Nacionālais kiberdrošības centrs

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

Rezerves kopiju veidošanas vadlīnijas

Saskaņā ar Ministru kabineta 2025.gada
25.jūnija noteikumiem Nr. 397

Šīs vadlīnijas izstrādātas, lai palīdzētu Nacionālās kiberdrošības likuma subjektiem (būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un IKT kritiskās infrastruktūras īpašniekiem) un citām organizācijām izveidot un uzturēt efektīvu rezerves kopiju sistēmu, ievērojot gan Nacionālās kiberdrošības likuma, gan kiberdrošības labās prakses principus.

Izstrādātājs – CERT.LV

Versija 1.1, 13.01.2026

SATURS

1. IEVADS

Mūsdienās informācijas sistēmu pieejamība un datu integritāte ir kļuvušas par būtisku priekšnoteikumu ne tikai uzņēmumu un valsts iestāžu darbībai, bet arī sabiedrības kopējai drošībai. Pieaugot kiberapdraudējumu un kiberdrošības incidentu (turpmāk kopā arī – **incidenti**) biežumam, organizācijām ir arvien nopietnāk jādomā par to, kā nodrošināt būtisko datu saglabāšanu un informācijas sistēmu operatīvu atjaunošanu pēc incidenta, lai spētu turpināt darbību bez būtiskiem pārtraukumiem.

Lai to panāktu, ir nepieciešams veidot rezerves kopijas – tās ir datu un/vai sistēmu un to konfigurācijas dublējumi, kas tiek uzglabāti neatkarīgi no primārās sistēmas. To galvenais mērķis ir nodrošināt iespēju atjaunot datus vai sistēmas pēc dažādiem incidentiem, tostarp kiberuzbrukumiem, tehniskām kļūmēm, cilvēku pieļautām kļūdām, dabas katastrofām vai citiem ārkārtas gadījumiem.

1.1. MĒRĶIS UN PIEMĒROŠANAS JOMA

Šīs vadlīnijas izstrādātas ar mērķi palīdzēt organizācijām izveidot un uzturēt efektīvu rezerves kopiju sistēmu, ievērojot gan Nacionālās kiberdrošības likuma (turpmāk – **NKDL**) prasības, gan kiberdrošības labās prakses principus. Lai gan vadlīnijās īpaši ņemti vērā NKDL un uz tā pamata izdoto 2025. gada 25. jūnija Ministru kabineta noteikumu Nr. 397 "Minimālās kiberdrošības prasības" (turpmāk – **MK Nr. 397**) nosacījumi, tās ir piemērojamas arī organizācijām, kuras nav NKDL subjekti, taču kuru darbība ir atkarīga no informācijas sistēmu darbspējas un pieejamības.

Vienlaikus katrai organizācijai pašai jāizvērtē, vai uz to attiecas kādi speciālie normatīvie akti, kuros var būt noteiktas atšķirīgas vai papildinošas prasības attiecībā uz rezerves kopiju veidošanu un glabāšanu. Šādos gadījumos ir piemērojamas speciālo likumu prasības, ciktāl tās nodrošina vismaz tikpat augstu kiberdrošības līmeni, kādu paredz NKDL.

Vadlīnijās izmantots vispārīgs apzīmējums "organizācija", kas attiecināms uz visiem NKDL subjektiem, tostarp valsts un pašvaldību iestādēm, kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem, kā arī uz jebkuru citu informācijas sistēmu īpašnieku, kas vēlas veidot savu rezerves kopiju sistēmu, balstoties uz šīm vadlīnijām.

Šīs vadlīnijas paredzētas galvenokārt kiberdrošības pārvaldītājiem, taču tās var būt noderīgas arī informācijas tehnoloģiju un informācijas drošības speciālistiem, kā arī organizāciju vadītājiem, kas pieņem stratēģiskus lēmumus par kiberdrošības nodrošināšanu.

1.2. REZERVES KOPIJU NOZĪME

Mūsdienu organizācijas ikdienas darbība būtiski balstās uz informācijas sistēmu un datu pieejamību. Šādos apstākļos datu zudums, bojājums vai nepieejamība, neatkarīgi no tā, vai tas rodas ļaunprātīga uzbrukuma, cilvēka kļūdas vai tehniskas kļūmes rezultātā, var radīt būtiskas sekas organizācijas darbībai, tās reputācijai un pat sabiedrības drošībai kopumā.

Rezerves kopiju sistēma ir viens no galvenajiem mehānismiem informācijas sistēmu un datu aizsardzībā, kas ļauj atjaunot zaudēto vai bojāto informāciju pēc incidenta. Tās galvenais uzdevums ir nodrošināt iespēju atgriezt informācijas sistēmas darbspējīgā stāvoklī un atjaunot datus pēc iespējas pilnīgākā un aktuālākā veidā.

Vienlaikus ir svarīgi atšķirt rezerves kopiju sistēmu no darbības nepārtrauktības plāna. Rezerves kopiju izveide un pārvaldība palīdz pārvaldīt informācijas zuduma risku un nodrošina

datu atjaunošanu incidenta gadījumā. Savukārt darbības nepārtrauktības plāns ir plašāks organizatorisks ietvars, kas aptver gan tehniskus, gan organizatoriskus pasākumus, lai nodrošinātu organizācijas spēju turpināt darbību traucējumu, t.sk., katastrofu apstākļos. Tas var ietvert, piemēram, pāreju uz alternatīvām informācijas sistēmām, komunikācijas procedūras, personāla aizvietošanas plānus, u.c. Lai gan rezerves kopijas ir svarīgas nepārtrauktības nodrošināšanai, ar tām vien nepietiek, lai pilnībā pasargātu organizāciju un novērstu incidentu radītās sekas.

Labi izstrādāta un pārvaldīta rezerves kopiju sistēma palīdz ne tikai nodrošināt atbilstību normatīvo aktu prasībām, bet arī stiprina organizācijas vispārējo noturību, garantējot datu pieejamību un integritāti. Efektīva rezerves kopiju sistēma būtiski samazina dažādu risku ietekmi uz organizāciju, tostarp:

- izspiedējvīrusu (*ransomware*) uzbrukumu sekas, kas var padarīt datus nepieejamus;
- iekšējo draudu ietekmi, piemēram, personāla tīšas vai netīšas kļūdas;
- tehnisku kļūmju radītus bojājumus;
- fizisku ārējo apdraudējumu sekas, piemēram, ugunsgrēkus, plūdus vai elektroapgādes pārtraukumus.

2. REGULĒJUMS

2.1. NACIONĀLĀS KIBERDROŠĪBAS LIKUMS UN MINIMĀLĀS KIBERDROŠĪBAS PRASĪBAS

NKDL ir viens no galvenajiem normatīvajiem aktiem kiberdrošības jomā Latvijā, kas transponē Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2555 (t.s. Tīklu un informācijas sistēmu drošības direktīva jeb TID 2) prasības, kā arī ietver papildu regulējumu, kas atbilst Latvijas nacionālajai kiberdrošības politikai un vajadzībām. Saskaņā ar NKDL 26. pantu Ministru kabinetam ir deleģētas tiesības noteikt kārtību, kādā subjekti nodrošina savu tīklu un informācijas sistēmu atbilstību minimālajām kiberdrošības prasībām. Tas ietver arī prasības un pasākumus, kas nodrošina informācijas sistēmu konfidencialitāti, integritāti, pieejamību, kā arī spēju atjaunot datus incidenta gadījumā.

Detalizēti noteikumi par rezerves kopiju sistēmu veidošanu NKDL subjektiem ir ietverti 2025. gada 25. jūnija Ministru kabineta noteikumos Nr. 397 "Minimālās kiberdrošības prasības", jo īpaši šo noteikumu 3.10. nodaļā ("Rezerves kopiju pārvaldība"). Šie noteikumi paredz, ka organizācijām jānodrošina rezerves kopiju veidošana katrai to īpašumā vai valdījumā esošajai informācijas sistēmai. Rezerves kopiju izveidei un pārvaldībai ir jāatbilst attiecīgajai sistēmas drošības klasifikācijas klasei, kas tiek noteikta saskaņā ar MK Nr. 397 5. pielikumu.

MK Nr. 397 prasības neaprobežojas ar klasisko izpratni par datu rezerves kopiju veidošanu. Noteikumi uzsver arī rezerves kopiju veidošanas nepieciešamību, lai nodrošinātu pilnīgu informācijas sistēmas atjaunošanas spēju incidentu gadījumā. Tas nozīmē rezerves kopiju veidošanu ne tikai glabātajiem datiem, bet arī informācijas sistēmas arhitektūras un konfigurācijas datu glabāšanu un aizsargāšanu no zudumiem. Tādējādi, MK Nr. 397 nodrošina detalizētu un praktiski īstenojamu regulējumu efektīvas rezerves kopiju sistēmas izveidei un uzturēšanai.

3. REZERVES KOPIJU VEIDI, TO ATRAŠANĀS VIETAS

Efektīvas rezerves kopiju sistēmas izveidei būtiski ir izvēlēties atbilstošāko rezerves kopiju veidu un glabāšanas risinājumu, ņemot vērā organizācijas darbības specifiku, risku novērtējumu un nepieciešamo datu atjaunošanas ātrumu. Izvēle starp dažādām rezerves kopiju metodēm ir saistīta ar to, cik bieži tiek veiktas kopijas, cik lielu datu apjomu nepieciešams dublēt, un cik ātri dati jāatjauno incidenta gadījumā (RTO (*Recovery Time Objective*) un RPO (*Recovery Point Objective*) rādītāji, kas detalizētāk skaidroti šo vadlīniju 4. nodaļā).

3.1. REZERVES KOPIJU VEIDI

Rezerves kopiju veidu izvēle ir atkarīga no vairākiem faktoriem – apstrādāto datu apjoma, sistēmas tehniskajām iespējām, riska tolerances, kā arī no tā, cik bieži un cik ātri nepieciešams atjaunot datus pēc incidenta. Katram kopiju veidam ir savas priekšrocības un ierobežojumi, un nereti efektīvākos rezultātus sniedz dažādu pieeju kombinēšana. Galvenokārt izšķir šāda veida rezerves kopiju veidus:

- **Pilna kopija**: Pilna rezerves kopija ir vienkāršs un pilnīgs dublēšanas veids, kurā tiek saglabāti visi atlasītie dati, neatkarīgi no izmaiņām. Tā nodrošina vienkāršāku datu atjaunošanu, jo visi faili ir vienā kopijā, taču tās izveide aizņem vairāk laika un vietas. Tāpēc pilnas kopijas parasti veido periodiski, piemēram, reizi nedēļā, kombinējot tās ar citiem dublēšanas veidiem. Mazām sistēmām vai kritiskiem datiem pilnas kopijas var veikt arī katru dienu;
- **Inkrementālā kopija**: Inkrementālā kopija saglabā tikai tos datus, kas mainījušies kopš pēdējās kopijas (pilnās vai inkrementālās), veidojot secīgu dublējumu ķēdi. Tā samazina glabāšanas apjomu un izveides laiku, taču sarežģī atjaunošanu, jo nepieciešama gan pēdējā pilnā, gan visas sekojošās inkrementālās kopijas. Ja kāda no tām nav pieejama, dati var nebūt pilnībā atjaunojami;
- **Diferenciālā kopija**: Diferenciālā kopija saglabā visus datus, kas mainījušies kopš pēdējās pilnās kopijas. Atšķirībā no inkrementālās, tā katru reizi salīdzina ar pilno kopiju, nevis iepriekšējo diferenciālo. Datu atjaunošanai nepieciešamas tikai divas kopijas – pilnā un pēdējā diferenciālā, kas padara procesu vienkāršāku un uzticamāku. Tomēr katra nākamā diferenciālā kopija aizņem vairāk vietas un ilgāku laiku, jo iekļauj visas uzkrātās izmaiņas;
- **Snapshot (*momentuzņēmums*)**: Snapshot, jeb momentuzņēmums fiksē sistēmas vai datu glabāšanas vides stāvokli noteiktā brīdī, ļaujot ātri atjaunot sistēmu, ja pēc izmaiņām rodas problēmas. Tas ir noderīgs testēšanai un kļūdu novēršanai, taču nav pilnvērtīga rezerves kopija, jo parasti tiek glabāts tajā pašā vidē kā oriģinālie dati. Līdz ar to tas ir labs papildinājums, bet ne aizstājējs tradicionālajām dublēšanas metodēm.

Rezerves kopiju veidu salīdzinošā tabula, kas atspoguļo galvenās priekšrocības un ierobežojumus:

Veids	Apraksts	Priekšrocības	Trūkumi
Pilna kopija	• Tiek izveidota visu izvēlēto datu pilna kopija	• Vienkāršākais atjaunošanas process • Skaidra un pilnīga datu struktūra	• Liels glabāšanas apjoms • Ilgs kopēšanas laiks, īpaši pie lieliem datu apjomiem
Inkrementālā kopija	• Saglabātā tikai izmaiņas kopš iepriekšējās kopijas (jebkāda veida)	• Ātra izveide • Mazs glabāšanas apjoms	• Atjaunošanai nepieciešamas visas iepriekšējās inkrementālās kopijas un pilnā kopija
Diferenciālā kopija	• Saglabā visas izmaiņas kopš pēdējās pilnās kopijas	• Ātrāka un vienkāršāka atjaunošana nekā inkrementālajai kopijai	• Apjoms pieaug ar katru nākamo kopiju līdz nākamajai pilnajai kopijai
Snapshot	• Sistēmas stāvokļa fiksācija konkrētā brīdī, bieži izmantots operētājsistēmās vai virtualizācijas vidē.	• Ļoti ātra izveide • Noderīga testēšanai vai konfigurācijas saglabāšanai	• Īslaicīgs sistēmas vides stāvokļa fiksācijas veids nevis rezerves kopija • Parasti glabājas tajā pašā primārajā sistēmā – nav aizsardzības pret sistēmas kompromitēšanu

Ņemot vērā, ka katram rezerves kopiju veidam ir savas priekšrocības un ierobežojumi, praksē bieži tiek kombinēti dažādi rezerves kopiju veidi. Piemēram, var tikt veiktas ikdienas inkrementālās kopijas un periodiskas (piemēram, reizi nedēļā) pilnās kopijas. Šāda pieeja ļauj efektīvi sabalansēt glabāšanas resursus un atjaunošanas ātrumu, ievērojot riska izvērtējumā noteiktās vajadzības.

3.2. REZERVES KOPIJU GLABĀŠANAS VEIDI

Būtisks lēmums, izstrādājot rezerves kopiju sistēmu, ir noteikt, kur šīs kopijas tiks glabātas. Tāpat kā rezerves kopiju veidiem, arī glabāšanas risinājumiem ir savas priekšrocības un ierobežojumi, kas rūpīgi jāizvērtē, ņemot vērā datu vērtību, sistēmas arhitektūru un pieejamos resursus. Galvenokārt izšķir šādus rezerves kopiju glabāšanas veidus:

- **Lokālās rezerves kopijas** (*on-premise*): Lokālās rezerves kopijas tiek glabātas tajā pašā infrastruktūrā kā primārie dati – uz vietējiem serveriem, NAS / SAN (*Network Attached Storage* / *Storage Area Network*) ierīcēm vai ārējiem datu nesējiem. Tās nodrošina ātru piekļuvi un atjaunošanu, kā arī pilnīgu kontroli pār glabāšanu un drošību. Tomēr tās ir pakļautas riskam, ja viss atrodas vienā fiziskā vietā. Tāpēc lokālās kopijas bieži kombinē ar attālinātiem vai mākoņrisinājumiem, lai uzlabotu datu drošību un noturību pret incidentiem;
- **Attālinātās rezerves kopijas** (*off-site*): Attālinātās rezerves kopijas tiek glabātas citā fiziskā vietā nekā primārā sistēma, pasargājot datus no lokāliem apdraudējumiem, piemēram, ugunsgrēkiem, plūdiem vai zādzībām. Tās var atrasties citā birojā, partnera telpās, datu centrā vai mākoņpakalpojumos. Šāda pieeja nodrošina datu pieejamību pat pilnīgas primārās infrastruktūras zaudēšanas gadījumā;
- **Mākoņrisinājuma rezerves kopijas** (*cloud*): Mākoņrisinājuma rezerves kopijas ir attālinātas kopijas, kas izmanto mākoņpakalpojumus datu glabāšanai. Tās piedāvā elastīgu un mērogojamu risinājumu, īpaši piemērotu organizācijām, kas vēlas samazināt

fiziskās infrastruktūras izmaksas. Šādi risinājumi bieži tiek izmantoti mazāk kritiskiem datiem vai kā daļa no hibrīda pieejas.

Izvēloties mākoņpakalpojumu, svarīgi pārliecināties par sniedzēja drošības līmeni un datu atjaunošanas iespējām. Jāņem vērā, ka pakalpojums ne vienmēr automātiski ietver rezerves kopiju izveidi, tas var būt klienta atbildībā vai pieejams kā atsevišķs maksas pakalpojums.

Pirms izvēlēties mākoņpakalpojumu, organizācijai jānodrošina, ka līgumā skaidri definēti pakalpojumu sniedzēja pienākumi attiecībā uz rezerves kopijām, kā arī organizācijas tiesības datu aizsardzības un kiberdrošības jomā. Pakalpojuma izmantošanai jāatbilst organizācijas kiberpārvaldības politikām, riska izvērtējumiem un darbības nepārtrauktības plānam. Tāpat kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem būtu ieteicams mākoņpakalpojumu izvēli jau sākotnēji saskaņot ar Satversmes aizsardzības biroju, lai pārliecinātos, ka izvēlētais risinājums atbilst noteiktajai riska politikai un neietver nepieņemamus apdraudējumus.

Līgumā būtu jāiekļauj šādi būtiski punkti:

- prasības attiecībā uz rezerves kopiju esamību, pieejamību un atjaunošanas termiņiem;
- datu glabāšanas ilgums un dzēšanas procedūras pēc līguma vai pakalpojuma pārtraukšanas;
- pakalpojuma sniedzēja tiesības piekļūt organizācijas datiem;
- informēšana par incidentiem, iespējas veikt incidentu izmeklēšanu un piekļūt sistēmas žurnālfailiem;
- tiesības veikt auditu vai iespēju pārskatīt neatkarīgu pušu revīzijas vai audita ziņojumus;
- informācijas drošības kontroles, tostarp datu šifrēšanas prasības pārsūtīšanas laikā un glabājot, piekļuves un autentifikācijas kontroles, kā arī informācija par šifrēšanas atslēgu pārvaldību;
- datu glabāšanas vieta / valsts;
- iespējas pārnest datus uz citu pakalpojumu sniedzēju, lai novērstu piesaistes vienam piegādātājam (*vendor lock-in*) risku.

Svarīgi ir izvērtēt, kurā valstī tiks glabāti organizācijas dati, jo datu uzglabāšana ārpus ES/EEZ var radīt papildu riskus, ja attiecīgās valsts regulējums nenodrošina pietiekamu datu aizsardzības līmeni. Īpaša uzmanība jāpievērš personas datu aizsardzībai (saskaņā ar Vispārīgo datu aizsardzības regulu) un kritiskās informācijas (piemēram, atbilstoši MK noteikumiem Nr. 397) glabāšanai. Jānorāda, ka rezerves kopiju izvietošanai ārpus subjekta IKT infrastruktūras būs jāpiemēro arī topošo MK noteikumu "Informācijas sistēmu izvietošanas un datu centru drošības prasības" nosacījumi par teritorijas un datu centru izvēli, kad tie stāsies spēkā.

Lai gan mākoņrisinājumi piedāvā elastību un izmaksu efektivitāti, tie var radīt arī drošības un atbilstības riskus. Tāpēc mākoņrisinājumi būtu jāizmanto kā daļa no hibrīda dublēšanas pieejas, apvienojot to priekšrocības ar lokālajām un attālinātajām kopijām, tādējādi uzlabojot datu aizsardzību un noturību.

Minimālās kiberdrošības prasības!

MK Nr. 397 4. nodaļa (Ārpakalpojuma prasības) nosaka nosacījumus un ierobežojumus ārpakalpojumu izmantošanai, kas ir jāievēro NKDL subjektiem. Šīs prasības

attiecas arī uz gadījumiem, kad rezerves kopiju veidošana, glabāšana vai uzturēšana tiek nodota trešajām pusēm (ārpakalpojumu sniedzējiem), piemēram, izmantojot ģeogrāfiski attālinātus datu centrus vai mākoņpakalpojumus. Cita starpā noteikumi paredz vispārēju aizliegumu slēgt ārpakalpojumu līgumu ar ārpakalpojuma sniedzēju, kas reģistrēts Krievijas Federācijā, Baltkrievijas Republikā, vai valstī, kas atzīta par terorismu atbalstošu valsti, vai tā patiesā labuma guvēji ir šo valstu pilsoņi. Savukārt kritiskās infrastruktūras īpašniekiem un tiesiskajiem valdītājiem ārpakalpojuma līgumu par A klases informācijas sistēmas tehnisko resursu iegādi atļauts slēgt, ja ārpakalpojuma sniedzējs un tehniskā resursa ražotājs atbilst MK Nr.397 94.punktam, tai skaitā ārpakalpojuma sniedzējam ir jābūt reģistrētam NATO, Eiropas Savienības vai EBTA dalībvalstī vai NATO Indijas un Klusā okeāna reģiona sadarbības valstī (turpmāk - IP4).

Papildus, kopiju izvietošanai ārpus subjekta IKT infrastruktūras, tai skaitā, izmantojot ārpakalpojumus, būs jāpiemēro arī topošo Ministru kabineta noteikumu "Informācijas sistēmu izvietošanas un datu centru drošības" prasības, kad noteikumi stāsies spēkā. Ir paredzams, ka šie noteikumi arī paredzēs, ka datu centrs, kurā uztur informācijas sistēmu vai tās daļu, tostarp rezerves kopiju sistēmas, drīkstēs atrasties tikai NATO, Eiropas Savienības, EBTA vai IP4 dalībvalstu teritorijā.

- **Hibrīda rezerves kopijas**: Hibrīdā pieeja rezerves kopiju veidošanā, apvienojot lokālās un mākoņrisinājuma priekšrocības, nodrošina gan ātru datu atjaunošanu no lokālajām kopijām, gan aizsardzību pret riskiem, izmantojot attālinātas kopijas, piemēram, pret kiberuzbrukumiem vai dabas katastrofām. Tā ļauj pielāgoties dažādiem atjaunošanas mērķiem, taču prasa rūpīgu plānošanu, piemēram, jānosaka, kuri dati tiek glabāti vai kur un kādos gadījumos tiek veikta to atjaunošana.
- **Izolētas rezerves kopijas** (*air-gapped*): Izolētas rezerves kopijas, kas tiek glabātas ārpus tīkla, ir viena no drošākajām aizsardzības metodēm pret kiberapdraudējumiem, īpaši izspiedējvīrusiem, jo tās nav pieejamas no kompromitētām sistēmām. Tās tiek veidotas uz noņemamiem nesējiem un pēc kopēšanas tiek atvienotas no infrastruktūras un tīkla. Lai gan šī pieeja nodrošina augstu datu noturību, tā prasa manuālu apstrādi līdz ar to ir mazāk piemērota biežām kopijām un kavē ātru datu atjaunošanu.

Tabulā apkopoti galvenie rezerves kopiju veidi ar to priekšrocībām un ierobežojumiem. Izvēloties risinājumu, svarīgi ņemt vērā organizācijas specifiku, datu aizsardzības prasības un atjaunošanas vajadzības, jo katram veidam ir savi plusi un mīnusi, kas ietekmē sistēmas nepārtrauktību un drošību konkrētos apstākļos:

Veids	Priekšrocības	Ierobežojumi
Lokālās kopijas	• Ātra piekļuve un atjaunošana • Pilna kontrole pār datiem un drošību.	• Var tikt kompromitēta kopā ar primāro sistēmu (piemēram, izspiedējvīruss) • Fiziskie incidentu riski
Attālinātas kopijas	• Aizsardzība pret lokāliem incidentiem • Uzlabota darbības nepārtrauktība dabas katastrofu gadījumā	• Nepieciešama papildu vai trešo pušu infrastruktūra • Lielāks atjaunošanās laiks
Mākoņ-risinājumu	• Elastība, mērogojamība • Automatizēta pārvaldība • Ārēja lokācija	• Datu aizsardzības un šifrēšanas jautājumi • Trešo valstu jurisdikcija • Atkarība no trešās puses

kopijas		• Ilgtermiņa izmaksas
Hibrīda pieeja	• Apvieno lokālo un attālināto rezerves kopiju priekšrocības: ātra lokālā atjaunošana + droša ārēja kopija	• Sarežģītāka pārvaldība • Izmaksas
Izolētas kopijas (*air-gapped*)	• Izolācija no incidentiem pret galveno infrastruktūru • Aizsardzība pret iekšējiem draudiem • Augsta uzticamība pilnīgas sistēmas atteices gadījumā	• Lēnāka datu atjaunošana • Manuāli procesi kopiju veidošanai un pārnešanai, papildus izmaksas • Nav piemērota ikdienas datu atjaunošanai

Rezerves kopiju sistēmu efektivitāte ir cieši saistīta ar to glabāšanas vietas izvēli un kopiju pieejamību incidenta gadījumā. Rezerves kopiju sistēmai jāspēj izturēt gan fiziskus draudus (piemēram, ugunsgrēku, plūdus, nesankcionētu personu piekļuvi), gan kiberuzbrukumus. Izvēloties rezerves kopiju glabāšanas vietu, organizācijai jāvērtē iespējamie riski un ieguvumi no dažādiem risinājumiem. Tāpat jāizvērtē spējas nodrošināt attiecīgajā vietā pietiekamu datu drošību un pieejamību atbilstoši organizācijas darbības nepārtrauktības plānam.

Minimālās kiberdrošības prasības!

MK Nr. 397 72.2. punkts paredz, ka A klases informācijas sistēmai vismaz vienai pilnai rezerves kopijai ir jābūt uzglabātai, nodrošinot atbilstību visām šādām prasībām:

- **no informācijas sistēmas atdalītos tehniskajos resursos** - rezerves kopijas tiek glabātas tehniski un loģiski nošķirtā vidē, kur tās nevar tikt izdzēstas, pārrakstītas vai citādi ietekmētas no primārās informācijas sistēmas. Šāda nošķirtība var tikt nodrošināta, piemēram, glabājot datus datu centrā ar neatkarīgu piekļuves pārvaldību un autentifikācijas mehānismiem, izmantojot starpsistēmu rezerves kopiju pārnešanai. Starpsistēma darbojas kā kontrolēts starpposms starp primāro sistēmu un glabāšanas vidi, tā tiek īslaicīgi savienota tikai rezerves kopijas izveides laikā. Šī prasība obligāti neparedz pilnīgi izolēti vidi vai izolētas kopijas veidošanu, taču nosaka pienākumu nodrošināt pietiekamu tehnisko un loģisko nošķirtību, lai viena incidenta rezultātā, kas skar primāro sistēmu, netiktu vienlaikus bojātas arī rezerves kopijas;
- **ģeogrāfiski attālinātā vietā**, piemēram, datu centrā, kas neatrodas tajā pašā fiziskajā vietā, kur izvietota primārā sistēma. Šāda pieeja nodrošina aizsardzību pret lokālām katastrofām (ugunsgrēkiem, plūdiem vai citiem vides riskiem);
- **telpās, kas aizsargātas pret nesankcionētu piekļuvi un aprīkotas ar automātisko ugunsgrēka atklāšanas un trauksmes signalizācijas sistēmu**. Šādai telpai jāspēj nodrošināt rezerves kopiju aizsardzību pret fiziskiem draudiem, vides faktoriem un iekārtu bojājumiem.

3.3. 3-2-1 PRINCIPS REZERVES KOPIJU IZVEIDĒ

Lai nodrošinātu augstu datu aizsardzības līmeni, rezerves kopiju sistēmas izveidē bieži tiek pielietots 3-2-1 princips. Šis princips palīdz samazināt datu zudumu risku, balstoties uz dažādu rezerves kopiju un to glabāšanas risinājumu vienlaicīgu izmantošanu.

3-2-1 princips paredz:

- **3 kopijas:**
  - Datiem ir jābūt vismaz trīs kopijās;
  - Tas nozīmē - 1 darba kopija (oriģināls) un vismaz 2 rezerves kopijas.

- **2 dažādi datu nesēji:**
    - Dati jāglabā vismaz uz diviem dažādiem tehniskajiem resursiem;
    - Piemēram, lokālais disks un mākoņglabātuve.
- **1 kopija ģeogrāfiski atdalītā vietā:**
    - Vismaz viena rezerves kopija jāuzglabā ģeogrāfiski citā vietā nekā primārā sistēma, lai aizsargātu datus lokālas katastrofas gadījumā.

Piemērs: lai ievērotu 3-2-1 principu, organizācija var glabāt darba kopiju savā serverī, vienu rezerves kopiju NAS iekārtā tajās pašās telpās un otru pie mākoņpakalpojumu sniedzēja vai trešās puses datu centrā, kas neatrodas tajā pašā fiziskajā vietā, kur izvietota primārā sistēma Šāda pieeja nodrošina augstu datu pieejamību un aizsardzību pret dažādiem draudiem, tai skaitā lokālām katastrofām. Turklāt tā atbilst arī normatīvajām prasībām, piemēram, MK Nr. 397 72.2 punktam attiecībā uz A klases informācijas sistēmām. Tomēr 3-2-1 ir tikai viens no iespējamiem modeļiem – rezerves kopiju stratēģija jāpielāgo katras organizācijas vajadzībām, tehniskajām iespējām un riskiem.

Piemērs: 3-2-1 princips nosaka paaugstinātas drošības prasības rezerves kopiju organizēšanai, jo tas paredz papildu aizsardzības slāņus primārajai rezerves kopiju sistēmai, nodrošinot vismaz vienu papildu rezerves kopiju. Šis princips nav noteikts MK Nr. 397 prasībās, tādēļ subjektiem tas nav obligāts. Tomēr, pamatojoties uz riska izvērtējumu un darbības nepārtrauktības prasībām, subjekti var pieņemt lēmumu to ieviest pilnā apjomā vai daļēji. Piemēram, subjekts var veidot nevis divas rezerves kopijas katrai darba kopijai, bet gan piemērot papildu kopiju nepieciešamību tikai dienas un nedēļas rezerves kopijām, ja tas atbilst identificētajiem riskiem un sistēmas / datu kritiskumam.

Lai arī 3-2-1 princips ir saistīts ar rezerves kopiju drošību, tas nenosaka kopiju veidošanas biežumu. Rezerves kopiju izveides biežums ir skaidrots šo vadlīniju 4.2. punktā, kas arī paskaidro MK Nr. 397 70. punktā noteiktās prasības.

4. REZERVES KOPIJU PLĀNOŠANA

Efektīva rezerves kopiju sistēma sākas ar pārdomātu plānu, kas balstīts uz organizācijas vajadzībām, sistēmu kritiskumu un atjaunošanas prasībām. Šāds plāns nodrošina ne tikai datu drošību un atbilstību normatīvajām prasībām, bet arī spēju ātri un uzticami atjaunot datus pēc incidentiem, tādējādi saglabājot darbības nepārtrauktību.

4.1. KĀDIEM DATIEM JĀTAISA REZERVES KOPIJAS

Pirms rezerves kopiju veidošanas jāveic datu atlase, balstoties uz riska un ietekmes analīzi, ņemot vērā sistēmu funkcionalitāti un nozīmīgumu. Tas nodrošina, ka kritiskie dati ir pienācīgi aizsargāti un ātri atjaunojami pēc incidenta.

Lai noteiktu, kuriem datiem jāveido rezerves kopijas, organizācijai jāatbild uz vairākiem jautājumiem:

- Vai šo datu zudums ietekmētu organizācijas spēju netraucēti sniegt pakalpojumus klientiem vai sabiedrībai?
- Vai attiecīgo datu zudums ietekmētu organizācijas iekšējos procesus vai darbības nepārtrauktību?
- Vai datu zudums varētu radīt juridiskas, reputācijas vai finanšu sekas organizācijai?
- Vai šie dati, tai skaitā to pieejamība, ir aizsargājami saskaņā ar normatīviem aktiem (piemēram, personas dati, komercnoslēpums, valsts noslēpums)?
- Vai šie dati ir unikāli, vai tie var tikt iegūti no citiem avotiem (piemēram, trešās puses datubāzēm)?

Papildus lietotāju, klientu un citiem organizācijā izmantojamajiem datiem, arī sistēmas konfigurācijas faili, izpildāmais kods, atbalsta programmatūra un citi ar informācijas sistēmas darbību saistīti dati ir jāiekļauj rezerves kopijās. Tas nepieciešams, lai nodrošinātu datu, kā arī pilnīgu informācijas sistēmas atjaunošanai pēc incidenta.

Audita un žurnālfailu dati, kas ir būtiski incidentu izmeklēšanai un atbildības noteikšanai, jāiekļauj rezerves kopijās un jāglabā atsevišķi no primārās sistēmas, piemēram, centralizētā žurnālfailu glabātuvē vai SIEM, lai tie paliktu neskarti dažādu incidentu gadījumos.

Ja rezerves kopijās tiek iekļauti personas dati, organizācijai ir jānodrošina, ka tās darbības atbilst Vispārīgās datu aizsardzības regulas (VDAR) un citu personas datu aizsardzības regulējumu prasībām.

Minimālās kiberdrošības prasības!

MK Nr. 397 68. un 69. punkts nosaka, ka rezerves kopijām jāietver visi nepieciešamie dati, lai varētu pilnībā atjaunot informācijas sistēmas darbību uz to brīdi, kad tika izveidota rezerves kopija. Šajās kopijās ir jāietver šādi dati:

- **Informācijas sistēmā glabātie dati**: tostarp lietotāju dati, klientu dati, transakcijas informācija un citi dati, kas ir būtiski organizācijas darbībai;
- **Izpildāmais kods**: jebkuri koda faili, kas nepieciešami sistēmas darbības nodrošināšanai;
- **Atbalsta programmatūra un bibliotēkas**: tas ietver visas atbalsta programmatūras un bibliotēkas, tostarp atvērtā koda komponentes, ja tās tiek izmantotas;

- **Automatizētie darbību skripti**: skripti, kas tiek izmantoti, lai automatizētu noteiktas darbības sistēmā;
- **Tehniskajos resursos regulāri veicamās darbības**: visas ikdienas darbības, kas jāveic, lai uzturētu sistēmu (piemēram, datu dzēšana, jauninājumu instalēšana), ja tie ir nepieciešami sistēmas darbības turpināšanai un atjaunošanai;
- **Operētājsistēmas uzdevumu pārvaldnieka komandas un izpildāmās datnes**: ieraksti un faili, kas nosaka, kādi darbi datorā jāveic automātiski noteiktā laikā. Piemēram, tie var būt uzdevumi, kas iestatīti, lai katru nakti noteiktā laikā veiktu datu rezerves kopēšanu, kā arī atsevišķi faili, kuros aprakstīts, kā tieši šī kopēšana notiek. Pārvaldnieku komandas var tikt iestatītas, izmantojot, piemēram, Task Scheduler (Windows), cron vai systemd timers (Linux);
- **Tehniskā dokumentācija**: dokumentācija, kas nepieciešama sistēmas administrēšanai un atjaunošanai;
- **Informācijas sistēmas versijas un saistīto bibliotēku versiju pirmkods,** ja tiek izmantotas atvērtā koda bibliotēkas;
- **Tehnisko resursu konfigurācijas**: konfigurācijas faili un sistēmas iestatījumi, datu pārraides tīkla konfigurācija.

Visiem šiem datiem ir jāveido rezerves kopijas, lai nodrošinātu, ka informācijas sistēmu var pilnībā atjaunot un tā var funkcionēt tāpat kā pirms incidenta. Rezerves kopijas jāveido ne tikai lietotāju, klientu un citiem organizācijas darbībai nepieciešamajiem datiem, bet arī konfigurācijām, programmatūrai un tās komponentēm, tādējādi nodrošinot biznesa nepārtrauktību un atbilstību normatīvajām prasībām.

Šo prasību praktisku izpildi būtiski atvieglo infrastruktūras kā koda (*IaC - Infrastructure as code*) pieejas izmantošana. Infrastruktūra kā kods ir informācijas sistēmas pārvaldības pieeja, kurā serveru, datu glabātuvi, tīkla konfigurācijas, drošības iestatījumus un citus programmatūras tehniskos resursus apraksta un uztur ar programmatūras kodu. Šāda pieeja ļauj sistēmas vidi atjaunot automatizēti, ievērojot organizācijas noteiktos konfigurācijas un drošības uzstādījumus.

Papildus, MK Nr. 397 25. punkts nosaka, ka subjektam ir jānodrošina, ka rezerves kopijas tiek veidotas arī kiberdrošības pārvaldības dokumentācijai (kiberdrošības politikai, IKT resursu un informācijas sistēmu katalogam, kiberrisku pārvaldības un IKT darbības nepārtrauktības plānam un kiberincidentu žurnālam), kas tiek glabātas atsevišķi no to oriģināliem.

4.2. REZERVES KOPIJU VEIDOŠANAS BIEŽUMS UN RPO

Datu atjaunošanas mērķa punkts jeb RPO (*Recovery Point Objective*) ir būtisks parametrs, kas nosaka, cik tālu pagātnē organizācija var atjaunot sistēmas un datus incidenta gadījumā. Tas norāda, cik daudz datu organizācija var atļauties zaudēt, neskarot tās darbības nepārtrauktību un attiecīgi arī nosaka, cik bieži ir jāveido rezerves kopijas.

RPO atbild uz jautājumu “Cik daudz datu organizācija var atļauties zaudēt?” un mēra laiku no incidenta brīža līdz pēdējās rezerves kopijas izveides laikam. Piemēram, ja RPO ir 4 stundas, tas nozīmē, ka organizācijai jāveido rezerves kopijas vismaz ik pēc 4 stundām, lai nepieļautu datu zudumu par ilgāku laika posmu.

Izvēloties atjaunošanas mērķa punktu (RPO), organizācijai jāņem vērā vairāki faktori, tostarp:

- informācijas sistēmās apstrādāto datu veidi un to vērtība organizācijai;

- tehniskie un cilvēkresursi, kas ir pieejami rezerves kopiju veidošana, glabāšanai un pārvaldīšanai;
- prasības un gaidas no ieinteresētajām personām (piemēram, klientiem vai sadarbības partneriem), kas sagaida augstu datu vai pakalpojumu integritāti;
- sistēmā esošo datu mainīguma biežums;
- piemērojamie normatīvie akti;
- datu klasifikācija un riska novērtējums, ja dati tiktu zaudēti.

Piemērs: Organizācijām, kas apstrādā finanšu datus, ir ļoti ierobežota pieļaujamā datu zuduma apjoma pieļaujamība - šādām sistēmām RPO parasti ir ļoti mazs, piemēram, tikai dažas minūtes, lai izvairītos no būtiskiem finanšu zaudējumiem. Savukārt mazāk kritiskajiem datiem, piemēram, arhīviem vai vecākiem dokumentiem, var būt pieļaujams veidot rezerves kopijas retāk, atbilstoši plānoto izmaiņu biežumam.

RPO vērtība jānosaka, ņemot vērā organizācijas darbības nepārtrauktības plānu, veicot riska un ietekmes analīzi un izvērtējot gan biznesa, gan tehnoloģiskos aspektus, kas ietekmē datus un to pieejamību. Būtiski ir arī ņemt vērā, kādas sekas var rasties datu zaudēšanas gadījumā, un noteikt, kāds biežums būs optimāls organizācijas vajadzībām.

Minimālās kiberdrošības prasības!

MK Nr. 397 nosaka minimālās prasības rezerves kopiju veidošanas biežumam un uzglabāšanas laikam. Atbilstoši MK noteikumu Nr. 397 70. punktam, subjektam ir jānodrošina, ka rezerves kopiju veidošanas periodiskums un uzglabāšanas laiks ļauj atjaunot informācijas sistēmu vismaz tādā stāvoklī, kāds bija:

- **A klases informācijas sistēmai** - iepriekšējā dienā, pirms nedēļas (7-31 diena), pirms mēneša (30-365 dienas), iepriekšējā gadā (vecāku par 365 dienām);
- **B klases informācijas sistēmai** - pēdējās nedēļas laikā (1-7 dienas), pirms nedēļas (7-31 diena), pirms mēneša (30-365 dienas), iepriekšējā gadā (vecāku par 365 dienām);
- **C klases informācijas sistēmai** - pirms pēdējām nozīmīgām izmaiņām informācijas sistēmā (piemēram, pirms migrācijas uz citu tehnoloģisku platformu), bet ne senāk kā pirms sešiem mēnešiem.

Piemērs: Lai nodrošinātu atbilstību MK Nr. 397 70. punktā noteiktajām prasībām, **A klases** informācijas sistēmai kā minimums nepieciešams:

- veikt ikdienas inkrementālās vai diferenciālās rezerves kopijas, lai būtu iespējams atjaunot datus vai sistēmu iepriekšējās dienas stāvoklī. Ieteicams uzglabāt vismaz pēdējās 7 inkrementālās kopijas vai pēdējo diferenciālo kopiju;
- reizi nedēļā izveidot pilnu rezerves kopiju (kombinācijā ar ikdienas kopijām), lai nodrošinātu iespēju atjaunot datus vismaz tādā stāvoklī, kāds bija pirms nedēļas. Uzglabāt vismaz vienu pilnu kopiju, kas ir vecāka par 7 dienām, bet jaunāka par 31 dienu;
- saglabāt vismaz vienu pilnu kopiju, kas ir vecāka par 30 dienām, bet jaunāka par 365 dienām, lai nodrošinātu atjaunošanu vismaz tādā stāvoklī, kāds tas bija pirms mēneša;
- saglabāt vismaz vienu kopiju, kas ir vecāka par 365 dienām, lai nodrošinātu atjaunošanu vismaz tādā stāvoklī, kāds tas bija iepriekšējā gadā.

Viens no iespējamiem risinājumiem A klases informācijas sistēmu rezerves kopiju veidošanas organizēšanai, lai nodrošinātu atbilstību MK Nr. 397 noteiktajām minimālajām prasībām, sākot ar 2026. gada 1. janvāri, varētu būt šāds:

1. Dienas inkrementālās kopijas (iepriekšējā diena):

- Tiek veidotas katru dienu no pirmdienas līdz svētdienai (29.12.2025., 30.12.2025., 31.12.2025., 01.01.2026., 02.01.2026., 03.01.2026..).
- Tiek saglabātas vismaz pēdējo 6 dienu kopijas līdz brīdim, kad tiek izveidota nākamā nedēļas pilnā kopija. Nākamajā pirmdienā (05.01.2026.) pēc pilnas kopijas izveides 4.janvārī., iepriekšējās nedēļas inkrementālās kopijas (29.12.2025. līdz 03.01.2026.) var dzēst.

2. Nedēļas pilnās kopijas (7 - 31 diena):

- Pilnās rezerves kopijas tiek veidotas katru svētdienu (28.12.2025., 04.01.2026., 11.01.2026., 18.01.2026., u.t.t.), un uz to pamata veido nākamās nedēļas inkrementālās kopijas.
- Jānodrošina, ka vienmēr ir pieejama vismaz viena pilna kopija, kas ir vecāka par nedēļu (7 dienām), bet jaunāka par vienu mēnesi (31 dienu). Šī prasība izpildās, ja katru nedēļas pilno kopiju glabā vismaz 15 dienas, t.i., līdz pirmdienai pēc aiznākamās svētdienas.
- Piemēram, 04.01.2026. izveidotā kopija tiek glabāta līdz 19.01.2026., savukārt 11.01.2026. izveidotā – līdz 26.01.2026. utt. Šāda rotācijas pieeja nodrošina, ka vienmēr ir pieejama kopija, kas ir 7–14 dienas veca, tādējādi izpildot prasības par 7–31 dienu perioda kopiju.

3. Mēneša pilnā kopija (30 - 365 diena) un gada pilnā kopija (vecāka par 365 dienām):

- Jāglabā vismaz viena pilna kopija, kas ir vecāka par 30 dienām, bet jaunāka par vienu gadu (365 dienām), kā arī viena pilnā kopija, kas ir vecāka par vienu gadu.
- Šo prasību iespējams izpildīt, ja ik pēc pusgada vienai no nedēļas pilnajām kopijām tiek noteikts ilgāks glabāšanas termiņš - vismaz pusotrs gads (aptuveni 78 nedēļas).
- Piemēram, var paredzēt, ka katru gadu janvāra un jūlija pirmajā svētdienā veidotajai nedēļas pilnajai kopijai tiek noteikts glabāšanas ilgums nevis tikai 15 dienas, bet pusotrs gads (1,5 gadi) plus aptuveni nedēļa (līdz nākamajai vai aiznākamajai pirmdienai, kad tiek dzēstas rezerves kopijas).
- *Piemērs*: 04.01.2026. (2026. gada janvāra pirmā svētdiena) veidotajai nedēļas pilnajai kopijai nosaka glabāšanas termiņu līdz 12.07.2027. Šādā gadījumā attiecīgā kopija dažādos laika posmos kalpos kā:
  - 7–31 dienu perioda kopija,
  - 30–365 dienu perioda kopija,
  - kopija, kas vecāka par 365 dienām (gada kopija).
- Tāpat 05.07.2026. (2026. gada jūlija pirmā svētdiena) veidotajai nedēļas pilnajai kopijai tiek noteikts glabāšanas termiņš līdz 10.01.2028., un šī pieeja tiek turpināta, nodrošinot mēneša un gada kopiju rotāciju un atbilstību MK Nr. 397 minimālajām prasībām.

Ņemot vērā, ka MK Nr. 397 70. punkts nosaka tikai minimālās prasības rezerves kopiju veidošanas biežumam un glabāšanas laikam, balstoties uz riska novērtējumu un datu sensitivitāti, organizācijai var būt nepieciešams nodrošināt vairākas rezerves kopiju versijas vai biežāku to izveidi, nekā paredz minimālās prasības. Piemēram, A klases informācijas sistēmai būtu ieteicams:

- reizi nedēļā izveidot pilnu kopiju un 6 nākamajās dienās veidot inkrementālās kopijas. Šīs kopijas glabāt līdz aiznākamās pilnās kopijas izveidei.
- katras nedēļas pilnās kopijas glabāt 5 nedēļas.
- vienu pilno rezerves kopiju no katra mēneša uzglabāt 13 mēnešus. Tas nodrošina iespēju atgriezties uz jebkuru mēnesi pēdējā gada laikā un vienu pēdējo mēnesi no iepriekšējā gada.

Piemērs: B klases informācijas sistēmai kā minimums nepieciešams:

- veidot pilnu rezerves kopija reizi nedēļā, lai būtu iespēja atgriezt datus vai sistēmas stāvoklī, kāds tas bija vismaz pēdējās nedēļas laikā. Nepieciešams uzglabāt vismaz vienu kopiju, kas ir jaunāka par nedēļu (septiņām dienām).
- saglabāt vismaz vienu pilnu kopiju, kas ir vecāka par 7 dienām, bet jaunāka par 31 dienu, lai būtu iespēja atjaunot datus vai sistēmas stāvokli, kāds tas bija vismaz pirms nedēļas.
- saglabāt vismaz vienu kopiju, kas ir vecāka par 30 dienām, bet jaunāka par 365 dienām, lai būtu iespējams atgriezt datu vai sistēmas stāvokli vismaz tādā stāvoklī, kāds tas bija pirms mēneša.
- saglabāt vismaz vienu kopiju, kas ir vecāka par 365 dienām, lai nodrošinātu iespēju atgriezt datu vai sistēmas stāvokli vismaz tādā stāvoklī. kāds tas bija iepriekšējā gadā.

Piemērs: C klases informācijas sistēmai kā minimums nepieciešams:

- izveidot un saglabāt vismaz vienu pilnu kopiju pirms jebkurām nozīmīgām izmaiņām sistēmā (piem., pirms migrācijas uz jaunu platformu);
- jebkurā gadījumā, ne retāk kā reizi sešos mēnešos veidot pilnu rezerves kopiju, nodrošinot, ka glabājas vismaz viena kopija, kas ir jaunāka par 6 mēnešiem.

4.3. ATJAUNOŠANAS LAIKA MĒRĶIS (RTO)

Atjaunošanas laika mērķis (*RTO - Recovery Time Objective*) nosaka maksimāli pieļaujamo laika periodu, kurā kritiskās sistēmas un dati pēc incidenta var būt nepieejami, pirms to atjaunošana jābūt pabeigtai. RTO aptver visus pasākumus, piemēram, datu atjaunošanu no rezerves kopijām, sistēmu kļūdu novēršanu un funkcionalitātes pārbaudi, ko veic atbildīgās IT komandas, un tā vērtībai jābūt iekļautai biznesa ietekmes analīzē kā daļai no kopējā maksimum pieļaujamā dīkstāves laika (*MTD - Maximum Tolerable Downtime*).

Maksimāli pieļaujamais dīkstāves laiks ir kopējais laika logs, cik ilgi organizācija var izturēt pakalpojumu pārtraukumu, pirms rodas neatgriezeniski zaudējumi biznesa darbībai, reputācijai vai atbilstībai normatīvajiem aktiem. MTD ietver gan RTO, gan darba atjaunošanas laiku (*WRT - Work Recovery Time*) kas nepieciešams, lai pilnībā pārbaudītu, validētu un atjaunotu sistēmu darbību normālā režīmā.

Saikne starp RTO un MTD ir tieša: RTO vienmēr jābūt īsākam par MTD, lai pēc dīkstāves un atjaunošanas posmiem atliktu pietiekams laiks sistēmu pilnīgai pārbaudei un pārejas procesiem. Piemēram, ja MTD ir noteikts 6 stundas, RTO var tikt plānots uz 4 stundām, atstājot papildu 2 stundas testēšanai, validācijai un pārējiem atjaunošanas soļiem. Šāda strukturēta pieeja nodrošina, ka pat neplānotu incidentu gadījumā pakalpojumi atgriežas tieši laikā, neapdraudot biznesa nepārtrauktību un atbilstību riska izvērtējuma atziņām.

5. REZERVES KOPIJU DROŠĪBAS PRINCIPI

Efektīva rezerves kopiju pārvaldība neierobežojas tikai ar datu glabāšanu. Ir būtiski nodrošināt, ka kopiju veidošana un glabāšana tiek veikta droši, kopijas ir nebojātas un atjaunojamas nepieciešamības gadījumā. Šie trīs aspekti, konfidencialitāte, integritāte un pieejamība, ir cieši savstarpēji saistīti un ir pamats uzticamai rezerves kopiju sistēmai, kas spēj atbalstīt organizācijas darbības nepārtrauktību un aizsargāt tās pret iespējamiem datu zuduma vai kompromitēšanas riskiem.

5.1. KONFIDENCIALITĀTE

Rezerves kopiju aizsardzība pret nesankcionētu piekļuvi ir ļoti svarīga, jo tajās glabājas organizācijai vērtīga informācija tāpat kā to oriģinālajos failos. Ir jānodrošina, lai trešās personas nevarētu piekļūt datiem visā rezerves kopiju dzīves ciklā. Šim nolūkam jāievieš gan tehniskie, gan organizatoriskie drošības pasākumi.

Viens no būtiskākajiem drošības līdzekļiem ir kriptogrāfisko aizsardzības risinājumu izmantošana datu pārsūtīšanas (*data in transit*) un glabāšanas laikā (*data at rest*). Tas nodrošina, ka pat gadījumā, ja dati tiek pārtverti vai citādi neautorizēti iegūti, tie būs nelasāmi bez atbilstošas atslēgas. Ieteicamie šifrēšanas līdzekļi:

- pārsūtīšanai - izmantojot virtuālo privāto tīklu (*VPN*), vai tādi šifrēšanas protokoli kā SFTP un TLS;
- glabāšanai - failu vai diska līmeņa šifrēšana, izmantojot AES-256 vai līdzvērtīgu algoritmu;
- ļoti sensitīvu datu gadījumā, kā arī, ja paredzētais kopiju glabāšanas laiks ir ilglaicīgs - ieteicams apsvērt pēckvantu kriptogrāfijas līdzekļu izmantošanu.

Papildus tehniskajiem pasākumiem ir jānodrošina arī rezerves kopiju fiziskā drošība. Jānovērš iespēja fiziski piekļūt datiem nepiederošām personām un jāpasargā kopijas no dabas katastrofām, piemēram, plūdiem vai ugunsgrēkiem. Fiziskās drošības pasākumi var ietvert:

- apsargājamas un slēgtas telpas ar ierobežotu piekļuvi tikai pilnvarotām personām;
- signalizācijas un videonovērošanas sistēmas;
- speciālas ugunsdzēšanas sistēmas, kas nebojā elektroniskās ierīces (piemēram, ar inertajām gāzēm vai skābekļa reducēšanu);
- serveru statīvi un paliktņi, lai aizsargātu iekārtas no iespējamām ūdens noplūdēm.

Lai pārliecinātos, ka rezerves kopijas izmanto tikai autorizēti lietotāji, ieteicams reģistrēt visas darbības ar rezerves kopijām - piekļuvi, lasīšanu, modificēšanu, dzēšanu un pārvietošanu. Šie žurnālfaili palīdzēs incidentu izmeklēšanā un neautorizētu darbību identificēšanā. Tāpat žurnālfailiem būtu jābūt dublētiem un/vai glabātiem atsevišķā, aizsargātā sistēmā.

Izmantojot trešo pušu pakalpojumus, piemēram, mākoņglabātuvi vai attālinātus datu centrus, svarīgi līgumiski nostiprināt datu aizsardzību un tiesības piekļūt rezerves kopijām.

Minimālās kiberdrošības prasības!

MK Nr. 397 72.1. punkts paredz, ka A un B klases informācijas sistēmu rezerves kopijām ir jānodrošina, ka tām gan fiziski, gan elektroniskajā vidē drīkst piekļūt tikai šādas personas:

- subjekta pilnvarotās personas;
- par rezerves kopiju atbildīgā persona;

- kiberdrošības pārvaldnieks.

Šī piekļuves kontrole ir jārealizē gan fiziski (piemēram, aizsargātas telpas vai drošus datu nesējus), gan loģiski (piemēram, izmantojot drošu autentifikāciju, autorizācijas mehānismus un piekļuves žurnālu uzturēšanu).

5.2. INTEGRITĀTE (INTEGRITĀTES PĀRBAUDE)

Rezerves kopiju integritāte nozīmē, ka dati rezerves kopijās nav mainījušies kopš to izveides brīža. Šis princips ir īpaši svarīgs, jo bojātas vai izmainītas rezerves kopijas incidenta gadījumā var padarīt sistēmu un datu atjaunošanu neiespējamu vai nopietni apdraudēt datu uzticamību.

Rezerves kopiju integritātes nodrošināšanai īpaša uzmanība ir jāpievērš rezerves kopiju vides loģiskajai izolācijai. Rezerves kopijām nevajadzētu būt pastāvīgi savienotām ar primāro sistēmu - ieteicams izmantot no primārās informācijas sistēmas tehniski vai loģiski atdalītas, izolētas vai tikai lasāmas (*read-only*) kopijas. Tas būtiski samazina risku, ka kiberuzbrukuma gadījumā uzbrucējs varētu vienlaikus kompromitēt gan primāro sistēmu, gan tās rezerves kopijas.

Tāpat ir svarīgi nodrošināt iespēju pārliecināties par kopiju nemainību. Rezerves kopiju integritāti iespējams pārbaudīt, izmantojot dažādus paņēmienus, piemēram:

- **kriptogrāfiskos jaucējalgoritmus** (*hash function*), piemēram, SHA-256, kuri ļauj salīdzināt izveidotās kopijas kontrolsummu ar oriģinālo datu kontrolsummu. Ir svarīgi nodrošināt, ka kontrolsummas vērtība tiek droši uzglabāta un aizsargāta pret izmaiņām;
- **speciālus rezerves kopiju pārvaldības rīkus**, kas nodrošina automātisku datu integritātes pārbaudi un uzraudzību.

Tas, cik bieži ir jāveic integritātes pārbaudes, ir atkarīgs no sistēmas svarīguma, no rezerves kopiju veidošanas biežuma un riska novērtējuma. Jebkurā gadījumā, integritātes pārbaudes ir jāveic plānoti, un to rezultāti ir jāfiksē.

Minimālās kiberdrošības prasības!

MK Nr. 397 nosaka konkrētas prasības attiecībā uz rezerves kopiju integritātes pārbaudēm:

- 71.3. punkts paredz, ka A klases informācijas sistēmai pēc katras rezerves kopijas izveides ir jāizveido rezerves kopijas satura kontrolsumma. Tas nozīmē, ka katru reizi, veidojot kopiju, ir jāizveido kontrolsumma, izmantojot kriptogrāfisko jaucējalgoritmu, un jāsalīdzina tā ar kontrolsummu oriģinālajam datu kopumam, kam tika veikta rezerves kopija. Kontrolsumma jāuzglabā, lai nodrošinātu iespēju veikt nākotnes integritātes pārbaudes.
- 72.3. punkts paredz, ka A un B klases informācijas sistēmai pēc rezerves kopijas pārvietošanas citā datu nesējā tiek pārbaudīta rezerves kopijas integritāte (piemēram, pārbaudot tās satura kontrolsummu). Tas nozīmē, ka, pārvietojot rezerves kopijas uz citu datu nesēju, ir jāsalīdzina jaunajā nesējā esošās kopijas kontrolsumma ar kontrolsummu, kas tika izveidota pirms pārvietošanas.

5.3. PIEEJAMĪBA (ATJAUNOŠANAS PĀRBAUDES)

Rezerves kopijas pilda savu mērķi tikai tad, ja tās ir praktiski izmantojamas datu vai visu sistēmu atjaunošanai. Tādējādi viens no būtiskākajiem aspektiem ir to pieejamība un iespēja tās atjaunot. Proti, ir svarīgi pārliecināties, vai, notiekot incidentam, rezerves kopijas tiešām var tikt izmantotas, lai atjaunotu sistēmu darbību atbilstoši noteiktajam atjaunošanas laika mērķim (RTO) un pieļaujamajam datu zuduma apjoma mērķim (RPO).

Rezerves kopiju pārbaudes būtu jāveic atbilstoši noteiktajam riska līmenim. Jau iepriekš jānosaka regularitāte un kārtība, kādā tiek pārbaudīta iespēja atjaunot datus un sistēmas darbību, izmantojot rezerves kopijas. Praktiski ieteicams izveidot testa vidi, kurā ir iespējams pārbaudīt rezerves kopiju izmantošanu sistēmu pilnai vai daļējai atjaunošanai bez ietekmes uz produkcijas vidi. Svarīgi ir, ka testi tiek veikti ne tikai failu vai datu atjaunošanai, bet arī uz visu informācijas sistēmu darbības atjaunošanu, izmantojot rezerves kopijas.

Vienlaikus ir jāpārliecinās, ka organizācijai būs pieejami nepieciešamie resursi rezerves kopiju atjaunošanai, īpaši gadījumos, kad kopijas tiek glabātas ilgtermiņā. Piemēram, ja rezerves kopijas tiek saglabātas lentēs vai citos specifiskos datu nesējos, ir jānodrošina, ka atbilstošā aparatūra to nolasīšanai būs pieejama arī nākotnē. Tāpat, ja rezerves kopiju izveide un atjaunošana ir atkarīga no konkrētas programmatūras, jāparedz, ka nepieciešamības gadījumā būs pieejama attiecīgā programmatūra un derīga tās licence. Pretējā gadījumā pat tehniski neskarta kopija var izrādīties neizmantojama.

Tāpat kā citām darbībām, rezerves kopiju sistēmas pārbaudes rezultāti ir jādokumentē, un bez kavēšanās jānodrošina atklāto trūkumu novēršana.

Minimālās kiberdrošības prasības!

MK Nr. 397 paredz pienākumus, kas saistīti ar rezerves kopiju pieejamības un lietojamības pārbaudēm:

- 73. punkts nosaka, ka subjektam ir jāiekļauj rezerves kopiju pārvaldības dokumentācijā kārtība, kādā tiek pārbaudīta informācijas resursu un informācijas sistēmu darbības atjaunošanas spēja no rezerves kopijām;
- 74.1. punkts uzliek par pienākumu kiberdrošības pārvaldniekam veikt ikdienas uzraudzību par rezerves kopiju sagatavošanu;
- 74.2. punkts nosaka pienākumu kiberdrošības pārvaldniekam veikt izlases pārbaudes, lai pārliecinātos par rezerves kopiju praktisko lietojamību:
    - A klases informācijas sistēmām - ne retāk kā reizi sešos mēnešos;
    - B klases informācijas sistēmām - ne retāk kā reizi gadā;
    - Jebkuras klases informācijas sistēmām - pēc būtiskām izmaiņām informācijas sistēmā vai rezerves kopiju veidošanas procedūrās.