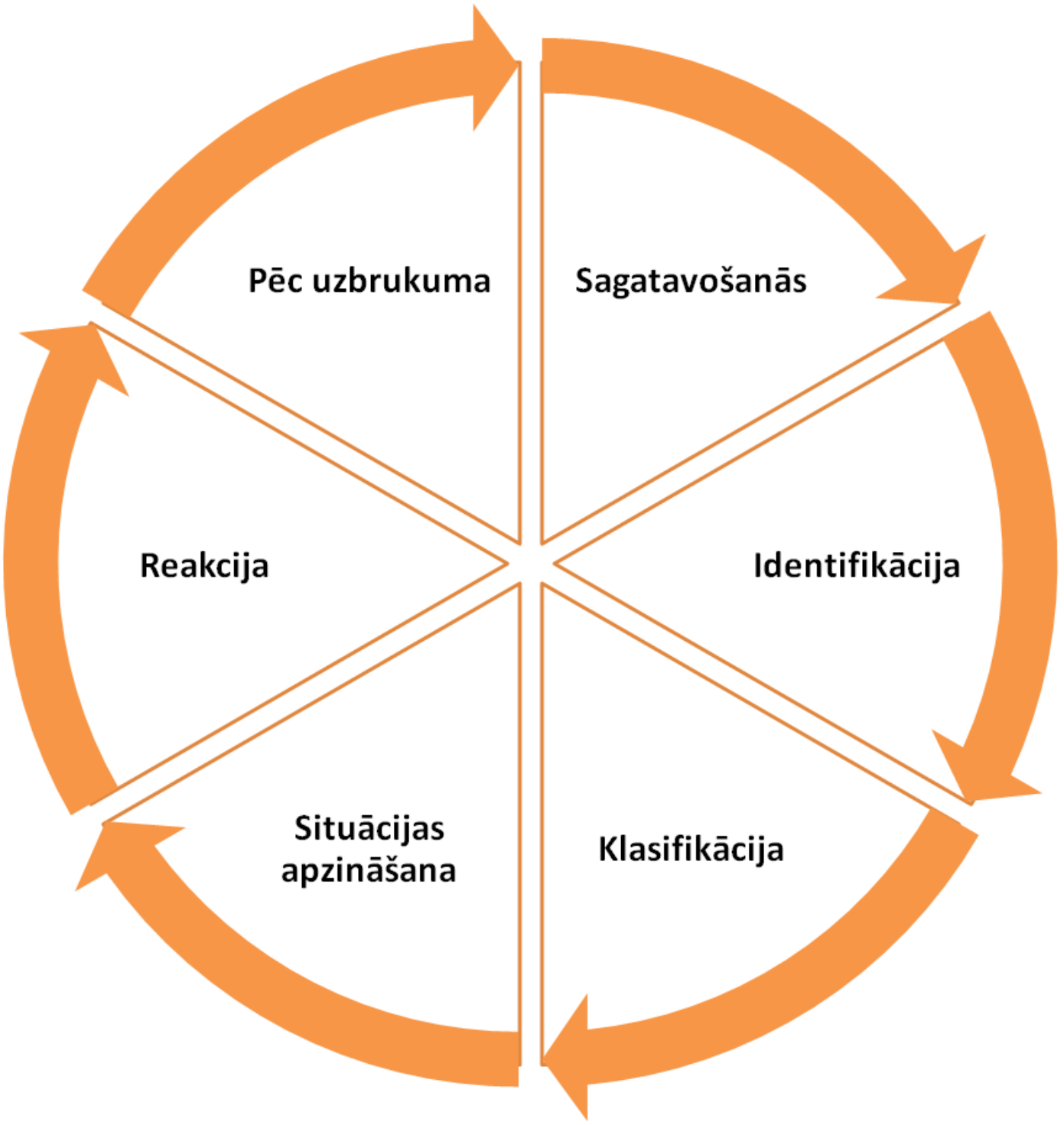
Uzbrukumu identifikācija

02.09.2014,

«IT drošības risku mazināšana pirms ES prezidentūras»

Baiba Kaškina


Pēc uzbrukuma
Sagatavošanās
Reakcija
Identifikācija
Situācijas apzināšana
Klasifikācija

Saturs

- Kurš identificē uzbrukumu
- Kas zināms par uzbrukumu
- Ko darīt???
- Komunikācijas process
  - Iekšējais
  - Ārējais

No kā uzzināt par uzbrukumu?

- Iestādes darbinieki
- Klienti vai lietotāji
- Ārpakalpojumu sniedzējs
- Tīkla vai IS monitoringa sistēma - neparasta aktivitāte
- CERT.LV
- Žurnālisti, prese...

No kā uzzināt par uzbrukumu?

- Iestādes darbinieki
- Klienti vai lietotāji
- Ārpakalpojumu sniedzējs
- Tīkla/ IS monitoringa sistēma - neparasta aktivitāte tīklā
- CERT.LV
- Žurnālisti, prese...

Kas īsti notiek – tehniskā informācija

- Monitoringa dati (NetFlow, Nagios, Zabix)
- Log faili (servera, IS, citi)
- Maršrutētāja dati (ja tam ir piekļuve)
- Firewall, ID/IP sistēmas
- Jārunā ar IPS un/vai mitināšanas pakalpojuma sniedzēju

Kas jānoskaidro par uzbrukumu?

- Kādi resursi pakļauti uzbrukumam
- Vai nenotiek vairāki uzbrukumi vienlaicīgi konkrētajai iestādei
- Potenciālais uzbrucējs
  - Robotu tīkls?
- Iespējamais uzbrukuma mērķis
  - Politisks?
- Vai Latvijā notiek citi uzbrukumi šajā laikā – saziņa ar CERT.LV

Nezaudēt galvu!

- Neveikt nepārdomātas nedokumentētas izmaiņas sistēmās un tīklos
- Neatslēgt visu no interneta
- Neizdzēst logfailus

Ko darīt???

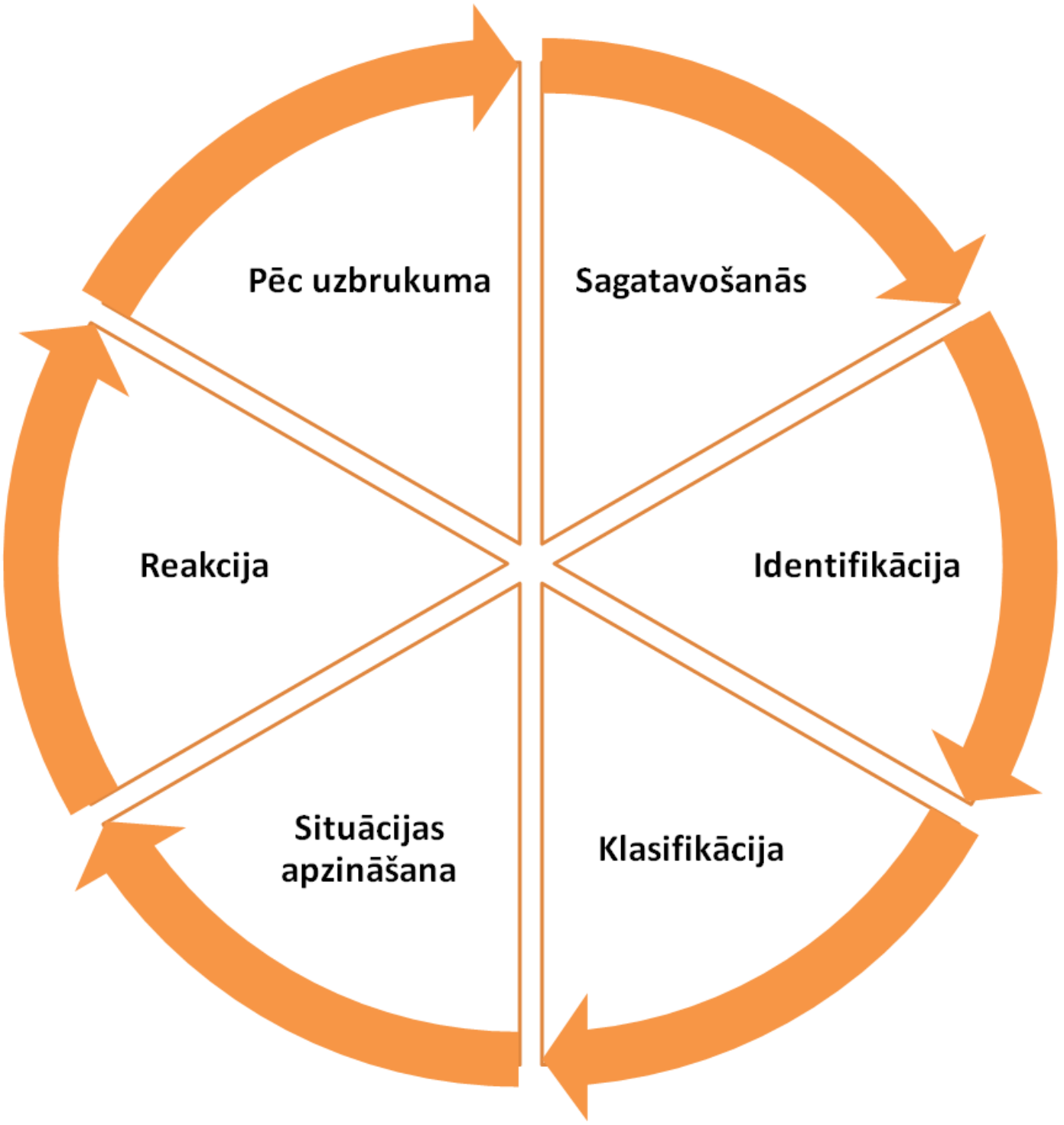
1. Nezaudēt galvu (iepriekšējais slaids!!!)
2. Identificēt uzbrukumā iesaistītos resursus un tos, kam vajadzētu strādāt, kas nav skarti
3. Kādi ir rezerves pakalpojumu sniegšanas līdzekļi/veidi
4. Ko iespējams darīt pašu spēkiem? Kāda palīdzība ir nepieciešama?
5. Informēt priekšniecību, kolēģus
6. Vienoties par ārējo komunikācijas procesu (kurš ko darīs)
7. Informēt, saukt palīgā CERT.LV

Iekšējais komunikācijas process

- Darbinieki, kas strādā pie uzbrukuma novēršanas
- Kāda informācija jāsniedz iekšējiem lietotājiem, kolēģiem (kas informēs?)
- Kāda informācija jāsniedz vadībai (kas informēs?)
- Iespēju robežās visiem vienota izpratne par situāciju

Ārējais komunikācijas process

- Kas ir atbildīgs par informāciju klientiem/sabiedrībai
- Informācija, ko sniedz pakalpojumu sniedzējam
- Ziņojums CERT.LV
- Vai tiks iesaistīta policija (pierādījumu saglabāšana)
- Informācija, ko sniedz citiem iesaistītajiem
- Nepieļaut paniku un sasteigtas darbības
- Nenoliegt uzbrukumu, nesniegt nepatiesu informāciju


Pēc uzbrukuma
Sagatavošanās
Reakcija
Identifikācija
Situācijas apzināšana
Klasifikācija