Nacionālais kiberdrošības centrs

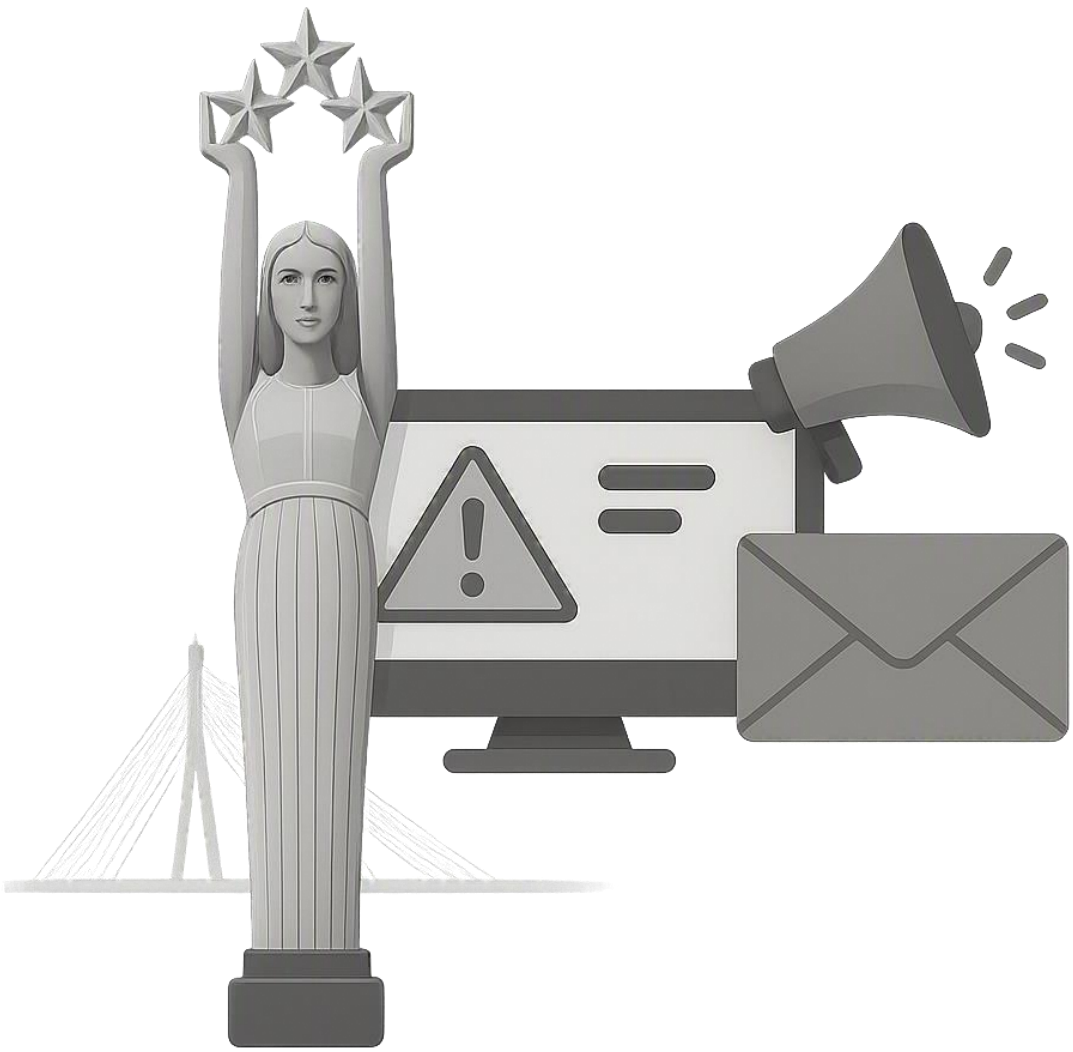
https://cyber.gov.lv, NIS2@mod.gov.lv, 67335131

Kiberincidentu ziņošanas vadlīnijas

Saskaņā ar Nacionālās kiberdrošības likuma 34. pantu,
Ministru kabineta 2025. gada 25. jūnija noteikumu
Nr. 397 7. sadaļu "Kiberincidentu vadība"

Šīs vadlīnijas ir paredzētas, lai nodrošinātu vienotu pieeju IKT resursos konstatēto incidentu ziņošanā. Vadlīnijas piedāvā metodiku un pieeju, kuru var piemērot visi Nacionālās kiberdrošības likuma (NKDL) subjekti, lai ziņotu par kiberincidentiem atbilstoši NKDL 34. pantā un Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397 "Minimālās kiberdrošības prasības" 119., 120. un 121. punktā noteiktajām prasībām.

Versija 1.0 02.06.2026



SATURS

1. IEVADS

1.1. MĒRĶIS UN PIEMĒROŠANAS JOMA

Šo vadlīniju mērķis ir nodrošināt vienotu pieeju ziņojumu iesniegšanai par kiberincidentiem, kas identificēti informācijas un komunikācijas tehnoloģiju (IKT) resursos. Ziņojumu iesniegšana ir būtiska daļa no kiberincidentu pārvaldības procesa.

Vadlīnijas piedāvā metodiku, kuru var piemērot visi Nacionālās kiberdrošības likuma (turpmāk – NKDL) subjekti, lai iesniegtu paziņojumu par notikušu kiberincidentu, kas ir negatīvi ietekmējis informācijas sistēmās un IKT resursos apstrādājamās informācijas konfidencialitāti, integritāti vai pieejamību.

Šīs vadlīnijas palīdzēs izprast, kādos gadījumos kiberincidents tiek uzskatīts par nozīmīgu un NKDL subjektiem ir jāiesniedz ziņojums atbilstoši Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397 "Minimālās kiberdrošības prasības" 119. punktam – aizpildot ziņojumu veidlapu formas, kādos gadījumos informāciju par notikušu kiberincidentu var paziņot, nosūtot attiecīgo informāciju Kiberincidentu novēršanas institūcijai CERT.LV e-pastā brīvā formā, un kādos gadījumos par notikušo kiberincidentu ir jāinformē arī kompetentās valsts drošības iestādes.

1.2. NORMATĪVAIS REGULĒJUMS UN LIETOTIE TERMINI

Vadlīnijas balstītas uz vairākiem normatīvajiem aktiem, kas kopumā veido tiesisko ietvaru kiberdrošības pārvaldībai Latvijā un Eiropas Savienībā:

- **NIS2 direktīva (Direktīva (ES) 2022/2555**) – paredz pasākumus vienādi augsta kiberdrošības līmeņa nodrošināšanai visā ES, nosakot stingrākas prasības būtisko un svarīgo pakalpojumu sniedzējiem, tostarp risku pārvaldības pasākumus, incidentu ziņošanas kārtību un atbildības mehānismus[1].

- Īstenošanas regula (ES) **2024/2690**[2] – Definē nozīmīgu kiberincidentu kritērijus un precizē NIS2 direktīvas piemērošanas noteikumus, nosakot prasības attiecībā uz DNS pakalpojumu sniedzējiem, TLD reģistriem, mākoņdatošanas un datu centru pakalpojumu sniedzējiem, satura piegādes tīkliem, pārvaldītu pakalpojumu un drošības pakalpojumu sniedzējiem, tiešsaistes platformām un uzticamības pakalpojumu sniedzējiem;

[1] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (Dokuments attiecas uz EEZ) - NIS 2 direktīva (https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32022L2555)

[2] Komisijas Īstenošanas regula (ES) 2024/2690 (2024. gada 17. oktobris), kas attiecībā uz DNS pakalpojumu sniedzējiem, TLD nosaukumu reģistriem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīkla nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem, pārvaldītu drošības pakalpojumu sniedzējiem, tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un sociālās tīklošanās pakalpojumu platformu nodrošinātājiem un uzticamības pakalpojumu sniedzējiem nosaka Direktīvas (ES) 2022/2555 piemērošanas noteikumus, kuri attiecas uz kiberdrošības risku pārvaldības pasākumu tehniskajām un metodiskajām prasībām un precizē, kādos gadījumos incidentu uzskata par būtisku Regula 2024/2690 (https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=OJ:L_202402690)

- **DORA. Eiropas Parlamenta un Padomes regula** (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011[3]

- **Nacionālās kiberdrošības likuma**[4] 34. pants NKDL subjektiem nosaka ziņošanas pienākumu par kiberincidentiem.

- Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397 "**Minimālās kiberdrošības prasības**" (turpmāk - MK 397) 118.punkts nosaka kritērijus būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un IKT kritiskās infrastruktūras īpašniekiem kiberincidenta būtiskuma noteikšanai.

2. TERMINOLOĢIJA

Vadlīnijās lietotā terminoloģija atbilst Nacionālās kiberdrošības likumā lietotajai terminoloģijai.

Termins	Apraksts
gandrīz noticis kiberincidents	notikums, kurš būtu varējis apdraudēt apstrādātus datus vai tīklu un informācijas sistēmu piedāvāto vai ar tīklu un informācijas sistēmu starpniecību pieejamo pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, bet kura pilnīga īstenošanās tika sekmīgi novērsta vai kurš neīstenojās;
kiberapdraudējums	jebkādi iespējami apstākļi, notikums vai darbība, kas atbilst Eiropas Parlamenta un Padomes 2019. gada 17. aprīļa regulas (ES) 2019/881 par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (turpmāk — regula 2019/881) 2. panta 8. punktā noteiktajai definīcijai;
kiberdrošības incidents (turpmāk — kiberincidents)	notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību;
nozīmīgs kiberincidents	pārrobežu kiberincidents vai tāds kiberincidents, kam ir ietekme uz sniegtā pakalpojuma nepārtrauktību vai sabiedrības interesēm un kas atbilst Ministru kabineta noteiktajiem kritērijiem;

[3] EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES)EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2022/2554 (https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32022R2554)

[4] Nacionālās kiberdrošības likums. (https://likumi.lv/ta/id/353390).

2. KĀRTĪBA, KĀDĀ NKDL SUBJEKTI IESNIEDZ PAZIŅOJUMU PAR KIBERINCIDENTU

2.1. ZIŅOŠANA CERT.LV PAR VISPĀRĪGIEM KIBERINCIDENTIEM

Ja kiberincidents **neatbilst** nozīmīga kiberincdenta pazīmēm (Skat. 2.3. un 2.4. punktus), tad šāds incidents būtu uzskatāms par nenozīmīgu kiberincidentu un ziņojums ir jāiesniedz kiberincidentu novēršanas institūcijai CERT.LV brīvā formā, to iesūtot uz: cert@cert.lv.

Informācijas apjoms, kas iespēju robežās jāsniedz CERT.LV par nenozīmīgu kiberincidentu:

- Notikuma apraksts (brīvā formā)
- Vai ir identificēts incidenta cēlonis (iekšējs, ārējs vai nezināms)?
- Skarto iekārtu uzturētie servisi un OS
- Saglabātie digitālie pierādījumi pirms darbības atjaunošanas
- Cita informācija, kas var palīdzēt incidenta atrisināšanā vai tā radīto seku mazināšanā

Kiberincidenta izmeklēšanai, ja tāda tiks veikta, būs nepieciešami arī sekojoši dati:

- Vai un kā tika nodrošināta un aizsargāta piekļuve IT sistēmām (konkrēts produkts, tā versijas, piekļuves ierobežojumi, paroļu politika, MFA veids un lietojums)?
- Žurnālfailu pieejamība (iekārtas, ārējs kolektors, IDS, SIEM, rezerves kopijas)
- Skarto iekārtu RAM kopijas izveides iespējas
- Datu nesēju spoguļkopijas, virtuālo mašīnu *snapshot,* iekļaujot RAM
- Tīkla plūsmas pieraksti
- Vai ir notikusi personas datu aizsardzības pārkāpums (ziņošanas pienākums DVI)?
- Plānotais darbības atjaunošanas laiks un uzņēmuma IT sistēmas stāvoklis
- Cita informācija, kas var palīdzēt incidenta izmeklēšanā

Ja informācija par kiberincidentu satur ierobežotas pieejamības informāciju – ziņojumu šifrē (PGP šifrēšanas metode vai līdzvērtīga).

Savukārt par notikumiem, kuri nav radījuši sekas, kas skartu informācijas konfidencialitāti integritāti vai pieejamību, NKDL subjekts var neziņot.

2.2. PIEMĒRI NENOZĪMĪGIEM KIBERINCIDENTIEM

Nenozīmīgi kiberincidenti ir tādi, kas nav radījuši ietekmi uz apstrādājamo datu konfidencialitāti, integritāti vai pieejamību. Attiecībā uz šādiem kiberincidentiem ziņojums brīvā formā ir jāsūta uz Kiberincidentu novēršanas institūcijas CERT.LV e-pastu: cert@cert.lv.

Tīkls un perimetrs
WAF (*Web Application Firewall*) apiešana ar reālu ekspluatāciju: veiksmīgs SQLi/XSS/SSRF[5] ar datu nolasīšanu/modifikāciju, RCE (*Remote Code Execution*), vai piekļuve iekšējiem resursiem (piem., SSRF uz mākoņa metadata pakalpojumu).
IPS (*Intrusion Detection System*) /IDS (*Intrusion Prevention System*) noteikšana ar iekšēju izpildi: POC (*Proof of Concept*)/ekspluatācija izraisa procesu palaišanu, čaulu, dropperu ielādi vai laterālo kustību (*lateral moovment*).
C2 (*Command and Control*) komunikācija notikusi: DNS (*Domain Name System*) sinkhole apiešana (DoH (*DNS over HTTPS*) /DoT (*DNS over TLS*)), "*beaconing*"s uz ļauniem domēniem/IP ar datu eksfiltrācijas pazīmēm.
Credential stuffing ar kontu pārņemšanām: vairāku kontu ATO (*Account TakeOver*), transakcijas/krāpšana, piespiedu paroles maiņas plašam lokam.
VPN (*Virtual privat network*) /Zero-Trust apiešana: neautorizēta ierīce/uzbrucējs iegūst piekļuvi, piekļūst sistēmām/datiem, eskalē privilēģijas (*privilage esaclation*). Tīkla iekārtu traucējumi ar biznesa ietekmi: maršrutētāja (*router*) / komutatora (*switch*) defekts, BGP (*Border Gateway Protocol*) incidents vai DDoS (*Distributed Denial of Service*) izraisa pakalpojuma nepieejamību vai SLO/SLA pārkāpumu[6].
Identitāte un piekļuve
MFA (*multi factor authentication*) apiešana/izspiešana: MFA fatigue/OTP (*One-Time Password*) pārtveršana/SIM-swap, kas noved pie konta kompromitēšanas (īpaši privileģēti konti).
Serviskonta kompromitēšana: serviskonta *bruteforce/credential leak* ar reālu piekļuvi, izpildi vai datu noplūdi. Biznesa procesu apstāšanās konta bloķējuma dēļ.
Neautorizēts OAuth piekrišanas piešķīrums[7]: ļaunprātīga lietotne saņem plašas tiesības (Mail.ReadWrite, Files.Read.All), tokenu eksfiltrācija un datu piekļuve.
Tokenu atskaņošana ar panākumiem: refresh/access token zādzība, sesijas pārņemšana, CSRF[8] (*Cross Site Request Forgery*)/*session fixation* ar autorizētu darbību izpildi.
E-pasts un lietotāju mijiedarbība

[5] SQLi (*SQL Injection*) / XSS (*Cross-Site Scripting*) / SSRF (*Server-Side Request Forgery*)

[6] SLO/SLA pārkāpums ir situācija, kad faktiskie pakalpojuma rādītāji (*SLI – Service Level Indicators*) nokrīt zem noteiktajiem mērķiem/saistībām attiecīgajā mērījumu logā.

Definīcijas

SLI: mērāms rādītājs (piem., pieejamība, kļūdu īpatsvars, 95 % latentums, atbildes laiks uz pieteikumu).

SLO: mērķa vērtība SLI (iekšējs vai publiski deklarēts mērķis; piem., 99.9% mēneša pieejamība).

SLA: līgumā noteikta saistība ar sekām (kredīti, līgumsods, izbeigšanas tiesības) un precīziem mērīšanas noteikumiem.

[7] Neautorizēts OAuth piekrišanas piešķīrums ir situācija, kad lietotājs vai administrators (bieži maldināts) piešķir trešās puses lietotnei piekļuves tiesības (scope) pie jūsu konta/datiem bez atļaujas vai pretrunā politikām. Tas ļauj lietotnei saņemt piekļuves/atsvaidzes marķierus (access/refresh tokens) un darboties jūsu vārdā (vai app-only režīmā), apejot paroli/MFA.

[8] CSRF (Cross-Site Request Forgery) – starpvietnes pieprasījuma viltojums. Uzbrucējs liek upura pārlūkam, kurš jau ir autentificēts mērķa vietnē, nemanāmi nosūtīt tai pieprasījumu (ar upura sesijas sīkdatni), izpildot upura vārdā darbību bez viņa piekrišanas.

Pikšķerēšana ar kompromitēšanu: lietotājs klikšķina un ievada akreditācijas datus (vai lejupielādē ļaunprogrammatūru); BEC (*Business Email Compromise*) ar maksājumu novirzīšanu[9].
Masveida ļaunprogrammatūras izplatīšana: vairāki galalietotāji (*end point*) inficēti, "smilšu kastes" (*sandbox*) apiešana, makro izpilde, laterāla kustība.
Kalendāra saite noved pie izpildes: ļaunprātīgs ICS[10]/*meeting add-in*[11] izraisa koda izpildi vai datu izpaušanu.
Galiekārtas/EDR
Ļaunprogrammatūra izpildīta ar noturību: persistences mehānismi, C2 (*command and control*), datu eksfiltrācija; ransomware šifrēšana jebkādā apjomā.
Laterālā kustība (*lateral movement*), vai akreditācijas datu izgūšana (*credential dumping*): LSASS piekļuve (*Local Security Authority Subsystem Service*), Pass the Hash /Ticket admin tiesību iegūšana.
USB izmantošana eksfiltrācijai vai izpildei: neatļauta datu kopēšana uz ārēju nesēju vai HID (*Human Interface Device injection*) injekcijas skriptu palaišana.
Lietojumprogrammas un tīmekļa servisi
API rate limit ietekmē pakalpojumu pieejamību: noturīgi 429 (*Too Many Requests*) / 503 (*Service Unavailable*) ar *transaction failure*, rindas "*dead letter*", neatgriezeniska datu nekonsekvence.
TLS problēmas ar ietekmi: savlaicīgi neatjaunots vietnes sertifikāts vai privātā atslēga kompromitētas, izsaucot dīkstāves vai MITM (*Man in the middle*) risku.
Mākoņpakalpojumi/SaaS
DLP apiešana/nestrādāšana: sensitīvi dati (PII - Personas identificējoša informācija, finanšu, veselības dati) kopīgoti ārēji un piekļuve apstiprināta (auditā redzama), iespējams regulatīvs ziņojums.
Publiska krātuve ar sensitīvu saturu un neautorizētu piekļuvi (nepareizas konfigurācijas dēļ): publisks *buckets/containers* ar PII (personas identificējošo informāciju) /BD (biznesa dati) un ar ārējiem GET/LIST pieprasījumiem ir iespējama piekļuve saturam.
Pre-signed URL/SAS izmanto trešā puse: lejupielādes reģistrētas, TTL bijis pārmērīgs, IP/ģeogrāfija neatbilst[12].

[9] BEC ar maksājumu novirzīšanu (*Business Email Compromise*) ir krāpšana, kur uzbrucējs, izmantojot kompromitētu vai imitētu e-pastu, panāk, ka uzņēmums pārskaita naudu uzbrucēja (bieži "naudas mūļa") kontā, nevis īstajam piegādātājam vai saņēmējam.

[10] "ICS" attiecas uz iCalendar failiem, kas bieži izmanto paplašinājumu ".ics". iCalendar standarts tiek izmantots, lai apmainītos ar kalendāra informāciju.

[11] Ļaunprātīgs "ICS/meeting add-in" ir uzbrukuma veids, kur:
ļaunprātīgs ICS (iCalendar .ics) kalendāra ielūgums vai saite tiek izmantota pikšķerēšanai/ekspluatācijai, vai
ļaunprātīgs/nelikumīgi ieviests sapulču spraudnis (*add-in*) Outlook/Teams/Zoom/Google vidē iegūst piekļuvi datiem un/vai injicē kaitīgu funkcionalitāti.

[12] Objektu glabātuvē (piem., AWS S3 vai Azure Blob) izveidota īslaicīgā piekļuves saite (*pre-signed URL/SAS*) ir nonākusi trešās puses rīcībā un tā ir to izmantojusi, lai lejupielādētu failu/s. Žurnāli rāda veiksmīgas lejupielādes, saites derīguma termiņš (TTL) bijis pārāk ilgs, un piekļuves IP/ģeogrāfija neatbilst gaidītajai.

Vāju kriptogrāfijas algoritmu (piem. TLS 1./1.1) izmantošana radījusi sekas/incidentu.
Dati un privātums
PII/SI (personu identificējoša informācija/sensitīvā informācija) nosūtīta ārējam adresātam bez iespējas atsaukt, un ir piekļuves/izmantošanas pazīmes; liels apjoms vai īpašo kategoriju dati (regulatīvais slieksnis VDAR 9.pants).
Fiziskā vide un iekārtas
Neautorizēta iekļūšana aizsargātā zonā: iekārtu zādzība/bojājumi, iespējama datu kompromitēšana (ja datu nesēji nešifrēti).
Ilgstošas videonovērošanas seguma zudums[13] vai sabotāža, notikušas paralēlas neatļautas aktivitātes.
Enerģijas/HVAC (*Heating, Ventilation and Air Conditioning*) defekti ar sekojošu ietekmi uz pakalpojumiem, vai IKT iekārtu bojājumiem.
Trešo pušu/atkarību notikumi
CDN (*content delivery network*) reģionāla/globāla kļūme ar klientu ietekmi[14]: pieejamības kritums, kļūdu pīķi virs SLO; neveiksmīgs *re-routing* vai pārāk gari DNS TTL (*Time to Live*).
Piegādātāja API izkrišana ar biznesa ietekmi: darījumu zudumi, norēķinu kavējumi, datu nekonsekvence, SLA pārkāpums.
Nepaziņota, vai ieilgusi uzturēšana ar dīkstāvi, vai datu kļūdām.
Kriptogrāfija un uzticamība
OCSP (*Online Certificate Status Protocol*) /CRL (*Certificate Revocation List*) traucējumi ar "*hard fail*": klienti nevar izveidot TLS, pakalpojumu nepieejamība.
PKI starpsertifikāta/ķēdes kļūda ražošanā, plašas validācijas kļūdas, klientu atteikumi.
Iekšējie procesi
Atrastā ievainojamība tiek aktīvi ekspluatēta, pierādīta ekspluatācija pirms ielāpa, kompromitēti serveri/konti.
NTP nobīde izraisa autentifikācijas kļūmes (*Kerberos/OAuth*) vai žurnālu integritātes zudumu vismaz daļai sistēmu.

[13] CCTV seguma zudums ir situācija, kad videonovērošanas sistēma vairs nesniedz paredzēto pārklājumu (attēlu/ierakstu) kādā zonā vai periodā, tādējādi zūd spēja reāli uzraudzīt vai vēlāk pārskatīt notikumus.

[14] Situācija, kad satura piegādes tīkls (CDN) noteiktā reģionā vai plašāk nespēj korekti apkalpot tīkla plūsmu , izraisot gala lietotājiem kļūdas, lēnumu vai nepieejamību (SLO/SLA pārkāpumu).

SIEM noteikumu/telemetrijas izslēgšana noved pie nepamanītas kompromitēšanas (ilgstošs *dwell-time*[15]).

Noslēgumā – ko ņemt par "nozīmīguma" kritēriju

- Ietekme: reāla CIA (konfidencialitāte/integritāte/pieejamība) ietekme vai SLO/SLA pārkāpums.
- Apjoms un ilgums: skarto lietotāju/sistēmu daudzums, dīkstāves laiks, pakalpojumu kritiskums.
- Sensitivitāte: PII/īpašas kategorijas, finanšu vai regulēti dati, iespējams ziņošanas pienākums uzraudzības iestādei.
- Kompromitēšanas pazīmes: noturība, laterālā kustība, privilēģiju eskalācija, C2 (*Command and Control*), datu eksfiltrācija.
- Trešo pušu atkarības: SLA pārkāpums ar biznesa ietekmi.

Ieteikums: salāgojiet šos piemērus ar savu incidentu novērtēšanas metodiku, ņemot vērā incidenta smaguma pakāpi un definējot mērāmos robežsliekšņus.

2.2. NOTIKUMI PAR KURIEM BŪTU VĒLAMS ZIŅOT

Kiberuzbrukumu novēršanā lielu lomu spēlē prevencija. Informācija par gandrīz notikušiem kiberincidentiem (uzbrukumu mēģinājumiem) ir svarīga, lai pamanītu un novērstu šādus un līdzīgus uzbrukumus valstiskā līmenī. Ir būtiski ziņot kiberincidentu novēršanas institūcijai CERT.LV par gandrīz notikušiem kiberincidentiem, ja uzbrukumā tiek izmantota informācija (vai dati), kas ir zināmi ierobežotam personu lokam, informācija par notikumiem, kas nav brīvi publiski pieejami internetā, personīgiem aspektiem (privātās dzīves niansēm) u.tml. Šādas ziņas kiberincidentu novēršanas institūcijai CERT.LV palīdz veikt preventīvās darbības un izskaust kiberuzbrucējus no IKT vides pirms tie ir paspējuši pastrādāt kibernoziegumu.

Kiberincidentu novēršanas institūcija CERT.LV sagaida un novērtē ziņojumus par gadījumiem, kad kiberuzbrukums nav izdevies (ir ticis novērsts) attiecībā uz:

- Mērķētiem mēģinājumiem pret kritiskām sistēmām, personām (personalizēti) vai datiem,
- Indikācijām par kompromitētām piekļuvēm vai akreditācijas datiem,
- Ļaunatūrām (*malware/ransomware*), ko AV (*Antivirus/antivīruss*) vai EDR (*Endpoint Detection and Response*) sanitizēja/karantinizēja, it īpaši uz serveriem vai administratoru iekārtām,
- Datu noplūdes notikumiem, ko apturēja DLP (*data loss prevention*) sistēma vai tīkla politika,
- Būtiskām konfigurācijas kļūdām vai atklātiem eksponētiem resursiem,
- Ievainojamību izmantošanas mēģinājumiem, kurus apturēja ugunsmūris vai ievades validācijas pārbaude,

[15] "*Dwell time*" attiecas uz laika periodu, kurā uzbrucējs atrodas tīklā, pirms viņu atklāj. Tas ir svarīgs drošības rādītājs, jo ilgāks "*dwell time*" var nozīmēt vairāk iespēju uzbrucējam nodarīt kaitējumu vai nozagt informāciju.

- DDoS mēģinājumiem, ko absorbēja (novērsa) pakalpojumu sniedzējs, ja tie skāra publiskos servisu, pakalpojumus vai gala lietotājus,
- **Trešās puses/supply-chain kiberincidentiem vai gandrīz notikušiem kiberincidentiem, kas varēja radīt būtisku ietekmi uz jūsu uzņēmuma spēju nodrošināt pakalpojumus vai datu pieejamību**,
- Ja potenciālā kiberincidenta gadījumā iespējamais ietekmes līmenis būtu bijis augsts (pieejamība, integritāte vai konfidencialitāte kritiskam pakalpojumam),
- Redzamām pazīmēm, ka incidents ir daļa no plašākas kampaņas pret nozari/reģionu,
- Izmantotu 0-day ievainojamību vai jaunu, maz aprakstītu tehniku.

Informāciju par gandrīz notikušiem incidentiem brīvā formā jāsūta uz: cert@cert.lv

2.3. NOZĪMĪGIE KIBERINCIDENTI UN ZIŅOŠANAS KĀRTĪBA

Par **nozīmīgu kiberincidentu** subjekts Nacionālās kiberdrošības likuma 34. panta otrajā, trešajā, piektajā un sestajā daļā noteiktajos termiņos **ziņo kompetentajai Kiberincidentu novēršanas institūcijai CERT.LV**, Satversmes aizsardzības birojam, nosūtot uz tās elektroniskā pasta adresi **elektroniski aizpildītu un parakstītu ar drošu elektronisko parakstu**:

agrīnā brīdinājuma veidlapu (10. pielikums)	– 24 Stundu laikā
* sākotnējā ziņojuma veidlapu (11. pielikums)	– 72 stundu laikā Uzticamības pakalpojumu sniedzējiem: – 24 stundu laikā
progresa ziņojuma veidlapu (12. pielikums)	– iesniedz, ja incidentu nav izdevies atrisināt mēneša laikā (pēc incidenta atrisināšanas iesniedz gala ziņojumu) - *ja attiecināms*
starpposma ziņojuma veidlapu (13. pielikums)	– Pēc pieprasījuma / nepieciešamības (*ja attiecināms*)
* galaziņojuma veidlapu (14. pielikums)	– 1 mēneša laikā no sākotnējā ziņojuma iesniegšanas

* minētās ziņojumu veidlapas ir iesniedzamas **obligāti**.

2.4. KIBERINCIDENTA NOZĪMĪGUMA KRITĒRIJI UN PIEMĒRI

Atbilstoši Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397 "Minimālās kiberdrošības prasības" 118. punktam kiberincidentus iedala **nozīmīgajos** kiberincidentos un kiberincidentos, kuri **nav uzskatāmi par nozīmīgiem** kiberincidentiem (noteikumu 120.punkts).

Zemāk, atbilstoši noteikumu 118.2. punktam, tiks sniegti skaidrojumi un piemēri, kad kiberincidents tiek uzskatīts par nozīmīgu un kiberincidenta ziņojums ir jāiesniedz saskaņā ar noteikumu 119.punktu (t.i. izmantojot noteiktās ziņojumu veidlapas).

Elektroniski parakstītas kiberincidenta ziņojuma veidlapas jāsūta uz: cert@cert.lv

Ja informācija par kiberincidentu satur ierobežotas pieejamības informāciju – ziņojumu šifrē (PGP šifrēšanas metode).

MK 397 118.punkta:	Incidenta piemērs – ziņojami atbilstoši ziņojumu veidlapām
118.2.1. kiberincidents apdraud sabiedrības veselību vai drošību, valsts drošību, ekonomisko drošību, valsts reputāciju, ārējās attiecības, pilsonisko brīvību vai pamattiesības;	Uzlauztas valsts oficiālās informācijas publiskošanas vietnes (piem., mājas lapas), izplatīta apzināti nepatiesa informācija Tiek uzlauzta oficiālā izdevuma "Latvijas Vēstnesis" tīmekļa vietne un aizstāts ārējā normatīvā akta teksts, vai datu bāze nav pieejama pilnībā. Uzbrukums Valsts vienotajai datorizētajai zemesgrāmatai, izmainot vai sagrozot īpašumu un īpašnieku datus.
118.2.2. kiberincidents rada mantiskus zaudējumus subjektam, citiem subjektiem, Latvijas Republikai, pakalpojumu saņēmējiem vai citām personām vismaz 500 000 euro vai 5 % apmērā no subjekta pēdējā finanšu gada apgrozījuma (atkarībā no tā, kura summa ir mazāka);	Viltus apmaksas dokumentu iesūtīšana, kā rezultātā uz krāpnieku kontu tiek pārskaitīti būtiski naudas līdzekļi (piem., par pasūtījumu). Iejaukšanās reālajā darījumā, aizstājot apmaksas dokumentus. Kiberuzbrukums subjekta informācijas sistēmai ar smagām finansiālām sekām pakalpojumu/funkciju nepieejamības gadījumā.
118.2.3. kiberincidents rada vai var radīt kaitējumu fiziskās personas dzīvībai vai veselībai;	*Ransomware* incidents slimnīcā (tiek nošifrēts iekšējais datortīkls), nav pieejami pacientu dati, paralizēta informācijas apmaiņa starp slimnīcas nodaļām un laboratorijām. Nav iespējams veikt neatliekamās un plānveida medicīniskās manipulācijas. Uzbrukumi, kas saistīti ar IoT un citām iekārtām, kas nodrošina pacientu dzīvības uzturēšanas funkcijas. Ūdens attīrīšanas sistēmas bojāšana kā rezultātā ūdenī tiek ievadīti reaģenti, kas vairākkārtīgi pārsniedz paredzamo devu. Individuālo gāzes vadības katlu vadības sistēmas kompromitēšana kā rezultātā var atvērt gāzes padevi bez gāzes katla palaišanas (aizdedzināšanas).
118.2.4. kiberincidents rada vai var radīt ietekmi uz ierobežotas pieejamības vai klasificētās informācijas konfidencialitāti, integritāti vai pieejamību;	Kļūmes pēc klasificēta informācija tiek nodota trešajai pusei (mākoņpakalpojuma nodrošinātājam). Nav izveidota pienācīga kontrole klasificētās informācijas apritei. Nozaudēts (nozagts) nešifrēts datu nesējs (t.sk. dators), kas satur IP informāciju, informācijas noplūde rada būtisku reputācijas zaudējuma (negatīvas ietekmes) risku.

118.2.5. kiberincidents ir izraisījis vai var izraisīt būtiskā vai svarīgā pakalpojuma saņemšanas vai IKT kritiskās infrastruktūras funkcionēšanas traucējumus;	Liela apjoma DDoS pret NKDL subjektu – kā rezultātā kritiskie pakalpojumi nav pieejami. Medijs nespēj nodrošināt apraidi (ilgākā laika periodā) infrastruktūras fiziska bojājuma dēļ. Darbības nepārtrauktības plāns nav ticis notestēts, atbildīgie darbinieki nav zinājuši nepieciešamās procedūras darbības atjaunošanai.
118.2.6. kiberincidents ir pārrobežu kiberincidents Nacionālā kiberdrošības likuma 1. panta 21. punkta izpratnē.	Latvijā reģistrēts uzņēmums **ar dažādām filiālēm ārzemēs** saskārās ar šifrējošā vīrusa uzbrukumu (*ransomware*), kā rezultātā tiek šifrētas uzņēmuma grāmatvedības un loģistikas sistēmas. Līdzīgas sfēras uzņēmumus Baltijas valstīs, piemēram, energoapgādes jomā, ir skāris kiberuzbrukumu vilnis, kura ietekme jaušama arī kaimiņvalstīs t.i. traucēta pakalpojumu pieejamība.

3. CITIEM KOMERSANTIEM VAI PRIVĀTPERSONĀM

Par konstatēto kiberdrošības incidentu ir iespēja brīvprātīgi ziņot kompetentajai kiberincidentu novēršanas institūcijai CERT.LV, nosūtot aprakstu brīvā formā uz e-pasta adresi cert@cert.lv

Kiberincidentu novēršanas institūcija CERT.LV vienojas ar personu, kura ziņojusi par kiberdrošības incidentu, par atbalsta sniegšanu kiberincidenta risināšanā (ja tāda ir nepieciešama).

Pēc savas iniciatīvas jebkurš var brīvprātīgi ziņot kompetentajai kiberincidentu novēršanas institūcijai CERT.LV par gandrīz notikušu kiberincidentu vai kiberapdraudējumu.

Brīvprātīga ziņošana par kiberdrošības incidentu, gandrīz notikušu kiberincidentu vai kiberapdraudējumu neuzliek personai papildu pienākumus.

4. NOTIKUMI, PAR KURIEM VAR NEZIŅOT

Ziņošana Kiberincidentu novēršanas institūcijai CERT.LV vai Satversmes aizsardzības birojam ir obligāta tikai NKDL subjektiem attiecībā uz nozīmīgiem incidentiem un incidentiem, kas netiek uzskatīti par nozīmīgiem, taču ir būtiski subjekta darbībā un radīja ietekmi uz apstrādājamās informācijas pieejamību, konfidencialitāti vai integritāti.

Par **nenozīmīgiem vai nebūtiskiem** kiberincidentiem tiek uzskatīti nelieli epizodiski notikumi, kas tika automatizēti vai manuāli novērsti, bez ietekmes uz subjekta darbību, piemēram:

Automatizēti un neveiksmīgi mēģinājumi
Portu skenēšana, kas bloķēta ar ugunsmūri.

Brute-force mēģinājumi, kas apstādināti ar rate-limiting/MFA/lockout (bez konta pārņemšanas).
DDoS, ko pilnībā novērš DDoS aizsardzības nodrošinātājs bez pakalpojuma nepieejamības.
Neparasti pieteikšanās mēģinājumi bloķēti ar nosacījumu piekļuves kontroli (*Conditional Access*), MFA pieprasīts/atteikts (bez piekļuves).
Pagaidu konta/serviskonta parole kļūdaini ievadīta vairākas reizes, konts īslaicīgi bloķēts (nav neatļautas piekļuves).
Atteikts OAuth/Consent pieprasījums aizliegtai trešās puses lietotnei (*Admin Consent Policy)* to bloķē[16].
Sesijas marķiera (*token*) atskaņošanas mēģinājums, kas nav derīgs – servera validācija noraida (signatūra/nonce pārbaudi neiztur).
Filtrēts kaitīga tīkla plūsmas saturs
SPAM un pikšķerēšana, ko filtrs nobloķējis (lietotājs neklikšķināja, nav kompromitēšanas pazīmju).
DMARC/DKIM/SPF bloķēta sūtītāja imitācija - vēstule netiek ievietota iesūtnē (*inbox*).
Kaitīga saite e-pastā nobloķēta ar URL repute gateway (lietotājs neklikšķina).
Kaitīgs pielikums, kas tika ievietots "karantīnā" pirms izpildes.
DNS sinkhole/no resolve ar ļaunprātīgiem domēniem, nav panākta savienojuma izveide.
Ugunsmūra bloķētie mēģinājumi (SQLi/XSS/SSRF) bez aplikācijas ietekmes.
IPS/IDS bloķējumi (piem., Eternal skenējumi) bez iekšējās izpildes.
Botu/credential stuffing datu plūsmu jeb tīkla pieprasījumu apjoms (*traffic*) bloķēts ar bot management/ratelimit (nav kontu pārņemšanas).
VPN/Zero Trust piekļuves mēģinājumi no neautorizētām ierīcēm, ko atteica drošības politika (bez piekļuves).
Iekšēji ātri novērstas nepilnības, kas nav saistītas ar sensitīvu datu apstrādi
Konfigurācijas kļūda ar minūšu dīkstāvi nelielai lietotāju grupai, bez būtiskas ietekmes.

[16] kāda trešās puses lietotne (piemēram, ārējs serviss vai rīks), mēģināja iegūt piekļuvi organizācijas datiem,
izmantojot OAuth autorizācijas mehānismu, bet piekļuve tika noraidīta, jo to bloķē organizācijas drošības politika – *Admin Consent Policy*.

Vienas darbstacijas aizdomīgs process, kura izcelsme ir noskaidrota, kurš tika novērsts un nav pierādījumu par turpmākām kaitīgām darbībām IS (nav konstatēts *lateral movement*).
UPS, barošanas bloka, cietā diska vai citas iekārtas atteice (bez ietekmes uz pakalpojumu un informācijas pieejamību).
Darbinieku kļūdas vai iekšējo procedūru neievērošana (ja tā nav novedusi pie incidenta un tās rezultātā netika ietekmēta informācijas konfidencialitāte, integritāte vai pieejamība).
PUA/Adware detekcija un karantīna, nav izpildes un persistences. Nostrādāja galiekārtas aizsardzība (AV/EDR), kas atklāja potenciāli nevēlamu lietotni (PUA/PUP) vai reklāmprogrammatūru (Adware), to nekavējoties bloķēja vai ievietoja karantīnā, un programmas kods netika palaists (izpildīts) un neizveidoja noturību (persistenci) sistēmā.
Skripts bloķēts ar AppLocker/Device Control (nav izpildīts).
Neatļautas USB ierīces mēģinājums, ko politika bloķē (bez datu nolasīšanas/ieraksta).
PowerShell Constrained Language Mode novērš komandletu[17] izpildi; EDR neuzrāda laterālo kustību.
Mākoņpakalpojumi/SaaS:
DLP (data loss prevention) politika bloķē ārēju kopīgošanu; lietotājs saņem atteikumu (nav noplūdes).
Nepareizi konfigurēts "publisks" iestatījums izstrādes vai testa videi (nav sensitīvu datu, bez piekļuves), novērsts nekavējoties.
Objekta glabātuvei (piem., AWS S3 vai Azure Blob) tika ģenerēta īslaicīga piekļuves saite (izveidots pre signed URL), bet tā tika anulēta/atsaukta, pirms kāds to izmantoja (nav piekļuves žurnālu).
Cloud Security Posture Management (CSPM) rīks atklāja, ka testa / izstrādes vidē kādam pakalpojumam ir atļauti vāji kriptogrāfijas elementi vai novecojuši protokoli (novērsts tajā pašā dienā, nav ietekmēti klientu dati). Faktiska drošības ietekme nav konstatēta.
Trešo pušu/atkarību notikumi

[17] Komandlete (*cmdlet*) ir PowerShell specifisks termins, kas apzīmē nelielu, uzdevumu orientētu komandu. Tā veic noteiktas funkcijas un ir daļa no PowerShell vides, kas ir uzbūvēta uz .NET Framework.

CDN (*Content Delivery Network* – satura piegādes tīkls) mezgla lokāla anomālija ar automātisku re-routingu (bez gala lietotāju ietekmes).
Piegādātāja API "*rate limit*" sasniegts, atkārtota pieslēgšanās veiksmīga (bez funkcionalitātes zuduma) - trešās puses (piegādātāja) API uz īsu brīdi atteic pieprasījumus, jo sasniegts atļautais pieprasījumu daudzums (rate limit), bet klients automātiski atkārto pieprasījumu (*retry*) un pieprasījumi izdodas.
Trešo pušu plānotie uzturēšanas darbi, kad pakalpojums nav pieejams (paziņotā laika ietvaros).
Kriptogrāfija un uzticamība
Savlaicīga TLS sertifikāta derīguma brīdinājuma saņemšana - sertifikāts atjaunots laikus (bez pārtraukuma).
OCSP/CRL pieprasījumu sporādiski time-out, klients izmanto *stapling/caching* (nav savienojumu kļūmju).
Iekšējās PKI starpsertifikāta rotācija ar brīdinājumu SIEM, bez klientu ietekmes.
Notikumi, kas nav incidents
Atrastas ievainojamības (skenera atklājumi) bez ekspluatācijas — tas ir risks/uzdevums, nevis incidents.
Īslaicīgi elektroenerģijas padeves traucējumi.
Viltus trauksmes (*false positives*), kas apstiprināti kā nekaitīgi.
Publiski eksponēto resursu skenēšana (piem. ievainojamību meklēšana),ja tā nerada pieejamības traucējumus.

Pirms uzskatīt incidentu (vai notikumu) par maznozīmīgu, novērtējiet notikumu kontekstu: atkārtoti, mērķēti vai koordinēti mēģinājumi var vairs nebūt "maznozīmīgi". Ja iesaistīti aizsargājami dati (personas dati, komercnoslēpumi u.c.) vai ir jebkāda pieejamības/konfidencialitātes/integritātes ietekme, novērtējiet notikumu atbilstoši incidentu klasifikācijas kārtībai un nozīmīgumam.

Pat "maznozīmīgi" gadījumi jāreģistrē, jāmonitorē un jāseko notikumu attīstības tendencēm (sliekšņu pārsniegumi, jaunu TTP (*Tactics, Techniques and Procedures*) parādīšanās).

Jāņem vērā, ka vairākkārtēji vienveidīgi notikumi (no iepriekš minētajiem piemēriem), kā arī to kombinācija būtu uzskatāmi par notikumiem, kuriem ir kiberincidentu pazīmes, t.i. par kuriem būtu jāziņo.

5. APKOPOJUMS

Nacionālās kiberdrošības likuma subjekti:	Citi		
	Ziņošana par **nenozīmīgiem** kiberincidentiem	Ziņošana par **nozīmīgiem** kiberincidentiem	Ziņošana par jebkādien identificētiem kiberincidentiem
Būtisko pakalpojumu sniedzēji **Svarīgo** pakalpojumu sniedzēji IKT **kritiskās infrastruktūras** īpašnieks vai tiesiskais valdītājs	Par kiberdrošības incidentu, kurš nav uzskatāms par nozīmīgu, ziņo kompetentajai kiberincidentu novēršanas institūcijai, nosūtot uz e-pasta adresi cert@cert.lv kiberdrošības incidenta aprakstu brīvā formā	Par nozīmīgu kiberincidentu **nekavējoties informē kompetento kiberincidentu novēršanas institūciju** un izpilda tās sniegtos norādījumus par rīcību kiberincidenta gadījumā. Nosūtot aizpildītu un elektroniski parakstītu kiberincidenta ziņojuma formu uz cert@cert.lv	Par konstatēto kiberincidentu ir iespēja brīvprātīgi ziņot kompetentajai kiberincidentu novēršanas institūcijai CERT.LV, nosūtot aprakstu brīvā formā uz e-pasta adresi cert@cert.lv Kiberincidentu novēršanas institūcija CERT.LV vienojas ar personu, kura ziņojusi par kiberincidentu, par atbalsta sniegšanu kiberincidenta risināšanā (ja tāds nepieciešams). Brīvprātīga ziņošana neuzliek personai papildu pienākumus.
IKT **kritiskās infrastruktūras** īpašnieks vai tiesiskais valdītājs		Vienlaicīgi kiberincidenta ziņojuma formas nosūta **Satversmes Aizsardzības birojam.**	

6. IZMANTOTIE STANDARTI UN LABĀS PRAKSES APKOPOJUMI

- ISO/IEC 27035-1:2023
- ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27043: Incident investigation principles and processes.
- NIST SP 800-61 Rev. 3
- NIST SP 800-86 (Integrating Forensic Techniques)
- CISA National Cyber Incident Scoring System
- ENISA - Good Practice Guide for Incident Management
- ENISA - Reference Incident Classification Taxonomy
- RFC 3227: Guidelines for Evidence Collection and Archiving

PIELIKUMS Nr.: 1 RĪCĪBA KIBERINCIDENTA GADIJUMĀ

Tūlītējas darbības pirmajās minūtēs stundās pēc tam, kad notikums jūsu uzņēmuma IKT infrastruktūrā ir apstiprināts kā:

- **Aktivizējiet incidentu pārvaldības plānu** un informējiet savu atbildīgo personu incidentu risināšanas jomā.

- **Klasificējiet incidentu un nosakiet tā radītās ietekmes smaguma pakāpi**. Attiecīgi, vai notikušajam kiberincidentam ir "nozīmīga kiberincidenta pazīmes".

- **Ierobežojiet incidenta turpmāko izplatīšanos**.
  Atslēdziet skartās iekārtas no tīkla (fiziski atvienojot tīkla kabeli vai atslēdzot portu vai SSID), bet neatvienojot skartās iekārtas no elektrības barošanas avota (ja vien nepastāv tieši draudi). Iekārtu atslēgšana no barošanas avota var radīt pierādījumu zudumu. EDR/SOAR gadījumā izmantojiet "*network containment*" vai "*isolate host*".

- **Nekavējoties nodrošiniet digitālo pierādījumu saglabāšanu** (*digital forensic*).
  Nerestartējiet skartās iekārtas, nepārinstalējiet tās un neveiciet nekādas citas darbības, kamēr tehniskie speciālisti nav veikuši pilnīgu digitālo pierādījumu saglabāšanu. Par pierādījumu saglabāšanu skatīt detalizētā skaidrojumā tehniskajam personālam. Digitālo pierādījumu saglabāšanu uzticiet speciālistiem.

- **Veiciet piekļuves** (akreditācijas) **datu nomaiņu** (no drošas, "incidentā neskartas" iekārtas). Veiciet piespiedu paroles maiņu, MFA ieviešanu/atkārtotu reģistrāciju, API atslēgu rotāciju, OAuth tokenu anulēšanu.

- **Bloķējiet IoCs/TTPs**.
  IoC (Indicators of Compromise) – konkrēti, novērojami kompromitācijas indikatori, kas liecina par uzbrukumu vai infekciju.
  TTPs (Tactics, Techniques, and Procedures) – uzbrucēja mērķi un darbības veidi (uzvedība), nevis konkrēti artefakti.

- **Veiciet incidenta izmeklēšanas procesa dokumentēšanu**. Dokumentējiet **laika līniju** (kas, kur, kad, un kādas darbības ir veiktas, iesaistītais personāls un komandas; pieņemtos lēmumus un iemeslus). Uzturiet aprites ķēdes (chain of custody) uzskaiti.

- **Saziņa un paziņošana**.
  Iekšējā komunikācija: nodrošiniet skaidru, precīzu un operatīvu komunikāciju ar jūsu uzņēmuma atbildīgajiem darbiniekiem, ievērojot "need to know" principu.

Ārējā komunikācija: sazinieties un informējiet Kiberincidentu novēršanas institūciju CERT.LV. Nozīmīgu kiberincidentu gadījumā iesūtiet elektroniski parakstītu ziņojuma formu. Ja incidents nav novērtēts kā nozīmīgs – iesūtiet brīvas formas paziņojumu uz e-pasta adresi: cert@cert.lv.
Ja ir pamats uzskatīt, ka incidenta rezultātā ir konstatējamas noziedzīga nodarījuma sastāva pazīmes vērsieties ar iesniegumu **Valsts policijā** (īpaši izspiešanas, finanšu krāpšanas u.c. gadījumos).
Ja kiberincidents ir skāris fizisko personu datus (piem., datu noplūdes, neautorizētas piekļuves u.c.), ziņojiet **Datu valsts inspekcijai** saskaņā ar Vispārīgās datu aizsardzības regulas 2016/679 prasībām.
Ziņojiet kompetentajai valsts drošības iestādei (ja attiecināms).
Informējiet savus sadarbības partnerus un skartās puses (informējiet tikai par faktu kā tādu – neizpaužot informāciju par kiberincidenta būtību un skartajiem resursiem).

- Kad kiberincidenta kaitīgās sekas ir novērstas, **veiciet kiberincidenta seku analīzi** (*lessons learned*) un ieviesiet nepieciešamos uzlabojumus, lai šādi kiberincidenti turpmāk neatkārtotos.

PIELIKUMS Nr.: 2 INFORMĀCIJA PAR INCIDENTU UN TĀS SAGLABĀŠANA

Pierādījumi par notikušo incidentu jeb digitālie pierādījumi jāfiksē pēc "volatilitātes kārtības" (kas ātrāk zūd, to saglabā vispirms) un ar pierādāmu integritāti (hash, ķēdes-uzskaite).

Ļoti volatīlie - visnenoturīgākie (nekavējoties):

- RAM atmiņas *dumps*; pierakstiet izmantoto rīku un versiju.
- Darbojošos sistēmu momentuzņēmums: procesi, atvērtie faili/ligzdas, tīkla savienojumi/sesijas, ARP/rout.tabulas, kešatmiņas (DNS), ielādētās bibliotēkas, pakalpojumi, pierakstītie lietotāji, sistēmas laiks.
- Tīkla "*live*" dati: īstermiņa paketnoķeršana (PCAP), ugunsmūra/SLB/VPN sesiju tabulas, WAF/IDS buferi, load balancer "*stickiness*" tabulas.
- Konteineri/orkestratori: podu žurnāli (Kubernetes podos esošo konteineru izvadlogi (stdout/stderr). Tie atspoguļo pašas lietotnes darbību (piem., piekļuves žurnāli, kļūdas), kubectl logs ar –since, kube-audit, mezgla dmesg, īslaicīgie sidecar buferi.

Mazāk volatīlie, bet joprojām pastāv pierādījumu pazušanas risks:

- EDR/XDR telemetrijas eksports, SIEM neapstrādātie notikumi (*raw*), monitoringa alertu konteksts.
- Mākoņa auditlogi un plūsmas logi īsā glabāšanā: AWS CloudTrail/CloudWatch, GuardDuty atradnes, VPC Flow Logs; Azure Activity/Sign-ins, Defender for Cloud, NSG flow; GCP Audit/Flow logs.
- SaaS auditlogi ar īsu vēsturi: Okta/Azure AD/Google Workspace/O365, Slack, Atlassian, Git, M365 Unified Audit log.

Noturīgie sistēmas artefakti (resursdatori/VM):

- Pilns diska attēls (*bit-level*) ar rakstīšanas bloķētāju vai VM/cluster snapshot (momentuzņēmums – sistēmas stāvokļa kopija noteiktā laika punktā, ko var izmantot atjaunošanai, klonēšanai vai pierādījumu saglabāšanai incidentā); atsevišķi – pagefile/hiberfil, swap.
- Windows: EVTX (Security, System, Application, Microsoft-Windows-Sysmon/Operational, PowerShell/Operational, TaskScheduler, Windows Defender, WindowsUpdate), Prefetch, Amcache/RecentFileCache, ShimCache (AppCompatCache), SRUM, MFT/USN Journal/$LogFile/$J, LNK/JumpLists, Recycle Bin, Registry hives (SAM, SYSTEM, SOFTWARE, SECURITY, NTUSER.DAT, UsrClass.dat), RDP un RemoteDesktop-Services **žurnāli**, DNS Client **logs,** IIS u.c.
- Linux/macOS: journalctl pilns eksports, /var/log/* (auth/secure, syslog/messages, audit.log), wtmp/btmp/lastlog, sudo/cron/apt-yum/dnf, sshd, bash vēstures (ar laika zīmogiem), /etc konfigurācijas, pakotņu manifests, LaunchAgents/LaunchDaemons (macOS).

- E-pasts: servera žurnāli (SMTP/transport), M365/Exchange audit, lietotāju pastkastes (PST/EDB) ar legal hold; SPF/DKIM/DMARC pārskati.
- Identitāte: AD domain controller Security logs, Azure AD sign-in/risk logs, MFA/Conditional Access, PAM žurnāli.
- Tīkls/perimetrs: ugunsmūru žurnāli, NetFlow/IPFIX, DNS resolvera/rekurzīvā DNS žurnāli, proxy/CASB, VPN, WAF/IDS/IPS, DLP, e-pasta vārtejas.
- Lietotnes/DB: web serveru piekļuves/kļūdu žurnāli, aplikāciju audit, API vārtejas, DB audit/transaction logi, konfigurāciju snapshoti.

Trešo pušu dati:

- Piegādātāju un hostinga pakalpojumu logi, CDN, maksājumu vārtejas, SMS/telefoni (MFA).
- MDM/EMM telemetrija (mobilās iekārtas), EMM audit.

Saglabāšanas secība (Order of Volatility – balstīts uz RFC 3227, ISO/IEC 27037):

- CPU/reģistri/kešatmiņa – praktiski netverami lauka apstākļos.
- RAM un dzīvie stāvokļi (ir visas īslaicīgās sistēmas darba laikā esošās lietas, kas eksistē tikai ieslēgtā sistēmā un ātri mainās vai pazūd pie izslēgšanas, restartēšanas vai arī laika gaitā) (procesi, savienojumi, buferi).
- Tīkla "in-flight" dati un sesiju tabulas; īslaicīgie mākoņa un konteineru žurnāli.
- Pagaidu faili un mainīgie logi lokālajās sistēmās.
- Pastāvīgā krātuve: disku/VM/klāstera snapshoti, failu sistēma, e-pasti, DB žurnāli.
- Attālās sistēmas un trešo pušu arhīvi.
- Rezerves kopijas un ilgtermiņa arhīvi.

Pierādījumu ticamība. Kā saglabāt digitālos pierādījumus, lai tie būtu izmantojami kā pierādījumi:

- Integritāte: katram artefaktam ģenerē SHA-256/SHA-512 hash; glabā hash atsevišķi; parakstiet, ja iespējams.
- Aprites ķēdes uzskaite (*chain of custody*): unikāls ID, apraksts, laiks, metode/rīks, persona, atrašanās vieta, katrs nodošanas posms ar parakstu.
- "Strādā ar kopijām" oriģinālus aizzīmogo; analīzi veic uz kopijām, kas tiek radītas digitālās izmeklēšanas mērķim (*digital forensic*).
- Rīki: izmanto uzticamu, versijotu rīku komplektu no tikai-lasāma nesēja; pierakstiet versijas un komandas.
- Laika sinhronizācija: NTP pierādījumi, laika josla, UTC atzīmes.
- Drošība: glabā šifrētā, piekļuves kontrolētā repozitorijā (WORM, S3 Object Lock un tml.); ierobežo piekļuvi "*need-to-know*"; reģistrē katru piekļuves faktu (logo piekļuvi).

Datu minimizācija/privātums: ievēro Vispārīgās datu aizsardzības regulas 2016/679 un nacionālos normatīvos aktus; uz incidentu datiem piemēro "*legal hold*" pamatprincipu (pierādījumi tiek vākti un saglabāti, lai izpildītu ar likumu uzliktu pienākumu) un definē glabāšanas termiņu.