JURISTA PADOMS

Kā stiprināsim noturību pret KIBERDROŠĪBAS RISKIEM

Informācijas un komunikācijas tehnoloģijas (IKT) ir kļuvušas par neatņemamu sastāvdaļu ikvienā uzņēmumā, taču mūsdienu ģeopolitiskajos apstākļos ievērojami ir audzis kiberuzbrukumu skaits un mērogs. Tādēļ būtiski ir pievērst uzmanību pieaugošajiem kiberdrošības riskiem un stiprināt sabiedrības un uzņēmumu noturību, nepieļaujot kiberapdraudējumus un kiberincidentus.

Ilustrācija: © Yevheniiya – stock.adobe.com

AGNESE GERHARDE

ZAB COBALT
zvērināta advokāta palīdze

Saeimā 2024. gada 20. jūnijā tika pieņemts jauns Aizsardzības ministrijas izstrādātais Nacionālās kiberdrošības likums, kas stājās spēkā 1. septembrī. Likums ne tikai uzlabos nacionālās kiberdrošības prasības, bet arī ievieš 2022. gadā pārskatīto Eiropas Savienības Tīklu un informācijas sistēmu drošības direktīvu[1] (Direktīva 2022/2555) jeb „NIS2", ar ko paredzēts panākt vienādi augstu kiberdrošības līmeni visā Eiropas Savienībā (ES). Ar NIS2 direktīvas ieviešanu Latvijā un jauno likumu tiek izveidota jauna institūcija – Nacionālās kiberdrošības centrs, un būtiski paplašināts to nozaru skaits, kurām būs jāievieš striktāki kiberdrošības nosacījumi. Ņemot vērā apjomīgās izmaiņas, jaunais likums aizstāj Informācijas tehnoloģiju drošības likumu un uz Nacionālās kiberdrošības likuma pamata tiks izdoti vairāki Ministru kabineta noteikumi, kas aizstās patlaban spēkā esošos.

ES kiberdrošības prasību reforma

Ņemot vērā straujo tehnoloģiju attīstību un nevienmērīgo kiberdrošības līmeni un pārvaldību starp ES dalībvalstīm, Eiropas Komisija jau 2020. gada nogalē nāca klajā ar priekšlikumu reformēt sākotnējo ES Tīklu un informācijas sistēmu drošības direktīvu[2] (Direktīva 2016/1148) jeb „NIS1", kas stājās spēkā 2018. gadā. 2022. gadā tika pieņemta jaunā NIS2 direktīva, kas aizstās sākotnējo tīklu un informācijas sistēmu drošības režīmu, novēršot konstatētos NIS1 direktīvas trūkumus un ieviešot stingrākus uzraudzības un administratīvo sankciju pasākumus. **Dalībvalstīm ir pienākums ieviest NIS2 direktīvu līdz 2024. gada 17. oktobrim.** Jāatzīmē, ka NIS direktīvas reforma ir tikai viens no plašā ES kiberdrošības regulējuma, un tas savstarpēji mijiedarbojas ar citiem ES tiesību instrumentiem, tai skaitā ar DORA regulu[3] (Regula 2022/2554), kas ir finanšu nozares specifisks kiberdrošības regulējums.

Paplašināts subjektu loks

Nacionālās kiberdrošības likuma subjekti ir iedalīti trīs grupās:

(i) **BŪTISKO PAKALPOJUMU SNIEDZĒJI** (likuma 20. pants),
(ii) **SVARĪGO PAKALPOJUMU SNIEDZĒJI** (21. pants),
(iii) **KRITISKĀ IKT INFRASTRUKTŪRA** (24. pants).

Jāatzīmē, ka nevar izslēgt iespēju, ka kāds no būtisko vai svarīgo pakalpojumu sniedzējiem ir vienlaikus arī kritiskās IKT infrastruktūras īpašnieks vai pārvaldnieks.

Svarīgo un būtisko pakalpojumu sniedzēji ietvers valsts un pašvaldības iestādes, kā arī vidējos un lielos uzņēmumus, kuri darbojas kādā no likumā uzskaitītajām nozarēm, piemēram, IKT, digitālie pakalpojumi, elektroniskie sakari, sabiedriskie mediji, enerģētika, transports, ūdens un pārtikas apgāde, medicīna un farmācija, ražošana, finanšu pakalpojumi, pasta pārvadājumi, izglītība, zinātne, apsardze. Vienlaikus par būtisko pakalpojumu sniedzējiem tiks uzskatītas arī organizācijas, **kuru darbības traucējumi var būtiski ietekmēt sabiedrības drošību, valsts aizsardzību, sabiedrības veselību,** vai var radīt būtisku sistēmisku risku, jo īpaši nozarēs, kurās šādam traucējumam var būt pārrobežu ietekme. Līdzīgi kā līdz šim, kritiskās IKT infrastruktūras sarakstā ietilpstošās iestādes un uzņēmumus apstiprinās Ministru kabinets.

Svarīgi ņemt vērā, ka jaunais likums aizstāj iepriekš lietotās Informācijas tehnoloģiju drošības likumā noteiktās subjektu kategorijas „pamatpakalpojumu sniedzēji" un „digitālo pakalpojumu sniedzēji".

Kritēriji vidējiem un lieliem uzņēmumiem

Uzņēmumu iekļaušanas kritēriji ir gan joma, kurā tie darbojas, gan uzņēmuma lielums un finanšu apgrozījums. Likuma 20. un 21. pantā noteikto jomu uzņēmumi tiek iekļauti likuma tvērumā, ja tie ir vidēji vai lieli saimnieciskās darbības veicēji.

Likums noteic, ka **vidējs saimnieciskās darbības veicējs** ir juridiskā vai fiziskā persona vai šādu personu apvienība, kas veic saimniecisko darbību Latvijas Republikā un atbilst **visām** šādām pazīmēm:

1) saimnieciskās darbības veicējs nodarbina līdz 249 nodarbinātajiem;
2) saimnieciskās darbības veicēja pēdējā finanšu gada kopējais neto apgrozījums ir vismaz 10 miljoni eiro, bet nepārsniedz 50 miljonus eiro vai gada bilances kopsumma ir vismaz 10 miljoni eiro, bet nepārsniedz 43 miljonus eiro.

Savukārt **liels saimnieciskās darbības veicējs** ir juridiskā vai fiziskā persona vai šādu personu apvienība, kas veic saimniecisko darbību Latvijas Republikā un atbilst **vismaz vienai** no šādām pazīmēm:

1) saimnieciskās darbības veicējs nodarbina vismaz 250 nodarbinātos;

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.

2 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

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) Nr. 909/2014 un (ES) 2016/1011.

Foto: Aivars Siliņš

2) saimnieciskās darbības veicēja pēdējā finanšu gada kopējais neto apgrozījums pārsniedz 50 miljonus eiro un gada bilances kopsumma pārsniedz 43 miljonus eiro.

Būtiskākie likuma subjektu pienākumi

Uzņēmumiem un iestādēm, uz kuriem attiecas jaunā likuma prasības, ceļā uz atbilstību ir vairāki soļi ar konkrētiem termiņiem. Vienlaikus jebkurš ir aicināts ieviest ikdienā šīs prasības, savukārt subjektu gadījumā negaidīt piemērošanas termiņu, bet rīkoties jau tagad.

1. Subjektu atbilstības noteikšana un reģistrācija

Uzņēmumiem un iestādēm pašiem būs jāizvērtē sava atbilstība likumam. Atbilstības gadījumā par būtisko vai svarīgo pakalpojumu sniedzēja statusu būs jāpaziņo elektroniski Nacionālajam kiberdrošības centram līdz **2025. gada 1. aprīlim**.

2. Kiberdrošības pārvaldnieka iecelšana

Katram subjektam būs pienākums iecelt kiberdrošības pārvaldnieku un par to paziņot kompetentām iestādēm līdz **2025. gada 1. oktobrim**. Šāda pārvaldnieka iecelšana veicinās efektīvu IKT infrastruktūras pārvaldību un drošību. Kiberdrošības pārvaldnieka prasības būs noteiktas gaidāmajos Ministru kabineta noteikumos par minimālajām kiberdrošības prasībām. Kiberdrošības pārvaldniekam būs jāatbilst likumā un noteikumos uzskaitītajām minimālām kvalifikācijas un drošības prasībām.

Kiberdrošības pārvaldniekam nav jābūt obligāti subjekta darbiniekam, tas varēs būt arī ārpakalpojuma sniedzējs, ja atbilst visām prasībām. Jāņem vērā, ka kiberdrošības pārvaldnieks nevarēs būs IT departamenta darbinieks.

3. Pašvērtējuma ziņojuma iesniegšana

Līdz **2025. gada 1. oktobrim** subjektiem būs jāiesniedz pašvērtējuma ziņojums. Šajā ziņojumā būs jānorāda, vai subjekts atbilst likumā noteiktajām prasībām, un jāpaskaidro neatbilstība, ja tāda tiek konstatēta. Subjektiem būs pieejama pašvērtējuma ziņojuma veidlapa, kas būs iekļauta kopā ar citām ziņojuma veidlapām jaunajos Ministru kabineta noteikumos par minimālajām kiberdrošības prasībām. Šāds ziņojums būs jāiesniedz reizi trīs gados, ja subjekti nav A drošības klases subjekti, kam savukārt ziņojums jāiesniedz reizi gadā. Svarīgi minēt, ka neatbilstības gadījumā subjektiem var tikt piemērots pienākums veikt ārējo auditu, kura izmaksas būs jāsniedz pašam subjektam.

4. Minimālās drošības prasību ievērošana un kiberrisku pārvaldība

Subjektiem būs pienākums veikt piemērotus un samērīgus tehniskos un organizatoriskos pasākumus, lai pārvaldītu kiberriskus un novērstu vai līdz minimumam samazinātu kiberincidentu ietekmi. Gaidāmie Ministru kabineta noteikumi noteiks prasības attiecīgi subjektu veidam un to risku kategorijai. Šie jaunie noteikumi aizstās Ministru kabineta 2015. gada 28. jūlija noteikumus Nr. 442 „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām", kas zaudēs spēku š.g. 18. oktobrī. Ir sagaidāms, ka minimālās kiberdrošības prasības ietvers pamatprasības visiem subjektiem un papildu prasības attiecīgi būtisko pakalpojumu sniedzējiem un kritiskajai IKT infrastruktūrai.

Saskaņā ar pieejamo noteikumu projektu subjektu pienākumi ietvers gan dažādas aktivitātes, gan arī obligātās dokumentācijas prasības. **Subjektiem būs nepieciešams organizēt kiberdrošības pārvaldības procesus,** ievērot kiberhigiēnu un veikt regulāras nodarbināto apmācības, izvērtēt konfidencialitātes, integritātes un traucējumu riskus, veidot rezerves kopijas un veikt auditācijas pierakstus.

Kiberdrošības pārvaldības dokumentācijai būs jāietver:

- kiberdrošības politiku;
- IKT resursu un informācijas sistēmu katalogu;
- kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu;
- kiberincidentu žurnālu.

Šos dokumentus varēs veidot kā vienotu dokumentu vai vairāku tematiski saistītu dokumentu kopu. Turklāt dokumentācija būs jāuzglabā drošā elektroniskā veidā, nošķirot kopijas no dokumentu oriģināliem, lai kiberincidenta vai bojājumu gadījumā, kas skar dokumentu oriģinālus, būtu pieeja kopijām.

ĀRPAKALPOJUMA LĪGUMA SLĒGŠANAI par IKT pakalpojumu un tehnisko resursu iegādi noteiktiem subjektiem būs jāievēro papildu prasības atkarībā no pakalpojuma un informācijas sistēmas kategorijas. Tādēļ ļoti būtiski jebkuram subjektam būs pārskatīt ārpakalpojumu veidu un iepazīties ar gaidāmo prasību ietekmi uz esošajiem un plānotajiem līgumiem par ārpakalpojumu.

Ārpakalpojuma līguma slēgšanai par IKT pakalpojumu un tehnisko resursu iegādi noteiktiem subjektiem būs jāievēro papildu prasības atkarībā no pakalpojuma un informācijas sistēmas kategorijas.

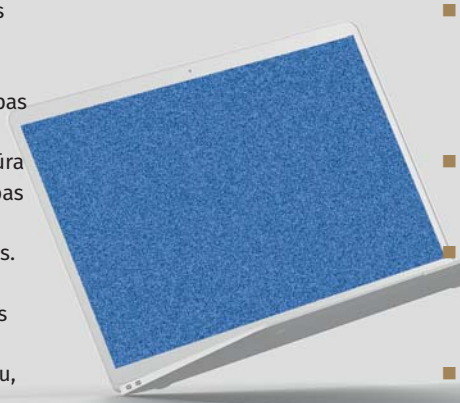
5. Pienākums ziņot par kiberdrošības incidentiem

Kiberdrošības incidentu gadījumā būs noteikta kārtībā, kādā ir jāziņo kompetentajām iestādēm. Konstatējot kiberincidentu, subjektam nekavējoties būs jāveic visas kiberincidenta novēršanai nepieciešamās darbības, kā arī nekavējoties par kiberincidentu jāinformē kompetento kiberincidentu novēršanas institūciju un jāizpilda tās sniegtos

UZRAUDZĪBAS IESTĀDES

Nacionālās kiberdrošības likumā noteikto subjektu uzraudzību un korektīvo funkciju īstenošanu veic Nacionālais kiberdrošības centrs un Satversmes aizsardzības birojs. Nacionālā kiberdrošības centra funkcijas kopš 1. septembra īsteno Aizsardzības ministrija sadarbībā ar Latvijas Universitātes Matemātikas un informātikas institūta struktūrvienību – **kiberincidentu novēršanas institūciju *CERT.LV*.** Centra ģenerāldirektors ir Aizsardzības ministrijas valsts sekretāra vietnieks – politikas direktors.

CERT.LV atbildībā ir reaģēšana uz kiberdrošības incidentiem, kibertelpas situācijas monitorings un draudu analīze, sensoru tīkla, DNS ugunsmūra un drošības operāciju centru darbības nodrošināšana, kā arī sabiedrības izglītošana kiberdrošības jautājumos. Nacionālais kiberdrošības centrs darbojas kā vienotais kontaktpunkts kiberdrošības jautājumos, īsteno nacionālo kiberdrošības pārraudzību, veido nacionālās kiberdrošības iniciatīvas, kā arī veido un īsteno starptautisko sadarbību kiberdrošības jomā.



Nacionālajam kiberdrošības centram ir **tiesības**:

- pieprasīt un saņemt informāciju par būtisko un svarīgo pakalpojumu sniedzējiem īpašumā un valdījumā esošajām IKT, to īstenotajiem un plānotajiem kiberdrošības un kiberrisku pārvaldības pasākumiem, kā arī par kiberincidentiem, kiberapdraudējumiem un ievainojamībām;
- pieņemt lēmumu un izdot administratīvo aktu, lai nodrošinātu Nacionālās kiberdrošības likumā noteikto pienākumu izpildi vai novērstu nacionālās drošības apdraudējumu vai kiberapdraudējumu;
- pieprasīt un saņemt no valsts un pašvaldību institūcijām to rīcībā esošo informāciju par būtisko un svarīgo pakalpojumu sniedzējiem;
- sniegt norādījumus, lai nodrošinātu Nacionālās kiberdrošības likumā būtisko un svarīgo pakalpojumu sniedzējiem noteikto pienākumu izpildi;
- piemērot soda naudu un veikt tiesiskā pienākuma piespiedu izpildi;
- pieprasīt un saņemt no datu centru operatoriem informāciju par tiem noteikto pienākumu izpildi.

norādījumus par rīcību kiberincidenta gadījumā.

Nozīmīga kiberincidenta gadījumā būs jāiesniedz nekavējoties, bet ne vēlāk kā 24 stundu laikā, agrīnais brīdinājums, savukārt 72 stundu laikā (uzticamības pakalpojumu sniedzējam – 24 stundu laikā) jāiesniedz sākotnējais ziņojumus par nozīmīgu kiberincidentu.

Tomēr ir aicinājums ziņot par katru konstatēto incidentu vai par gandrīz notikušu kiberincidentu vai kiberapdraudējumu, jo kompetentās institūcijas var palīdzēt tos novērst un iesaistīt operatīvās iestādes pēc nepieciešamības. Brīvprātīga ziņošana par gandrīz notikušu kiberincidentu vai kiberapdraudējumu neuzliks personai papildu pienākumus.

Neatbilstības gadījumā – ievērojami naudas sodi

Līdz ar NIS2 direktīvas ieviešanu, būtisks jauninājums ir sankcijas par kiberdrošības prasību neievērošanu. **Piemērojamās sankcijas būs atkarīgas no subjekta veida.** Privāto tiesību juridiskajām personām varēs piemērot soda naudu un piespiedu izpildes noteikumus, ja tiek konstatētas būtiskas neatbilstības. Tādējādi, līdzīgi kā par Vispārīgās datu aizsardzības regulas neievērošanu, arī par kiberdrošības prasību neievērošanu varēs piemērot ievērojamus naudas sodus.

Ministru kabinets noteiks kārtību, kādā nosakāma finanšu gada neto apgrozījums, no kura aprēķina soda naudu, un soda naudas apmēra noteikšanas kritērijus. Kompetentās iestādes būs tiesīgas piemērot sekojošus sodus:

- būtisko pakalpojumu sniedzējiem **līdz 10 miljoniem** eiro, bet, ja tā pēdējā finanšu gada kopējā neto apgrozījuma summa pārsniedz 500 miljonus eiro, **– līdz 2% no pēdējā finanšu gada kopējā neto apgrozījuma**.
- Svarīgo pakalpojumu sniedzējiem **līdz 7 miljoniem eiro**, bet ja tā pēdējā finanšu gada kopējā neto apgrozījumu summa pārsniedz 500 miljonus eiro, **– līdz 1,4% no pēdējā finanšu gada kopējā neto apgrozījuma**.
- IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam **līdz 10 miljoniem eiro**, bet ja tā pēdējā finanšu gada kopējā neto apgrozījuma summa pārsniedz 500 miljonu eiro, – **līdz 2% no pēdējā finanšu gada kopējā neto apgrozījuma**.

Kiberdrošība – jebkura uzņēmuma prioritāte

Ņemot vērā, ka pēdējo gadu laikā ir strauji pieaudzis kiberuzbrukumu skaits un paplašinājusies kiberrisku ietekme, kiberdrošībai būtu jābūt jebkura uzņēmuma prioritātei. Lai gan Nacionālās kiberdrošības likuma prasības būs piemērojamas pakāpeniski 2025. gadā un tās attieksies uz noteiktiem uzņēmumiem un iestādēm, ikviens tomēr ir aicināts laikus izvērtēt un ieviest kiberdrošības pārvaldību atbilstoši uzņēmuma darbības specifikai. BJP