CERT.LV drošības operāciju centrs: no haosa līdz kārtībai klienta infrastruktūrā

Kristīne Kaula
Andris Medjānis

9.12.2025

CERT.LV
Cyber Incident
Response Institution

Drošības operāciju centrs (SOC)

Mērķauditorija

- Valsts un pašvaldību iestādes
- Valsts nozīmes datu centri
- Kritiskā Infrastruktūra

Mērķis

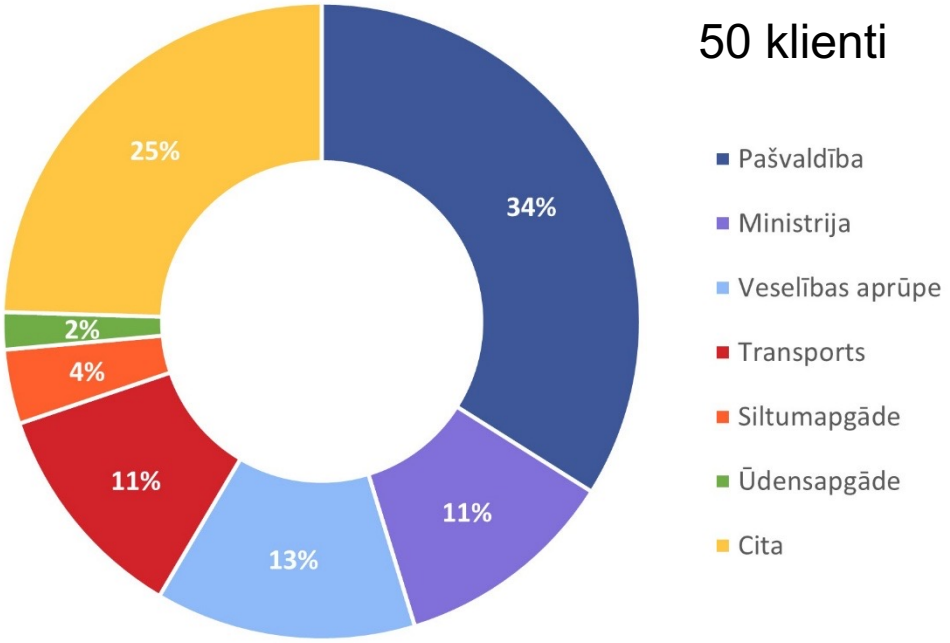
- Nacionālais kiberdrošības likums (NKDL)
- Savlaicīgi identificēt, mazināt un apturēt kiberapdraudējumu un kiberincidentu kaitējumu

Pakalpojuma process

- Jāslēdz pakalpojuma līgums.
- Programmatūra (*Elastic agents*) tiek instalēta uz gala iekārtām, piemēram, lietotāju darbstacijām un serveriem.
  (netiek instalēti uz tīkla iekārtām, lietu iekārtām (IOT))
- **Tvērums klienta infrastruktūrā** - Endpoint detection and response (**EDR**) - Drošības telemetrijas datu vākšana un apstrāde: Operētājsistēmām Windows, Linux, MacOS, citās operētājsistēmās, instalējot aģentus, lai detektētu kiberapdraudējumus.
- **Caurspīdīgs process** - visi dati tiek glabāti Latvijā uzturētos CERT serveros, klientam ir iespēja sekot līdzi un mācīties/analizēt piekļūstot *Dashboard.*

Pakalpojumiem var pieteikties sūtot epastu uz cert@cert.lv

Klienti pa sektoriem

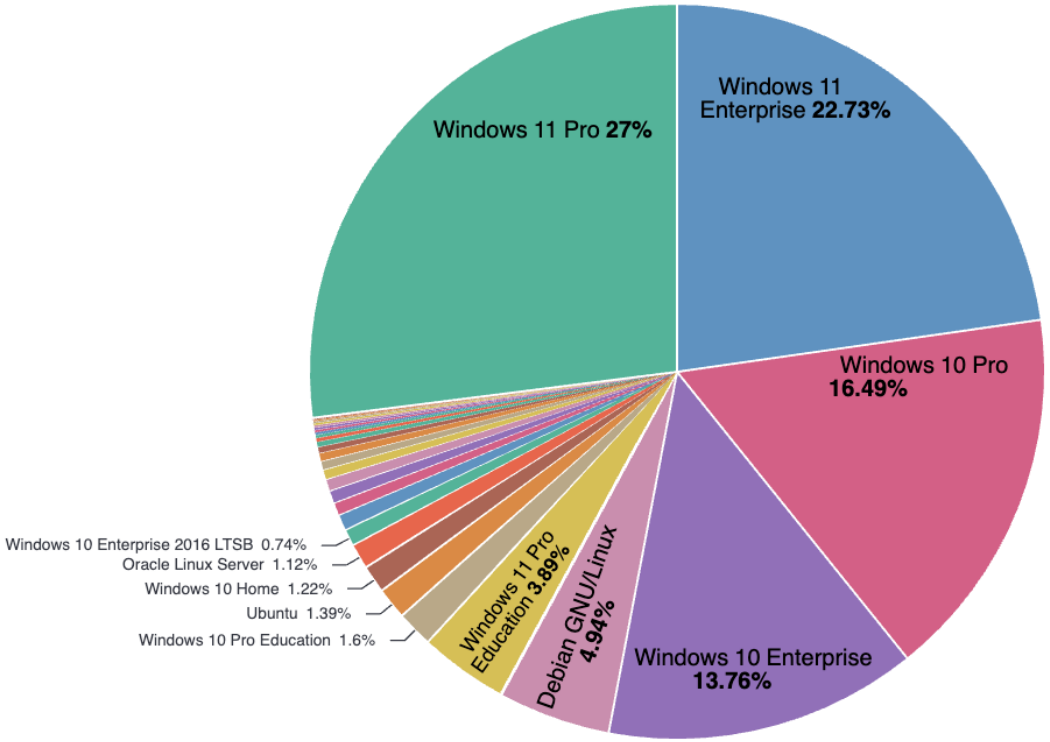


50 klienti

45 tūkstoši gala iekārtas

CERT.LV

OS versijas



Trauksmes – klienta piemērs

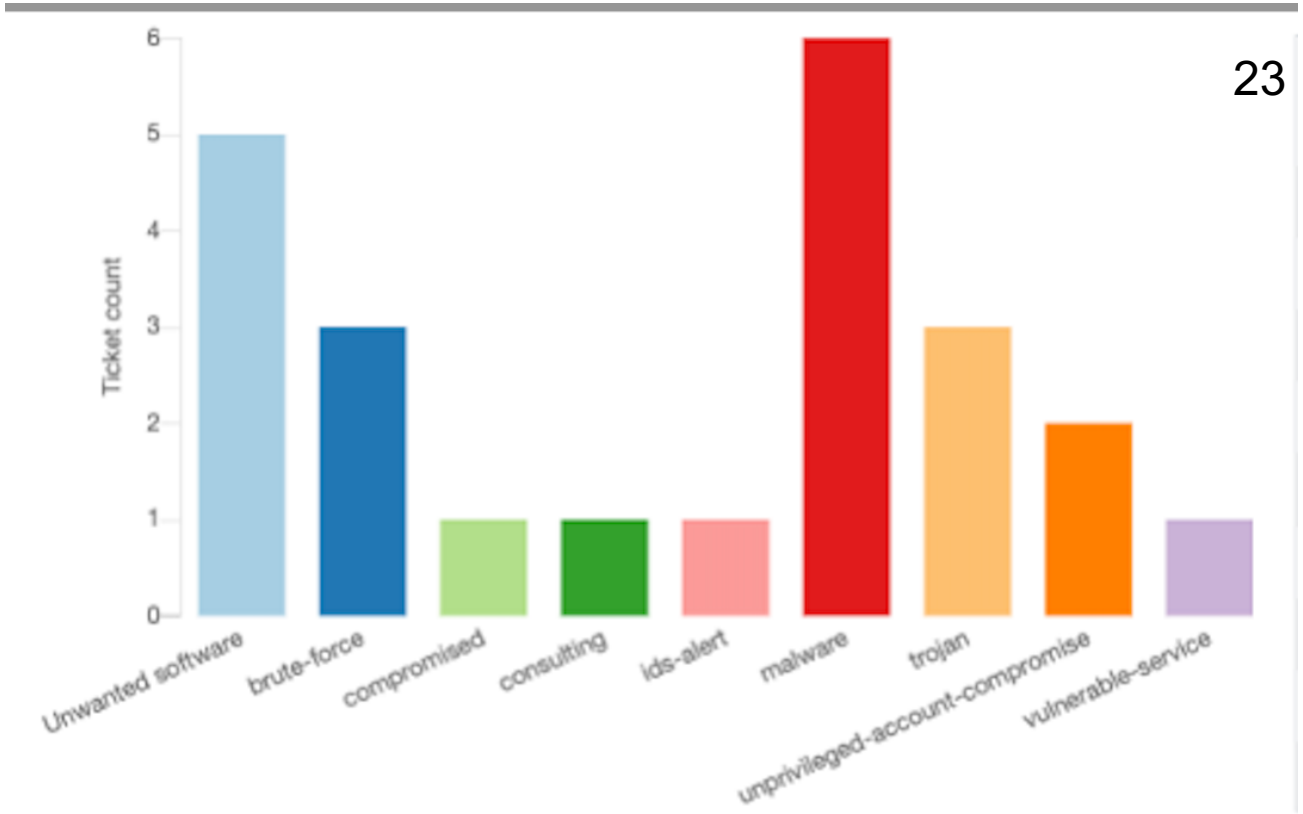
Severity levels

Levels	Count
Critical	739
High	20
Medium	1k+
Low	1k+

1200 iekārtās
30 dienās

759 trauksmes 12 manuāli izmeklējumi
80 iekārtas (**7%**) ģenerē kritiskas un augsta kritiskuma trauksmes
Vēlamais: līdz 1% iekārtu ģenerē trauksmes (Ražotāja *Elastic* ieteikums)

Kiberincidenti gada laikā



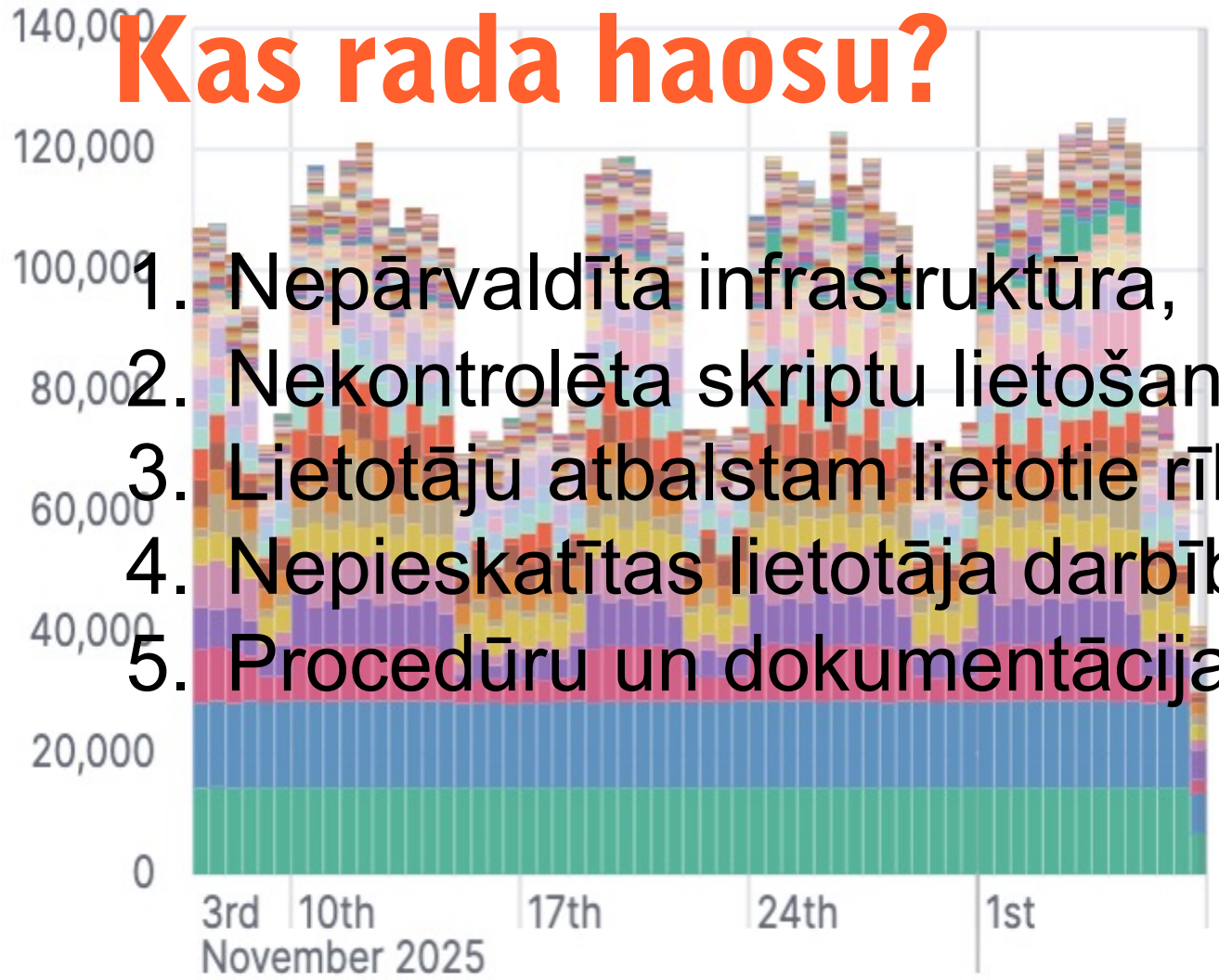
Windows OS

Sākotnējā piekļuve:

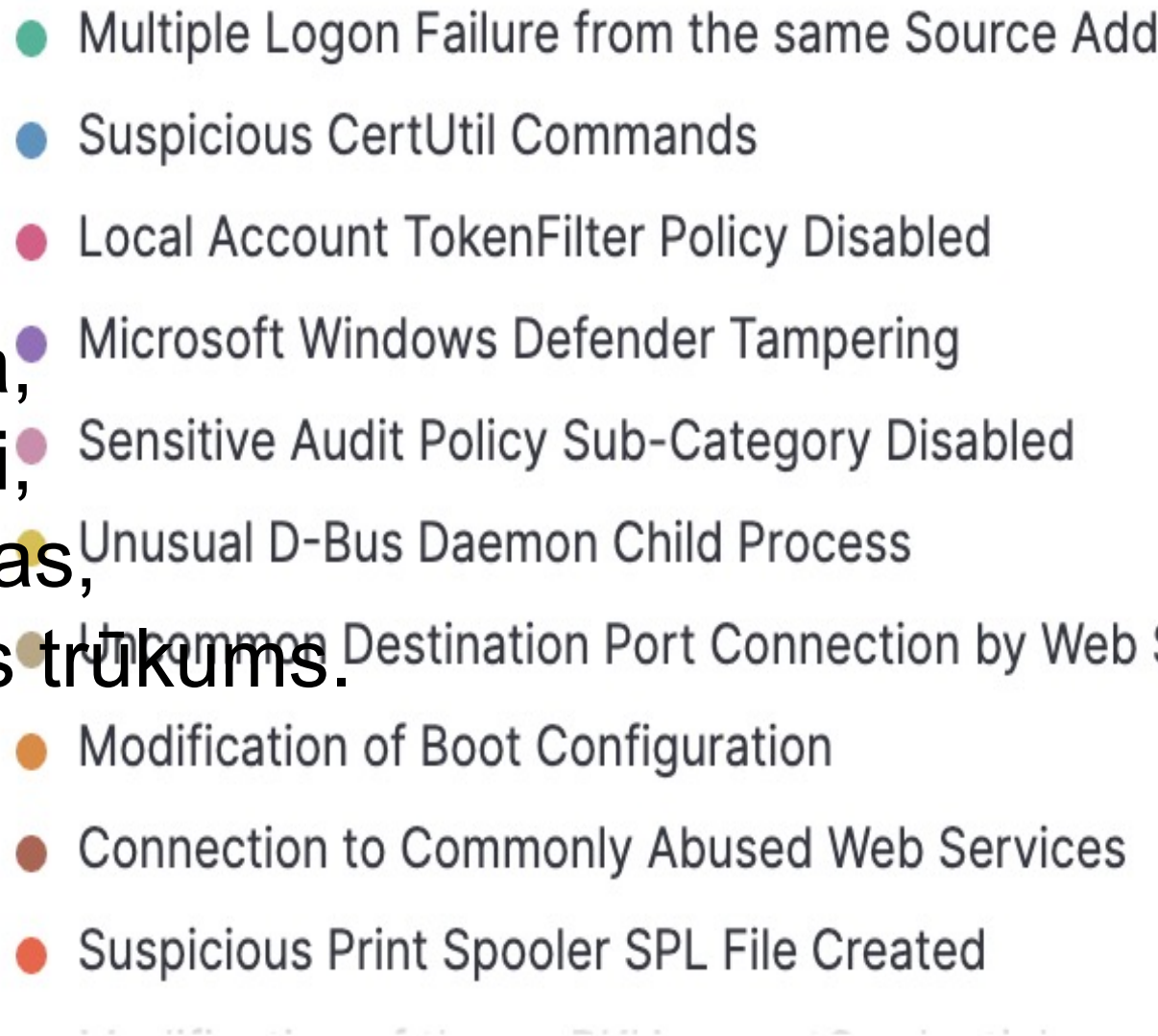
1.pārlūku paplašinājumi
2. viltus captcha
3.zibatmiņas
4.pikšķerēšana

owing: 6,099,299 alerts

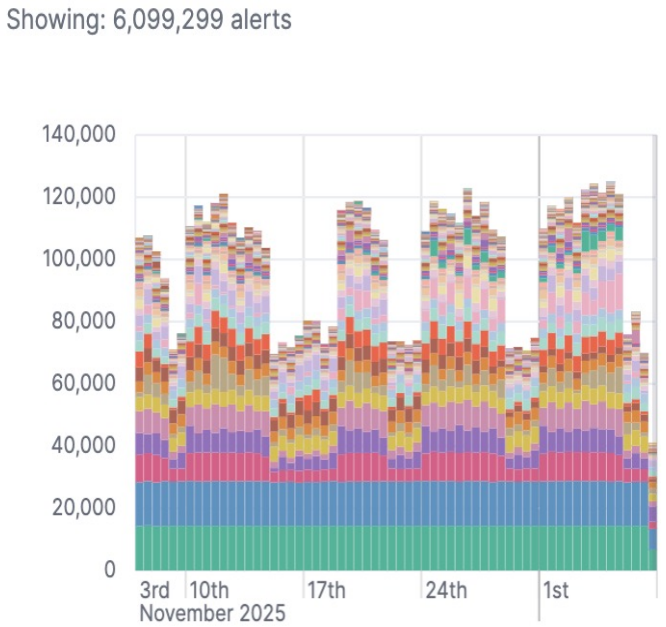
Kas rada haosu?



1. Nepārvaldīta infrastruktūra,
2. Nekontrolēta skriptu lietošana,
3. Lietotāju atbalstam lietotie rīki,
4. Nepieskatītas lietotāja darbības,
5. Procedūru un dokumentācijas trūkums.



Kā rodas haoss?



- Izdomāta organizācija ‘ABC’, darbojas 20 gadus;
- Trīs IT darbinieki – atbalsts (helpdesk), administrators, drošībnieks;
- Visi uzsāka darbu pirms 5 gadiem, kad mainījās vadība;
- Pārņēma IT saimniecību ar vienīgo dokumentāciju ‘paroles.txt’;
- 100 lietotāju gala iekārtas un 3 serveri;
- …Raspberry Pi gaitenī, kas kontrolē klimatu. Noklusējuma parole, jo to samainot kondicionēšana nedabojas;
- …Mēhāniķa dators garāžā, Windows 7, ir tīklā, bet nav domēnā;
- …Sens grāmatvedības dators, kurš gatavo svarīgu ikmēneša atskaiti;
- Maršrutētājā redzams, ka ir vēl 30 aktīvu iekārtu;
- Atbalsts lieto VNC, jo ātri un vienkārši. Teamviewer un Anydesk attālināti;
- Izmantojam joprojām kontu admin.ritvars ar paroli Vasara2010!;
- Ir Zabbix monitorings, kuru nevar atvērt, bet salabot ir darbu sarakstā;
- Žurnālfaili drošības pēc ieslēgti visi, bet to ir pārāk daudz;
- **Nav mūsu izvēle. Nosargāt vidi? Pārvaldīt? Izmeklēt incidentu?**

Nepārvaldīta infrastruktūra

Konstatētais:
nepilnīga iekārtu inventarizācija,
nekontrolēta lietojumprogrammu izmantošana,
trūkst centralizētas pārvaldības.

Riski!

Ko darīt?
Centralizēta, homogēna pārvaldība (piem., AD)
Automatizēts lietojumprogrammu baltais saraksts.

CERT.LV

Nepārvaldīta infrastruktūra

- Pilna iekārtu inventarizācija
  - Grāmatvedības + AD + tīkla aktivitātes + telpu apgaita + rīki;

- Pilna programmatūras inventarizācija – izklājlapu tabula;
  - PowerShell komanda ‘Get-Package’;
    (Get-Package | Out-File "\\serveris\mape\$($env:COMPUTERNAME)_programmas.txt");
  - Definējam bāzes aprīkojumu, definējam papildinājumus;
- Papildinām izklājlapu ar lietotāju sarakstu;

- Centralizēta pārvaldība (piem., DC vai InTune)
  - AD jāpērk serveris? Mākonis daži desmiti eur/mēn.;
  - CAL licences, manuāla administrēšana dārgāka;
  - Lietotāji paši var pārvaldīt iekārtas;
  - Samba DC (papildu izmaksas Linux speciālistam);
  - Pat 10 iekārtas liek ieviest centrālu pārvaldību;
  - Iespējams, lietojam Microsoft 365.

CERT.LV

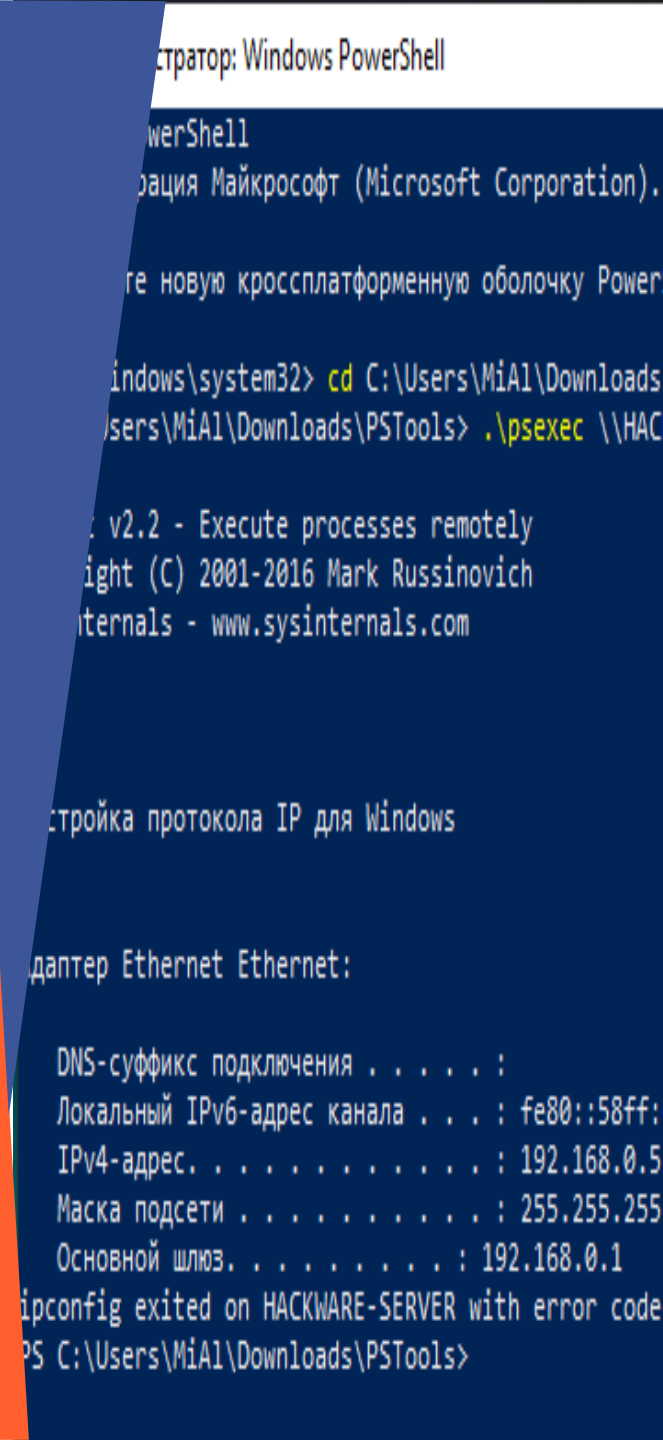
Skriptu lietošana

Pašrakstīti, skripti infrastruktūras pārvaldībai:
Konstatētais: psexec,WMI,VBS,PS
Nav ieslēgta žurnalēšana, trūkst dokumentācijas, procedūru.

Riski!

Ko darīt?
Viens - rīks, platforma, darbstacija, krātuve, admin.konts;
Moderns rīks un disciplīna;

Adekvāta žurnalēšana (ražotāja vadlīnijas);
Parakstīt PS skriptus un nepieļaut neparakstītu izpildi



CERT.LV

Lietotāju atbalstam lietotie rīki

Konstatētais:
iestādē lieto vairākus rīkus lietotāju atbalstam:
AnyDesk, Teamviewer, novecojušus rīkus

Riski!

Ko darīt?
Viens rīks komandrindai, viens darbavirsmai;
Laba pārvaldība (viens admin.darbstacija, ugunsmūris);
Microsoft nav laba sesijas koplietošanas rīka, ir alternatīvas;
Zvans > Ekrāna attēls > IM > Moderna platforma.

CERT.LV

Nepieskatītas lietotāja darbības

Konstatētais:
atļauts izpildīt failus no USB,
iekopēt un palaist programmatūru no *user profile*

Riski!

Ko darīt?
Programmatūras baltais saraksts

Nav AppLocker, bet izstrādātāja problēma
Centrālā pārvaldība, centrāla atjaunināšana
Ar priviliģētu lietotāju uzdevumu pārvaldniekā:
winget upgrade --all --silent --accept-source-agreements --accept-package-agreements

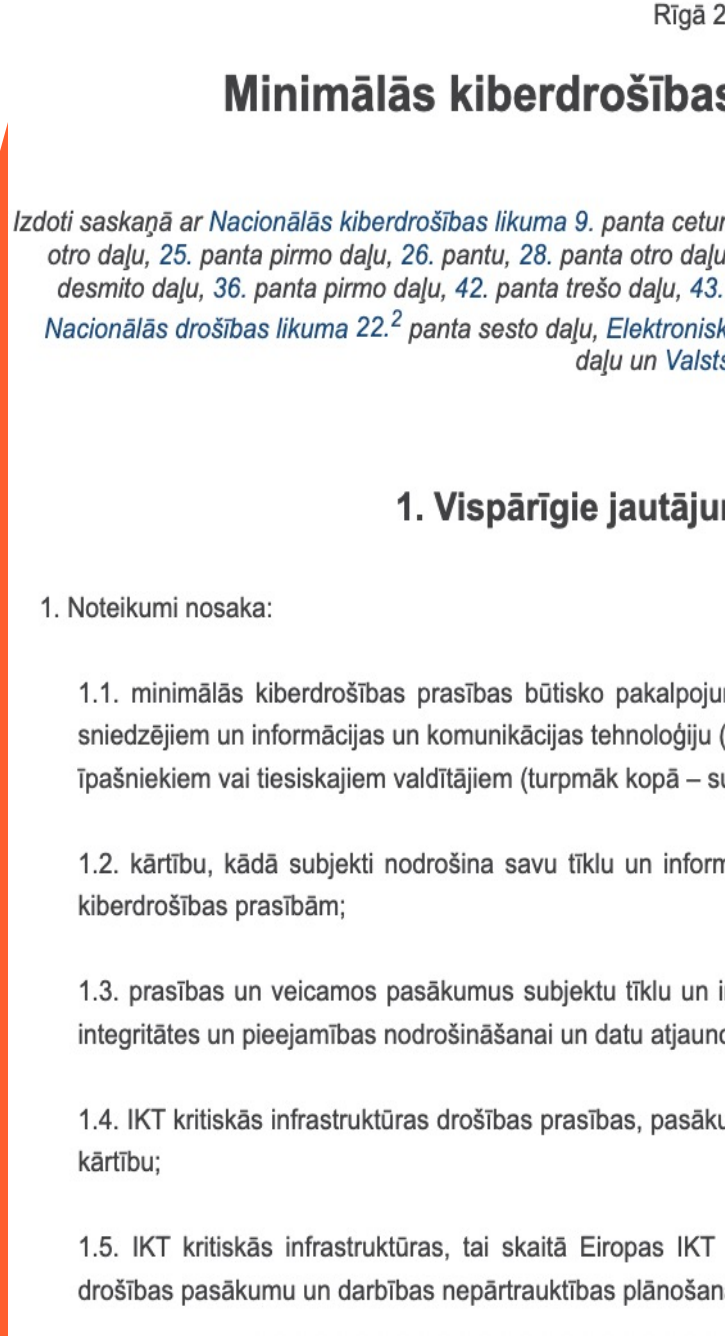
CERT.LV

Procedūru un dokumentācijas trūkums

Konstatētais:
Vairāki drošības risinājumi, trūkst kopīgas izpratnes
Procedūras, dokumentācija
Darbinieku lomas un atbildība

Riski!

Ko darīt?
Tehniskā dienasgrāmata (aizsargāta) piezīmes, komentāri, izmaiņas.



Rīgā 2

Minimālās kiberdrošības

Izdoti saskaņā ar Nacionālās kiberdrošības likuma 9. panta cetur otro daļu, 25. panta pirmo daļu, 26. pantu, 28. panta otro daļu desmito daļu, 36. panta pirmo daļu, 42. panta trešo daļu, 43. Nacionālās drošības likuma 22.[2] panta sesto daļu, Elektronisk daļu un Valsts

1. Vispārīgie jautāju

1. Noteikumi nosaka:

1.1. minimālās kiberdrošības prasības būtisko pakalpoju sniedzējiem un informācijas un komunikācijas tehnoloģiju (īpašniekiem vai tiesiskajiem valdītājiem (turpmāk kopā – su

1.2. kārtību, kādā subjekti nodrošina savu tīklu un inform kiberdrošības prasībām;

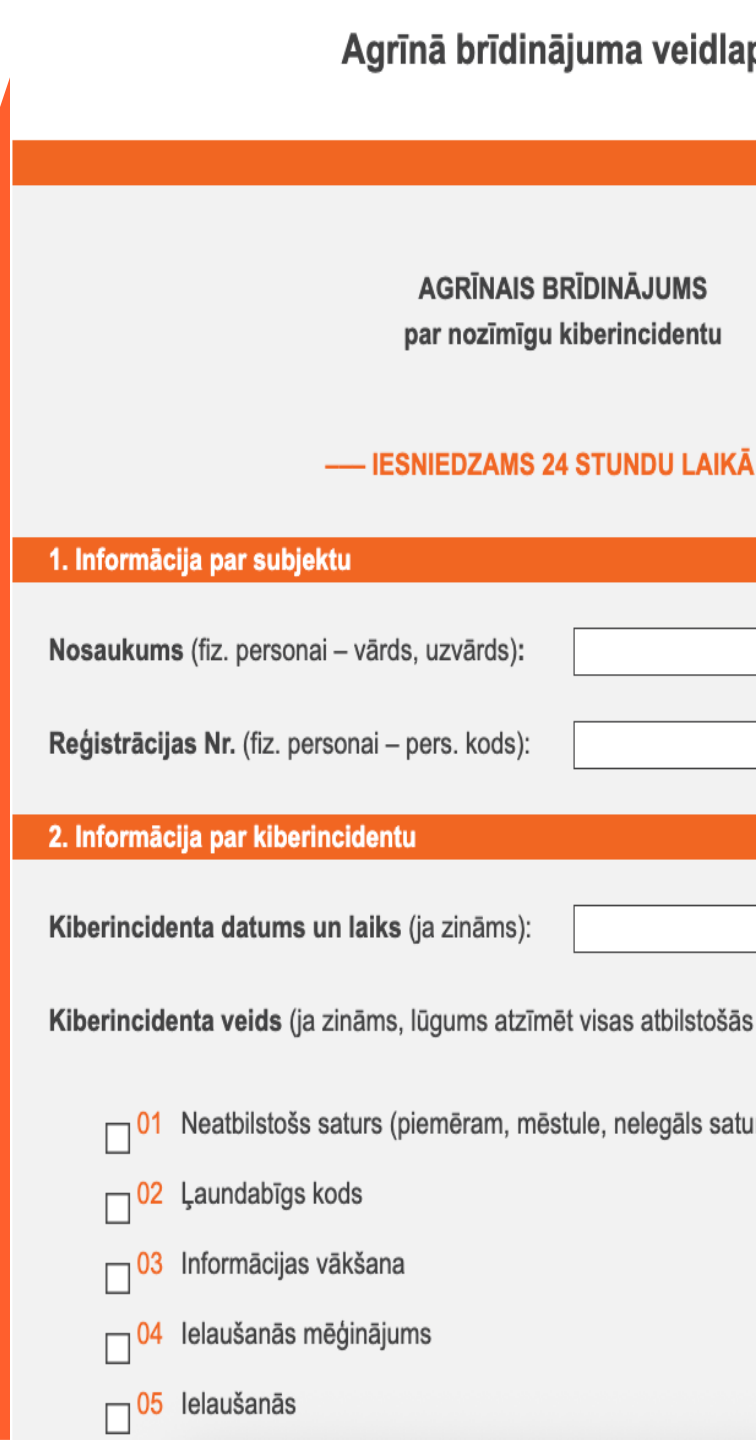
1.3. prasības un veicamos pasākumus subjektu tīklu un i integritātes un pieejamības nodrošināšanai un datu atjaun

1.4. IKT kritiskās infrastruktūras drošības prasības, pasāku kārtību;

1.5. IKT kritiskās infrastruktūras, tai skaitā Eiropas IKT drošības pasākumu un darbības nepārtrauktības plānošan

Darbu saraksts

- Pilnīga invertizācija: sistēmas, iekārtas, programmatūra. Novecojušo sistēmu migrēšana/izolēšana. Ievainojamību skanēšana.
- Programmatūras baltais saraksts ierobežojošā režīmā.
- Skriptu lietošana: žurnalēta, dokumentēta.
- Viens attālinātās piekļuves rīks.
- Dokumentācija.



Agrīnā brīdinājuma veidlap

AGRĪNAIS BRĪDINĀJUMS
par nozīmīgu kiberincidentu

— IESNIEDZAMS 24 STUNDU LAIKĀ

1. Informācija par subjektu

Nosaukums (fiz. personai – vārds, uzvārds):

Reģistrācijas Nr. (fiz. personai – pers. kods):

2. Informācija par kiberincidentu

Kiberincidenta datums un laiks (ja zināms):

Kiberincidenta veids (ja zināms, lūgums atzīmēt visas atbilstošās

- ☐ 01 Neatbilstošs saturs (piemēram, mēstule, nelegāls satu
- ☐ 02 Ļaundabīgs kods
- ☐ 03 Informācijas vākšana
- ☐ 04 Ielaušanās mēģinājums
- ☐ 05 Ielaušanās

CERT.LV

Vairāk informācijas:

cert@cert.lv

https://cert.lv/

X certlv

certlv