Rekomendācijas infrastruktūras kiberdrošības noturības uzlabošanai pret kiberuzbrukumiem

Zemāk tabulā pieejami AS "Latvijas valsts meži" kiberdrošības incidentā iesaistītās kiberuzbrucēja infrastruktūras tīkla indikatori. Iesakām tos uzraudzīt, īpaši svarīgi tas ir tiem infrastruktūras turētājiem, kuri nav ieviesuši CERT.LV pakalpojumus SOC un ABS.

IP	Pielietojums
185.44.76[.]137	Skenēšana, potenciāla datu eksfiltrācija, komunikācijas serveris (C2)
185.103.164[.]149	Sliver C2 komunikācijas serveris
80.96.108[.]88	Komunikācijas serveris (C2)
38.29.212[.]164	Izspiedējvīrusā esošā IP
159.26.105[.]137	Proton VPN
66.163.117[.]146	Komunikācijas serveris (C2)
62.169.136[.]21	Proton VPN
66.163.117[.]25	Uzbrucēja kontrolē
172.241.228[.]78	Sliver C2 komunikācijas serveris

Kopumā par nevēlamu uzskatāma jebkāda komunikācijas atļaušana no/uz anonimizācijas servisiem kā *TOR* vai arī publiski/anonīmi pieejamajiem tunelēšanas servisiem tādiem kā *Cloudflare Tunnel / Microsoft Dev Tunnels / ngrok tunnels* u.c. Valsts iestāžu tīklu saziņa ar VPN pakalpojumu sniedzēju tīkliem un komercdatu centru tīkliem arī jāizskata kā potenciāli aizdomīga.

Rekomendācijas infrastruktūras kiberdrošības noturības uzlabošanai pret kiberuzbrukumiem

CERT.LV (Kiberincidentu novēršanas institūcija) ir tālāk apkopojusi rekomendācijas infrastruktūras kiberdrošības noturības uzlabošanai pret kiberuzbrukumiem:

- Sekot **Nacionālās kiberdrošības likumam (NKDL);**
- Sekot Ministru kabineta noteikumiem **Nr. 397 "Minimālās kiberdrošības prasības"**;
- Sekot **Nacionālā kiberdrošības centra (NKDC)** un **CERT.LV (Kiberincidentu novēršanas institūcijas)** publiskotajai informācijai;
- **Infrastruktūras turētājiem ir pilnībā jāpārzina visu savu ārējā tīkla un IT ārpakalpojumu infrastruktūra** t.i. serveri, tīmekļa servisi, vārtejas, mākoņpakalpojumi, autentifickācijas pakalpojumi u.c. servisi un iekārtas, kas ir publiski eksponētas internetā. Jāuzrauga to programmatūras versiju drošības ielāpi un jāpārliecinās par to, ka ir ieviesta segmentācija.
- **Atjauninājumi jāattiecina arī uz organizācijas iekšējā tīkla servisiem** un jāveic tīkla segmentācija, lai kompromitēta ārējā tīklā esoša sistēma nekļūst par vārteju uz iekšējā tīkla resursiem.

CERT.LV CVD platforma

Ārējā tīklā eksponēto resursu ievainojamību testēšanai aicinām izveidot un pārvaldīt savas organizācijas programmu CERT.LV **Koordinētā ievainojamību atklāšanas (CVD) platformā:** https://cvd.cert.lv/. Pirms lietošanas jāiepazīstas ar "**Platformas lietošanas noteikumiem**".

- Infrastruktūras turētājiem ir jābūt izveidotam IKT resursu katalogam (IKT resursu un informācijas sistēmu katalogs, MK397, punkts 3.4), kas satur ārēji un iekšēji eksponētos resursus, to attiecīgās programmatūras un to versijas. **NAV iespējams sargāt infrastruktūru, ja tās turētājs nezina no kā tā sastāv un kas ir jāsargā.**
- Izmantojot programmatūru versiju informāciju, meklēt publiski pieejamās ievainojamības (https://www.cve.org/, https://nvd.nist.gov/search, ES ievainojamību datubāze https://euvd.enisa.europa.eu/search).
- Nekavējoties veikt internetā publiski pieejamo IKT resursu atjaunināšanu.

- Pārliecināties, ka VISIEM publiski pieejamajiem servisiem ar lietotāju autentifikāciju ir ieviesta 2FA kontrole.
- Atjaunināt novecojušas programmatūras, kas satur publiski zināmas ievainojamības.

- Gadījumā, ja tiek identificēta kritiska/augsta riska ievainojamība, to ir nepieciešams nekavējoties atjaunināt! Papildus uzmanību ir jāpievērš iekārtām, kuras nav atjauninātas vairāk kā gadu.

- Gadījumos, kad pamatoti nav iespējams ieviest atjauninājumus, veikt citus preventīvus pasākumus, kas mazina un kontrolē neatjauninātas sistēmas riskus.

- Starp Publiskā tīklā pieejamām jeb *DMZ* tīkla iekārtām un korporatīvo tīklu ir jānodrošina strikta segmentācija - tā, lai no tām nevar piekļūt citiem ar šo lomu nesaistītiem resursiem, piemēram, aktīvās direktorijas tīklam un citiem būtiskiem resursiem. Divu dažādu tīklu segmenti (*VLAN*) bez striktas ugunsmūra politikas starp tiem nav uzskatāma par segmentāciju.

- Nodrošināt, ka serveru lietotājiem ir dažādas *SSH* piekļuves atslēgas un paroles. Tas samazina uzbrucēja iespējas brīvi pārvietoties tīklā. Papildus rekomendējam izslēgt paroles autentifikāciju un strikti izmantot tikai šifrētas *SSH* atslēgas, kuras nekad netiek glabātas uz serveru iekārtām.

- Nepieciešams pārskatīt visus tīklā esošos servisa lietotājus (lietotāji, kuriem ir iestatīts *SPN*). Šo lietotāju daudzumu ir nepieciešams samazināt, kā arī tiem ir jāuzstāda drošas paroles. Standarta aktīvās direktorijas lietotājus nekad neiestata kā servisa lietotājus.

- Nodrošināt iespēju saglabāt sistēmu telemetriju/žurnālfailus atsevišķā/neatkarīgā sistēmā, uzstādīt kādu no (*SIEM/SOC*) risinājumiem, kas nodrošina žurnālfailu agregāciju / uzglabāšanu / incidentu izmeklēšanas iespējas, iekārtas šifrēšanas / bojāejas / dzēšanas / likvidācijas gadijumā.

- Iepazīties ar CERT.LV sagatavoto informāciju par kompromitēta *Windows* domēna atpazīšanu, risku mazināšanu un atgūšanos pēc uzbrukuma (*Mitigation/Hardening*): https://cert.lv/lv/2021/03/kompromiteta-domena-atpazisana-un-atgusanas-pec-uzbrukuma.

- Droši konfigurēt gan serverus, gan darbstacijas, sekojot labās prakses vadlīnijām. Kā labu paraugu var izmantot *STIG* (https://stigviewer.com/stigs), kur pieejamas rekomendācijas gan populārākajām operētājsistēmu versijām, gan konkrētai programmatūrai. Tāpat ir pieejams arī *Microsoft* izstrādāts rīku kopums "*Windows Security Baselines*", kas palīdz *Windows* administratoriem novērtēt esošo situāciju domēnā un konfigurēt iekārtas atbilstoši labajai praksei. Rīki pieejami lejupielādei šeit: https://www.microsoft.com/en-us/download/details.aspx?id=55319.

- Automatizēti kontrolēt infrastruktūrā atļautās programmatūras lejupielādi un izpildi (programmatūras baltais saraksts, piemēram, izmantojot *Microsoft* piedāvāto rīku *Applocker*). Papildu informācija par tā bāzes konfigurāciju pieejama šeit: https://cert.lv/uploads/pasakumi/Andris_Medjanis_Esi_dross_27_03_2025.pdf

- Rekomendējam striktāku darbstaciju ugunsmūra konfigurāciju (vairāk informācija: https://cert.lv/lv/2026/02/vebinars-efektiva-windows-ugunsmura-parvaldiba-17-februari).

- Rekomendējam ieviest regulāru tīkla skenēšanu ar ievainojamību skenētāju, piemēram, *Nessus* (https://www.tenable.com/downloads/nessus) vai *OpenVAS* (https://openvas.org/).

- Aicinām iepazīties ar CERT.LV izstrādāto materiālu par minimālajām ieteicamajām prasībām auditācijas iestatījumiem *Windows* domēna infrastruktūrā, kā arī tās ieviest https://cert.lv/lv/2026/01/rekomendacijas-auditesanas-iestatijumiem-windows-domena-infrastruktura.

- Ievērot Nulles uzticamības (*ZTA*) pamatprincipus:

    - pilnīga verificēšana,
    - piekļuves ar minimālām privilēģijām lietošana,
    - darbs no pieņēmuma, ka jau notiek pārkāpums.

CERT.LV pakalpojumi

Iepazīties ar pilno CERT.LV pakalpojumu klāstu un piemērojamību saviem resursiem iespējams šeit: https://cert.lv/lv/pakalpojumi

VISI CERT.LV PAKALPOJUMI IR BEZMAKSAS!

CERT.LV pakalpojumu klāsta pārskats:

CERT.LV *- Kiberincidentu novēršanas institūcija, dibināta 2006.gadā, ir „Latvijas Universitātes Matemātikas un informātikas institūta" (LU MII) struktūrvienība, kas darbojas Latvijas Republikas Aizsardzības ministrijas pakļautībā Nacionālās kiberdrošības likuma ietvaros. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā.*

Kontakti: cert@cert.lv, +371 67085888 (ziņojumu pieņemšana - 24x7), www.cert.lv