AIZSARDZĪBAS
MINISTRIJA

Kā publiskā un privātā sektora organizācijām, uz kurām attiecas Nacionālās kiberdrošības likuma prasības, rīkoties incidentu gadījumā?

Nozīmīga kiberincidenta gadījumā:

1. **24 stundu** laikā elektroniski jāiesniedz kiberincidentu novēršanas institūcijai CERT.LV agrīnais brīdinājums par nozīmīgo kiberincidentu.

2. **72 stundu** laikā (uzticamības pakalpojumu sniedzējam – 24 stundu laikā) elektroniski jāiesniedz CERT.LV sākotnējais ziņojums par nozīmīgo kiberincidentu.

3. Pēc saskaņošanas ar CERT.LV (informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs – arī ar kompetento valsts drošības iestādi) nekavējoties jāinformē pakalpojumu saņēmēji par kiberdrošības pasākumiem vai līdzekļiem, ko izmantot, incidenta mazināšanai un apdraudējuma novēršanai, ja vien šādas informācijas izpaušana nerada jauna nozīmīga kiberincidenta risku, vai nav pretrunā ar nacionālās drošības interesēm.

4. Mēneša laikā pēc sākotnējā ziņojuma iesniegšanas, jāiesniedz CERT.LV galaziņojums par nozīmīgā kiberincidenta atrisināšanu.

5. Ja nozīmīgo kiberincidentu nav iespējams atrisināt mēneša laikā, jāiesniedz CERT.LV progresa ziņojums par nozīmīgā kiberincidenta risināšanu, galaziņojumu iesniedzot pēc kiberincidenta atrisināšanas.

Personas, uz kurām neattiecas augstākminētie pienākumi, kiberincidenta gadījumā veic visas tā novēršanai nepieciešamās darbības un var brīvprātīgi ziņot CERT.LV par konstatēto kiberincidentu. CERT.LV vienojas ar personu par atbalsta sniegšanu kiberincidenta risināšanā. Brīvprātīga ziņošana par kiberincidentu neuzliek minētajai personai papildu pienākumus.