AIZSARDZĪBAS
MINISTRIJA

PADOMI KIBERDROŠĪBAS VEICINĀŠANAI

(iestāžu vadītājiem)

1. SKAIDRI NOSAKIET, KA KIBERDROŠĪBA IR PRIORITĀTE

Kiberdrošība sākas ar savas informācijas un komunikāciju tehnoloģiju saimniecības apzināšanu. Prioritizējiet esošā IKT parka inventarizāciju kā pirmo darāmo darbu.

Jums ir nepieciešams kāds, kas sistemātiski pārvaldītu un uzraudzītu informācijas tehnoloģiju līdzekļus, personāla drošības un darba procedūras – informācijas drošības vadītājs. Šo lomu var sekmīgi pildīt tikai tad, ja informācijas drošības vadītājs ir iesaistīts iestādes vadībā, ir neatkarīgs no IT daļas un viņa sniegto vadlīniju gadījumā tiek nodrošināts iestādes augstākās vadības atbalsts. Ja nepieciešams, datu pārvaldības organizēšanā var apvienot lomas, kas izriet no dažādiem tiesību aktiem, piemēram, informācijas drošības vadītājs un datu aizsardzības speciālists. Vairāk par informācijas drošības vadītāja lomu lasiet šeit.

2. IZMANTOJIET NOTEIKTOS STANDARTUS UN LABĀS PRAKSES

Iestādes informācijas drošības organizācijai jābūt balstītai uz noteiktajiem standartiem/normatīvajiem aktiem un labajām praksēm. Organizējot informācijas un tīkla drošību, iestādes vadītājiem jāpieprasa, lai tiek nodrošināta atbilstība noteikumiem un notiek sistemātiskas atskaites. Pašreiz kiberdrošības minimālie standarti ir noteikti Ministru kabineta 2015. gada 28. jūlija noteikumos Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām”. Pašlaik tiek gatavoti grozījumi šajos noteikumos, kā arī tiek izstrādātas kiberhigiēnas vadlīnijas. Taču jau esošie noteikumi sniedz atbildes uz jautājumu, kā organizēt informācijas tehnoloģiju līdzekļu pārvaldību, piekļuves un lietotāju tiesības, rezerves kopijas, datu nesēju aizsardzību u.c. jautājumus. IT drošības dokumentācijas paraugus var atrast šeit.

3. IZMANTOJIET VALSTS INSTITŪCIJAS OTRĀ LĪMEŅA DOMĒNU

Ne mazāk būtiski ir pārvaldīt iestādes valdījumā esošos domēnu vārdus, nodrošinot visu resursu pārvaldīšanu visā to dzīves ciklā. Aicinām iestāžu īpašumā esošo tīmekļvietnēm izmantot vienotu domēnu vārdu un elektroniskā pasta adrešu veidošanas kārtību, lietojot otrā līmeņa tīmekļvietņu domēna vārdu gov.lv. Vienota un droša domēna izmantošana ne tikai pasargā iestādes un sabiedrību no krāpnieciskām aktivitātēm, bet arī veicina sabiedrības uzticēšanos valsts un pašvaldību institūcijām. Iestādes izmantotos domēnus ir jāturpina uzturēt arī pēc tam, kad tie vairs netiek izmantoti, lai novērstu šo domēnu vārdu izmantošanu ļaunprātīgu un krāpniecisku darbību veikšanai.

4. PLĀNOJIET ATBILSTOŠUS RESURSUS KIBERDROŠĪBAS NODROŠINĀŠANAI

Tas, cik daudz līdzekļu jāpiešķir kiberdrošības pasākumiem, var atšķirties, balstoties uz drošības prasībām, kas attiecas uz konkrēto iestādi, iestādē pieejamo kompetenci un iestādes risku izvērtējumu. Iestādes IKT budžeta apstiprināšanas procesā ir jāpieprasa, lai IT vadītājs sadarbībā ar informācijas drošības vadītāju veic risku izvērtējumu un atsevišķi norāda ar kiberdrošību saistītās izmaksas. Nepieciešamības gadījumā CERT.LV var palīdzēt ar metodiku un informāciju risku izvērtējuma sagatavošanai.

5. REGULĀRI PĀRBAUDIET PAKALPOJUMU UN SISTĒMU DROŠĪBU

Vienojieties par principiem iestādē, ka pirms jaunu servisu vai jaunu versiju ieviešanas (dzīves uzsākšanas), vienmēr ir jāveic drošības testi. Ir jāpieprasa sistemātiska savu pamatpakalpojumu pārbaude vismaz reizi 2 gados, tam nepieciešama līgumu esamība un finanšu līdzekļu plānošana budžetā. Publiskā sektora iestādes un kritiskās infrastruktūras turētāji var saņemt bezmaksas pakalpojumu klāstu no CERT.LV.

CERT.LV pakalpojumu katalogā pieejami šādi pakalpojumi:

- Incidentu izmeklēšana (cert@cert.lv)
- Agrās brīdināšanas tīkla (ABS) sensors
- DNS ugunsmūris (dnsmuris.lv)
- CERT.LV SOC (SIEM un EDR/XDR) pakalpojumi
- CERT.LV draudu medības
- CERT.LV ielaušanās testi / audits
- Pikšķerēšanas uzbrukumu simulācija
- CERT.LV vadīti darbinieku izglītošanas semināri

6. APMĀCIET DARBINIEKUS PAR KIBERDROŠĪBU

Kiberdrošība iestādē kopumā ir atkarīga no pārdomāti ieviestas kiberdrošības politikas un katra darbinieka kiberpratības. Diemžēl pieredze rāda, ka bieži vien lietotāji mēdz rīkoties neapdomīgi un riskanti, kādēļ ir būtiski darbiniekus regulāri apmācīt, sniedzot pamatzināšanas par kiberhigiēnu un tās sistemātiski atsvaidzinot. Ja iestādei nav sava resursa, lai organizētu apmācības, publiskā sektora organizācijās to var palīdzēt nodrošināt CERT.LV, kas organizē dažādus informatīvus pasākumus gan visiem organizācijas darbiniekiem, gan tehniskajiem ekspertiem un par IT drošību atbildīgajiem.

7. IEGULDIET TĪKLU AIZSARDZĪBĀ UN VIENOTAS TELEMETRIJAS UZRAUDZĪBĀ

Izmantojiet ielaušanās novēršanas un atklāšanas risinājumus (ielaušanās noteikšanas sistēma IDS/Ielaušanās aizsardzības sistēma IPS), centralizētu drošības telemetrijas apkopošanu un apstrādi (SIEM/EDR/XDR) un pieprasiet informācijas drošības pārvaldniekam reģistrēt un analizēt drošības telemetrijas anomāliju apstrādi atbilstoši jūsu kiberdrošības politikai. Tīkla plūsmas drošības notikumu telemetrija incidenta izmeklēšanai būtu jāuzglabā vismaz 1 mēnesi. Normatīvie akti nosaka vēl ilgāku glabāšanu. CERT.LV nodrošina bezmaksas tīkla plūsmas (agrās brīdināšanas sistēma – ABS) sensorus un citus pakalpojumus publiskā sektora iestādēm un kritiskās infrastruktūras turētajiem. Lai noskaidrotu vairāk par šiem pakalpojumiem un tos pieteiktu, aicinām sazināties ar cert@cert.lv.

8. ŠIFRĒJIET DATU APMAIŅU

Viens no biežāk pielietotajiem uzbrukumu vektoriem ir saistīts ar iestādes e-pasta korespondences ļaunprātīgu izmantošanu. Pieprasiet, lai iestādes datu apmaiņa un jo īpaši e-pastu apmaiņa būtu šifrēta. Pilns ieteikumu saraksts e-pasta drošības nodrošināšanai ir atrodams ASV kolēģu vietnē https://cyber.dhs.gov/bod/18-01/, bet detalizētāku padomu saņemšanai vienmēr ir vērts sazināties ar cert@cert.lv.

9. PIEPRASIET, LAI CERT.LV TIKTU INFORMĒTS PAR IEVAINOJAMĪBĀM UN INCIDENTIEM

Neturiet informāciju par kiberincidentiem pie sevis un informējiet CERT.LV, kas uzrauga Latvijas kibertelpu. Ziņošana par katru incidentu ir nepieciešama, lai novērtētu kopējo situāciju valstī un tā ļauj mazināt arī citu iestāžu ievainojamības. Ātra ziņošana un informācijas apmaiņa ar CERT.LV palīdz mazināt riskus valstī kopumā un veicina vispārīgas drošības pamatprincipu īstenošanu. Saskaņā ar ITDL[1] pienākums ziņot par incidentiem ir visām valsts un pašvaldību iestādēm, kā arī IT kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem. Par incidentu ziņo, rakstot uz cert@cert.lv vai zvanot uz tālruni 67085888.

[1] Drīzumā ITDL tiks aizstāts ar Nacionālās kiberdrošības likumu.

10. PIEPRASIET INCIDENTA IZMEKLĒŠANAI KRITISKO AUDITĀCIJAS PIERAKSTU UZGLABĀŠANU UN APSTRĀDI

Vienojieties par auditācijas pierakstu saglabāšanas un apstrādes principiem, jo tas incidenta gadījumā palīdzēs identificēt iespējamos pārkāpumus un ar pakalpojumu nepārtrauktību saistītas problēmas. Svarīgi vienoties, kuri kritiskie auditācijas pieraksti tiks glabāti, un vēlams tos glabāt vismaz 1 gadu. Vairāk informācijas par žurnālu glabāšanu meklējiet www.cert.lv.

11. KARTĒJIET RISKUS UN UZTURIET IESTĀDES KRĪZES PLĀNU, PLĀNOJOT DARBĪBAS NEPĀRTRAUKTĪBU

Novērtējiet savus biznesa riskus un sagatavojiet plānu B. Ir svarīgi, lai būtu rīcības plāns krīzes pārvarēšanai un to sistemātiski praktizētu iestādē. Iepazīstieties ar mākoņpakalpojumu izmantošanas iespējām Latvijā un Eiropas Savienības vai NATO dalībvalstīs, lai plānotu pakalpojumu un darbības nepārtrauktībai kritisko datu pieejamību gadījumos, kad pamata infrastruktūra varētu nebūt pieejama.

12. IZMANTOJIET UZTICAMAS IZCELSMES UN DROŠUS PAKALPOJUMUS

Nav ieteicama tādu pakalpojumu un IKT risinājumu izmantošana, kuru izcelsmes vai uzturēšanas valsts ir ārpus Eiropas Savienības vai NATO. Izvēloties pakalpojumu sniedzējus, prasību izstrādē iekļaujiet vismaz tāda līmeņa IKT drošības prasības, kādas tiktu izvirzītas, ja plānoto pakalpojumu nodrošinātu ar saviem tehnoloģiskajiem resursiem, tai skaitā auditācijas pierakstu prasības un rīcību ārkārtas situācijās (drošības incidentos). Prasībās jāiekļauj arī personu datu apstrādes prasības, ja attiecināms, arī pakalpojuma sniedzēja nodarbināto apliecinājumus (par drošības prasību ievērošanu, tai skaitā par ierobežotas pieejamības un klasificētās informācijas neizpaušanu). Noteikti jāparedz informācijas resursu nodošana pakalpojuma pārtraukšanas gadījumā. Rūpīgi jāizvērtē bezmaksas mākoņpakalpojumu izmantošana. Bezmaksas bieži vien nozīmē, ka nebūs iespējams uzstādīt datu apstrādes ģeogrāfisko ierobežojumu, prasības auditācijas pierakstiem, rezerves kopijām vai datu izgūšanai pēc pakalpojuma pārtraukšanas.

13. PIEVIENOJIES KIBERDROŠĪBAS KOMPETENČU KOPIENAI UN CERT.LV KIBERDROŠĪBAS TĒRZĒTAVAI MM.CERT.LV

Kiberdrošības kompetenču kopiena kalpo kā sadarbības platforma valsts un pašvaldību iestādēm, privātā sektora profesionāļiem un kiberdrošības jomas pētniekiem. Vairāk par kiberdrošības kompetenču kopienu var uzzināt šeit vai rakstot uz e-pasta adresi NCC@mod.gov.lv. Savukārt iestādes IT un IT drošības personāls ir aicināts pievienoties mm.cert.lv tērzētavai, kas ļauj operatīvi uzzināt un dalīties ar aktuālo informāciju kibertelpā. Lai pievienotos, jāraksta uz e-pasta adresi cert@cert.lv.

UZZINI VAIRĀK:

www.cert.lv cert@cert.lv