KIBERDROŠĪBAS CEĻVEDIS

Nacionālais kiberdrošības centrs

SĀKOTNĒJIE SOĻI PIRMS KIBERDROŠĪBAS PĀRVALDNIEKA IECELŠANAS

Katrai organizācijai, kas darbojas vai sniedz pakalpojumus Latvijā, ir jāizvērtē, vai uz to attiecas Nacionālā kiberdrošības likuma prasības. Šīs prasības attiecas uz svarīgo un būtisko pakalpojumu sniedzējiem, kā arī informācijas un komunikācijas tehnoloģiju (IKT) kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem.

1. SOLIS

KIBERDROŠĪBAS PĀRVALDNIEKA IECELŠANA

Katrai organizācijai, kura ir Nacionālās kiberdrošības likuma subjekts, jānosaka atbildīgā persona par kiberdrošību jeb kiberdrošības pārvaldnieks. Ministru kabineta noteikumos par minimālajām kiberdrošības prasībām noteiktas kiberdrošības pārvaldniekiem izvirzāmās kvalifikācijas un drošības prasības. Par kiberdrošības pārvaldnieka noteikšanu jāpaziņo kompetentajai uzraudzības iestādei (Nacionālajam kiberdrošības centram vai IKT kritiskās infrastruktūras īpašniekiem – Satversmes aizsardzības birojam), iesniedzot aizpildītu paziņojuma veidlapu. Paziņojumu var iesniegt, nosūtot to uz uzraudzības iestādes E-adresi.

2. SOLIS

APZINI PROCESUS UN INFRASTRUKTŪRU

Katram Nacionālās kiberdrošības likuma subjektam ir jāapzina savi procesi un sniegtie pakalpojumi, kurus ietekmē informācijas un komunikācijas tehnoloģijas (IKT), kā arī IKT infrastruktūra un informācijas sistēmas. Tas ir nepieciešams, lai identificētu un mazinātu potenciālos kiberdrošības riskus, plānojot un īstenojot nepieciešamos drošības pasākumus.

3. SOLIS

IZVEIDO KATALOGU

Lai uzturētu aktuālo IKT infrastruktūras un informācijas sistēmu uzskaitījumu, subjektam jāizveido IKT resursu un informācijas sistēmu katalogs. To var veidot, izmantojot kādu no pieejamajiem tehnoloģiskajiem risinājumiem, vai arī manuāli, ievadot un regulāri aktualizējot datus par attiecīgajiem resursiem un informācijas sistēmām. Ministru kabineta noteikumos par minimālajām kiberdrošības prasībām ir noteikts minimālais katalogā iekļaujamo ziņu apjoms.

4. SOLIS

IDENTIFICĒ UN NOVĒRTĒ RISKUS

Subjektam jāizvērtē kiberdrošības riski un jānovērtē to potenciālā ietekme uz informācijas resursu konfidencialitāti, integritāti un pieejamību. Balstoties uz šo izvērtējumu, subjektam katrai tā īpašumā vai valdījumā esošajai informācijas sistēmai jāpiešķir kategorija – A (paaugstinātās drošības), B (pamata drošības) vai C (minimālās drošības) – atbilstoši Ministru kabineta noteikumos par minimālajām kiberdrošības prasībām ietvertajai metodikai.

5. SOLIS

IZSTRĀDĀ POLITIKU UN PLĀNU

Katram subjektam jābūt diviem nozīmīgākajiem dokumentu blokiem – kiberdrošības politikai, kas nosaka organizācijas kiberdrošības pārvaldības mērķus, principus un vispārīgas pamatnostādnes, kā arī kiberrisku pārvaldības un IKT darbības nepārtrauktības plānam, kas ietver detalizētu risku analīzi un pasākumu plānu to mazināšanai, kā arī rīcības plānu krīzes vai nozīmīga kiberincidenta gadījumā. Prasības šo dokumentu saturam ir noteiktas Ministru kabineta noteikumos par minimālajām kiberdrošības prasībām.

6. SOLIS

APMĀCI DARBINIEKUS

Viens no nozīmīgākajiem soļiem, lai stiprinātu katras organizācijas noturību pret kiberdraudiem, ir personāla apmācības. Darbiniekiem ir jāzina par aktuālajiem kiberriskiem un jāprot droši strādāt digitālajā vidē. Subjektu uzdevums ir organizēt regulāras kiberhigiēnas apmācības visiem nodarbinātajiem, kuri strādā ar IKT, kā arī kiberdrošības apmācības par IKT atbildīgajam personālam.

7. SOLIS

ZIŅO PAR INCIDENTIEM

Nacionālās kiberdrošības likums paredz noteiktu kārtību, kādā subjektiem jāziņo kompetentajai kiberincidentu novēršanas institūcijai – CERT.LV vai MilCERT – par konstatētajiem kiberdrošības incidentiem. Par nozīmīgiem kiberincidentiem jāziņo Nacionālās kiberdrošības likumā noteiktajā termiņā, iesniedzot noteikta parauga veidlapas, kas ir apstiprinātas ar Ministru kabineta noteikumiem par minimālajām kiberdrošības prasībām.

8. SOLIS

VEIC PAŠVĒRTĒJUMU

Lai novērtētu, vai subjekts ir izpildījis Nacionālās kiberdrošības likuma prasības, katram subjektam ir jāaizpilda un līdz 1. oktobrim jāiesniedz kompetentajai uzraudzības iestādei pašvērtējuma ziņojums. Tajā subjektam jāatzīmē prasības, kurām tas atbilst, un jāpaskaidro, kā tiek nodrošināta šī atbilstība. Pašvērtējuma ziņojums IKT kritiskās infrastruktūras un A kategorijas informācijas sistēmu īpašniekiem un tiesiskajiem valdītājiem jāiesniedz reizi gadā, bet pārējiem subjektiem – reizi 3 gados. Pašvērtējuma ziņojuma veidlapa ir apstiprināta ar Ministru kabineta noteikumiem par minimālajām kiberdrošības prasībām.

Aizsardzības ministrija
NCC-LV LATVIJAS KIBERDROŠĪBAS KOORDINĀCIJAS CENTRS
ECCC EIROPAS KIBERDROŠĪBAS KOMPETENČU CENTRS
Līdzfinansē Eiropas Savienība