LATVIJAS PAŠVALDĪBU SAVIENĪBA

Mazā Pils iela 1, Rīga, LV-1050
Tālr. 67226536, fakss 67212241
e-pasts: lps@lps.lv
www.lps.lv

Nod. maks. kods: 40008020804
Nor. konts LV53UNLA0001001700906
AS "SEB banka"
kods UNLALV2X

Rīga
06.09.2018. Nr. 0720182104/A1271
Uz 25.07.2018. Nr. MV-N/1836

Aizsardzības ministrijai

Par Latvijas kiberdrošības stratēģiju nākošajam plānošanas periodam

Priekšlikums Aizsardzības ministrijai nākamā plānošanas perioda (2019.–2022. gadam) Latvijas kiberdrošības stratēģijas izstrādes laikā veikt auditu, lai noskaidrotu, kur atrodas ministriju, dienestu, pašvaldību un citu iestāžu ievadītie dati. Vēlamies informēt, ka iestādes ir datu lietotāji, rediģētāji un ievadītāji, bet ne visi dati atrodas valsts īpašumā esošos serveros. Sakarā ar to, ka tīkla infrastruktūra starp iestādēm nav vienota un dati tiek sūtīti, izmantojot globālo tīmekli (internetu), kas būtiski palielina datu noplūdes risku, jāievieš vienots tīkla risinājums starp iestādēm. Papildus vēršam uzmanību arī uz mākoņdatošanas pakalpojuma izmantošanu, jo nav kontroles mehānismu, kā nodrošināt datu drošību, piemēram, mākoņdatošanas pakalpojumā "Office 365", "OneDrive", "Dropbox". Izskatīt iespēju valsts mērogā izmantot e-pasta serverus, kas elektroniskās vēstules sūta tikai šifrētā veidā.

Ieteikums valsts mērogā veidot centralizētu datu pārraides tīklu starp iestādēm, ko uzrauga, piemēram, CERT, kas būtu kā galvenā vārteja uz globālo tīmekli (internetu). Risinājums būtiski palielinātu datu tīkla drošību, jo iestāžu galvenajiem vārtejas maršrutētājiem būtu iespēja neizmantot noklusēto vārteju (*default route*). Izmantojot noklusēto vārteju, maršrutētājs, aiz kura atrodas iestādes datu tīkla infrastruktūra, ir viegli sasniedzams no globālā tīmekļa, no jebkuras IP adreses. Ieviešot centralizētu datu tīklu ar šifrēšanu un skaidri definētām vārtejām, var turpināt izmantot vēsturiski ieviestos datu pārraides servisus, kas šobrīd ir neaizsargāti un bez iespējas datu pārraidi šifrēt. Šādu centralizētu risinājumu var veidot, izmantojot VPN (virtuālie privātie tīkli) ar IPsec šifrēšanu vai ideālajā gadījumā izdalītas optiskās dzīslas starp iestādēm. Izmantojot centralizētu tīklu, piemēram, uz CERT, būtu iespēja centralizēti kontrolēt datu plūsmu starp iestādēm, nodrošinot pārskatāmību (monitoringu) un aizsardzību ar centralizētu ugunsmūri. Papildus šāds risinājums pildītu iestāžu centralizētā datu tīkla datu izsūtīšanu un saņemšanu no globālā tīmekļa (interneta). Ja starp iestādēm būtu pieejama izdalīta optiskā dzīsla, rezerves kopijas (*backup*) varētu glabāt kādā citā pašvaldības iestādes serveru telpā. Šāds risinājums būtu pilnvērtīgs rezerves kopiju glabāšanai, jo rezerves kopijas atrastos dažādos ģeogrāfiskos punktos. Papildus izdalīto optisko dzīslu starp pašvaldībām var izmantot kā rezerves datu kanālu gadījumos, ja kāda no optiskajām līnijām tiktu bojāta vai būtu apkopē.

Vēlamies vērst uzmanību uz CERT organizētajiem pasākumiem, kuros informācijas sistēmas tiek uzlauztas mācību nolūkos. Šādos pasākumos ir pierādījies, ka visievainojamākās ir *Microsoft Windows* operētājsistēmas. Atvērtā koda operētājsistēmas ir ievainojamas, ja nav korekti iestatītas. Sakarā ar jauno *Microsoft*

Windows 10, kas atjauninājumus var saņemt no citām darba stacijām nekontrolēti un lietotāja ierīces datus nosūta *Microsoft*, nepieciešams centralizēti nodrošināt iestāžu darba staciju datu tīklā pārraidāmo datu kontroli. Šāda kontrole būtu iespējama ar centralizētu iestāžu datu tīklu, kuram ir kontrolēta pieeja globālajam tīmeklim (*internet*). Izmantojot atvērtā koda operētājsistēmas (uz *unix* bāzes), jāņem vērā, ka tās vēsturiski dalītas dialektos "BSD" un "System 5". Ieteikums serveru risinājumos izmantot *unix* operētājsistēmas dialektā "BSD", kas ir ar daudz lielāku dzīves ciklu un kam katra nākamā versija savietojama ar iepriekšējo versiju. Papildu drošība atvērtā koda operētājsistēmām ir jau failu sistēmā, kur iespējams norādīt datnes pieejas tiesības. Atvērtā koda operētājsistēmās kodola līmenī ir pieejams ugunsmūris, kas būtiski palielina drošību atšķirībā no *Microsoft* operētājsistēmas, kuras ugunsmūris ir tikai atsevišķa aplikācija. Atvērtā koda operētājsistēmām ir pieejamas failu sistēmas, kas var glabāt liela apjoma informācijas daudzumu; papildus izmantojot *Logical Volume Manager* (LVM) iespējas, tā var būt dinamiski palielināma un šifrējama.

Mākoņdatošanai ir lielas priekšrocības, bet valsts iestādēm nav ieteicams izmantot globālajā tīmeklī pieejamos mākoņdatošanas pakalpojumus, jo iestādes apstrādā personu datus, kas būtu jākontrolē. Ieteikums CERT piesaistīt Latvijas Atvērto tehnoloģiju asociāciju (LATA), lai izveidotu pilnvērtīgu mākoņdatošanas pakalpojumu, kuru kontrolētu valsts atbildīgās iestādes, piemēram, CERT, serveru telpā. Mākoņdatošanas serveri, kas būtu pieejami iestādēm no iestāžu centralizētā datu tīkla, varētu būt arī kā rezerves kopiju glabātuve. Mākoņdatošanas serverī datnes netiek pilnībā dzēstas vai neatgriezeniski rediģētas. Papildus tam iestādēm būtu ērtāk vērsties pie mākoņdatošanas pakalpojuma sniedzēja un atgūt zaudēto informāciju.

Latvijas kiberdrošības stratēģijā visi uzskaitītie mērķi ir vērsti uz preventīvām darbībām, bet varbūt vajadzētu ieviest arī pozīciju, kas paredzētu rīcības plāna izstrādi, informācijas sniegšanu, kā rīkoties, un palīdzību reālā kibernozieguma gadījumā gan fiziskai personai, gan juridiskai personai vai valsts iestādei, lai radītu drošības sajūtu, ka nepieciešamības gadījumā katrs var saņemt padomu vai praktisku palīdzību.

Lai efektīvi sasniegtu Kiberstratēģijā definēto mērķi "sabiedrības izglītošana", ņemot vērā izmaiņu straujo vidi informācijas tehnoloģiju (IT) jomā, katrā valsts un pašvaldības institūcijā būtu nepieciešams:

1. veicināt par IT drošību atbildīgo darbinieku piedalīšanos starptautiskās IT drošības konferencēs;
2. nodrošināt regulāras apmaksātas mācības IT drošības jomā vismaz personām, kuru pienākumos ietilpst IT drošības jautājumu risināšana un pārvaldība, organizācijas darbinieku apmācīšana par IT drošības jautājumiem, piemēram, šādās tēmās:
   - *CyberSec First Responder: Threat Detection and Response* (CFR)
   - *CompTIA Cybersecurity Analyst* (CySA)
   - *CompTIA Advanced Security Practitioner* (CASP)
   - Sertificēta informācijas sistēmu drošības profesionāļa (CISSP) sagatavošanas kurss
   - *Certified Ethical Hacker v.10* (CEH)
   - Sertificēts informācijas sistēmu auditors (CISA)
   - Sertificēts informācijas drošības vadītājs (CISM)

Attiecībā uz kiberdrošības noturības veicināšanas mērķa sasniegšanu vispirms jānodrošina informācijas aprite par esošo kiberdrošības noturības līmeni, šī līmeņa

izmaiņām, izmaiņu cēloņiem (ja iespējams, aprakstot konkrētas situācijas un to risinājumus), t. i., informēt atbildīgās personas valsts un pašvaldību institūcijās par kiberdrošības noturības līmeni valsts un pašvaldības institūcijās un rekomendējamiem pasākumiem kiberdrošības noturības līmeņa celšanai un digitālās drošības risku mazināšanai.

Ir ES dokuments *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. [JOIN(2013) 1 final] - 7/2/2013*, kas nosaka Eiropas kiberdrošības stratēģiju ar šādiem mērķiem:
- To achieve cyber resilience: develop capabilities and cooperating efficiently within the public and private sector;
- To secure critical information infrastructures;
- To reduce cybercrime;
- To develop the industrial and technological resources for cybersecurity;
- To contribute to the establishment of an international cyberspace policy.

Šie mērķi ir diezgan līdzīgi AM izvirzītajiem mērķiem, tomēr nesakrīt: te jautājums par pamatojumu – kāpēc nacionālā līmenī virzām līdzīgus, bet nedaudz citus mērķus nekā ES?

Jāņem vērā, ka ES ir uzsākusi pārskatīt Eiropas kiberdrošības stratēģiju. 2017. gada 13. septembrī tika publicēts dokumenta projekts *Proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('"Cybersecurity Act'")*, kas piešķir jaunu lomu *European Union Agency for Network and Information Security (ENISA)* un ES līmenī beidzot nosaka ar kiberdrošību saistīto terminu definīcijas (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0477). Papildus tam ES kiberdrošībai veltītajā vietnē (http://www.consilium.europa.eu/en/policies/cyber-security/) ir publicēti materiāli, kas paredz jaunas aktivitātes, piemēram, *EU-wide cyber security certification scheme* ieviešana, *Creating an effective criminal law response*, attiecīgi arī Latvijas kiberstratēģijas mērķi un aktivitātes būtu jāsaskaņo ar esošajiem un jaunajiem ES noteiktajiem mērķiem un attīstības virzieniem.

Priekšsēdis Gints Kaminskis

06.09.2018. 14:19
1115
Guntars Krasovskis, padomnieks informācijas tehnoloģiju jautājumos
67508560, 29104238, guntars.krasovskis@lps.lv