Kas Latvijai ir svarīgs kiberdrošībā 2014.gadā?

Jānis Sārts, Aizsardzības ministrijas valsts sekretārs, Nacionālās informācijas tehnoloģiju drošības padomes priekšsēdētājs

01. marts 2014 00:02

Latvijas virtuālo telpu, kurā saplūst fiziskā un digitālā rīcība, raksturo dinamiska attīstība, kur mijiedarbojas valsts pārvalde, sabiedrība un ekonomika.

Latvijas sabiedrība ir arvien aktīvāka informācijas un komunikācijas tehnoloģiju piedāvāto iespēju izmantotāja, ko apliecina arī fakts, ka privātpersonu īpatsvars, kuras regulāri lieto internetu, ir pieaudzis no 50% 2009.gadā līdz 70% 2013.gadā.

Arvien plašāk tiek izmantots drošs e-paraksts, elektroniski parakstīti ir jau aptuveni 1,7 miljoni dokumentu , bet portālā Latvija.lv ir pieejami 65 dažādi e-pakalpojumi. Latvijā ir attīstījies spēcīgs informācijas tehnoloģiju privātais sektors, kur kā piemērus var izcelt Latvijā samērā nesen radīto uzņēmumu Cobook, Infogram un sociālā tīkla Ask.fm popularitāti pasaules mērogā un spēju piesaistīt ievērojamus finanšu līdzekļus. Ir skaidri redzams, ka Latvijā nepārtraukti notiek modernas un inovatīvas sabiedrības attīstība.

Uzticība kibertelpai un tās drošība ir jebkuras informācijas sabiedrības fundamentāls pamats, un bez tās nav iespējama stabila un ilgtspējīga attīstība. Tāpēc arvien pieaugošais informācijas un komunikācijas tehnoloģiju pielietojums valsts, biznesa un vispārējās sabiedrības līmenī, nosaka, ka, līdz ar kibertelpas iespēju paplašināšanos, palielinās tās apdraudējumu skaits un sarežģītība. Ir neizbēgami, ka valstīm aizvien vairāk nāksies domāt par savas sabiedrības aizsargāšanu šķietami abstraktajā kibertelpā, un celt gan institūciju, gan indivīdu izpratni par atbildīgumu kibertelpā.

Latvija pēdējos gados ir veikusi nozīmīgus pasākumus, lai ieliktu pamatus virzībai uz drošāku kibertelpu, starp kuriem var minēt IT drošības likumu, CERT.LV vienības izveidi, nesen pieņemto Latvijas kiberdrošības stratēģiju 2014.-2018.gadam, kā arī uzsākto Kiberzemessardzes vienības veidošanu. Latvijas līdzšinējie soļi kiberdrošības jomā tiek atzinīgi novērtēti arī Eiropas un starptautiskā līmenī.

Apzinoties, ka kibertelpas drošība kļūst par nacionālās drošības neatņemamu sastāvdaļu, Aizsardzības ministrija (AM) ir uzņēmusies vadošās valsts institūcijas lomu kiberdrošības politikas jomā, un vadot Nacionālās informācijas tehnoloģiju drošības padomi (turpmāk – Padome), šim gadam ir izvirzījusi trīs kiberdrošības jomas prioritātes, kas aptver gan nacionāla, gan starptautiska mēroga pasākumu īstenošanu ceļā uz drošāku Latvijas kibertelpu.

Valsts sektors: no labticīgas ignorances uz atbildīgu pieeju

Lai arī kibertelpā drošs nevar justies neviens, visaptveroši aizsardzības pasākumi ļauj nodrošināt digitālo procesu nepārtrauktību, uzticamu informācijas apriti un drošu datu uzglabāšanu, kas ir svarīgi kā privātā, tā valsts sektorā. Labi apzinoties, cik cieša saistība ir nedrošām, neuzticamām informācijas tehnoloģijām ar komerciālajiem zaudējumiem, finanšu sektors ir vieni no līderiem savas kibertelpas aizsardzības pasākumu nodrošināšanā. Tomēr kibertelpas kopējā ainā šis sektors aizņem nosacīti nelielu daļu iepretim tam vairākumam, kuru nereti vada pārliecība, ka virtuālā vide ir kaut kas tāls, abstrakts un nesaistāms ar to, kas notiek fiziskajā realitātē.

Valsts uzdevums ir rūpēties par savas informācijas un komunikācijas tehnoloģiju (IKT) infrastruktūras

un valsts informācijas sistēmu drošību, kā arī aizsargāt IKT kritisko infrastruktūru, lai nodrošinātu valstij un sabiedrībai būtiskas pamatfunkcijas, kur kā zināmākās var minēt telekomunikācijas, satiksmi un enerģētiku. Šobrīd IT drošības likums valsts, pašvaldību institūcijām un privātajiem komersantiem nosaka pamata prasības, tomēr daudzām institūcijām kiberdrošība beidzas līdz ar drošības prasību "minimālā komplekta" izpildi.

Tiesa, ir novērojama pozitīvā tendence, ka institūcijas sāk apzināties nepieciešamību rūpīgāk attiekties pret savu informācijas sistēmu un lietotāju datu drošību. Tāpat, jāmin, ka šogad valsts pārvaldē tiks uzsākta centralizētas IKT drošības profilakses platformas izveide, kas būtiski palielinās valsts iestāžu spējas identificēt un novērst informācijas tehnoloģiju drošības incidentus. Tomēr progress attiecībā uz institūciju pieeju kiberdrošībai ir bīstami lēns attiecībā pret tiem riskiem un draudiem, kas kibertelpā strauji attīstās katru dienu.

Tādi nopietni incidenti kā ielaušanās Valsts ieņēmumu dienesta datu bāzē 2010.gadā un 2013.gada beigās izgūtie 3000 lietotāju dati no Nodarbinātības valsts aģentūras sistēmām , apliecina, ka institūcijām jāturpina mācīties, cik lielu ietekmi uz viņu darbu var atstāt neaizsargātas informācijas sistēmas. Protams, ierobežoti finanšu resursi un kompetentu speciālistu trūkums ir šķērslis procesu ātrākai virzībai, tomēr pamata problēma vēl joprojām ir vispārējā paviršā attieksme pret nepieciešamību pēc šādiem drošības pasākumiem.

Padome uzskata, ka šajā gadā ir būtiski stiprināt valsts resora kiberdrošības līmeni. Fokuss tiks vērsts uz izpratnes līmeņa celšanu par aizsardzības pasākumu nepieciešamību darbam virtuālajā telpā, un institūciju mudināšanu iespēju robežās rīkoties vēl pirms bezatbildība ir radījusi ekonomiskus vai sociālus zaudējumus. Pievēršot adekvātu uzmanību kiberdrošībai politiskā un valsts pārvaldes līmenī, ir iespējams stimulēt pārmaiņas plašākā valsts mērogā. Ir svarīgi demonstrēt, ka mūsdienās, kad virtuālā vide dominē pār fizisko, drošības līmeni daudz vairāk var ietekmēt nevis fiziskie, bet digitālie draudi – kiberuzbrukumi, kibernoziegumi, kiberhuligānisms, kiberspiegošana u.c. Padome ir pārliecināta, ka valsts sektoram ar savas attieksmes maiņu ir jābūt kā paraugam privātajam sektoram un ikvienam indivīdam. Savukārt privātajam sektoram būs izšķiroša loma, lai veicinātu savu un visas Latvijas globālo konkurētspēju, un tur neiztikt bez spēcīgas kompetences informācijas tehnoloģiju drošības jomā.

Prezidentūra – lielas iespējas un lieli izaicinājumi

Latvijas prezidentūra Eiropas Savienības (ES) Padomē 2015.gada pirmajā pusē būs nozīmīgs notikums, kurš Latvijai pavērs iespējas pierādīt savu politisko briedumu, veidojot ES politiskās prioritātes un dienaskārtību, organizējot svarīgas ES institūcijas darbu, kā arī vadot ekspertu darbu dažādās darba grupās. Kā vienu no prezidentūras prioritātēm Latvija ir izvirzījusi informācijas sabiedrības stiprināšanu , kur liela loma būs kiberdrošības izaicinājumu risināšanai un kibertelpas aizsardzības stiprināšanai kā nacionālā, tā ES mērogā. Latvijai prezidentūras laiks jāuztver kā izdevība pārējai Eiropai demonstrēt mūsu līdzšinējos sasniegumus e-pārvaldē, informācijas sabiedrības un tehnoloģiju attīstībā un kiberdrošībā. Līdztekus tam, Latvijas mērķis šo sešu mēnešu laikā ir būt galvenajam ideju un iniciatīvu virzītājam, veicinot sakārtotāku un drošāku ES kibertelpu.

Pēdējos gadu dalībvalstis strādā pie ES direktīvas, kas noteiktu vienādi augstus standartus attiecībā uz tīklu un informācijas drošību. Ņemot vērā atšķirības starp dalībvalstīm kiberdrošības ziņā, Latvija ir ieinteresēta pēc iespējas augstāku drošības standartu noteikšanā. Taču tik, cik lielas ir atšķirības drošības līmeņa ziņā, tikpat lielas nesaskaņas ir par to, kā saskaņot direktīvas mērķus ar dalībvalstu nacionālajām interesēm un kapacitāti. Pastāv iespēja, ka šīs direktīvas izstrāde turpināsies mūsu prezidentūrā, kas nozīmē, ka kopā ar ES Kiberdrošības stratēģiju, Latvijai būs jāvada nozīmīgu dokumentu izvērtēšana un virzība uz reālu to mērķu īstenošanas uzsākšanu.

Lai arī kiberdrošības politisko izaicinājumu pārvarēšana būs izšķiroša mūsu prezidentūras sekmīguma novērtējumā, var apgalvot, ka vēl svarīgāka par to būs kibertelpas tehniskās drošības garantēšana. Pusgads Eiropas skatuves centrā nozīmēs ne tikai gozēšanos starmešu gaismā, bet arī gatavību uzņemt un atvairīt potenciālos triecienus. Nesenā Lietuvas prezidentūra skaidri demonstrēja, cik ļoti prezidējošai valstij ir jārēķinās ar iespējamību, ka neapmierinātība ar visas ES rīcību vai lēmumiem tiek pausta kiberuzbrukumu veidā pret prezidējošo valsti.

Lietuvieši veiksmīgi izturēja savu nacionālo kiberspēju piespiedu testēšanu, tomēr Latvijai tāpēc nevajadzētu zaudēt modrību un atlikušos 10 mēnešus līdz 2015.gadam nepieciešams izmantot, lai maksimāli sagatavotos paaugstināta kiberapdraudējuma periodam. Pirmajā šī gada Nacionālās

informācijas tehnoloģiju drošības padomes sēdē institūcijas informēja par saviem gaidāmajiem darbiem prezidentūras sakarā un priecē, ka drošības pasākumu ieviešana vai uzlabošana ir apzināta kā viena no prioritātēm.

Ņemot vērā kiberdrošības jautājumu komplekso dabu, likumsakarīgi liels ir arī iesaistīto institūciju loks (kopā 17), kas Latvijā atbild par kibertelpas drošības stiprināšanu. Padome turpmākā gada laikā strādās ar visām iesaistītajām pusēm, lai stiprinātu nacionālo koordināciju gan īstenojot prezidentūras politiskās prioritātes, gan rūpējoties par tehniskās kapacitātes atbilstību šim augsta līmeņa pasākumam. Prioritāte būs ne tikai valsts institūciju darba koordinācijai, bet arī konstruktīvas sadarbības turpināšanai un plašai nozares pārstāvju iesaistei. Uz esošo resursu bāzes, AM ir izveidojusi sekretariātu Padomes darba organizēšanai un atbalstīšanai, bet Nacionālo bruņoto spēkos uzsākot Kiberzemessardzes formēšanu, ir piesaistīti jau pirmie Latvijas privātā sektora speciālisti, uz kuriem varam paļauties kā spēcīgu papildspēku potenciālas krīzes situācijas gadījumā.

Sadarbība ar starptautiskajiem partneriem

Virtuālās vides [nemateriālā daba] nosaka to, ka kibertelpai nav ģeogrāfisku robežu un valsts kibertelpā nav norobežota no draudiem, kuri var rasties jebkurā citā pasaules malā. Tādējādi neviena valsts nevar pati saviem spēkiem mazināt kibertelpā esošos apdraudējumus un atrisināt tajā esošās problēmas. Sadarbība ar citām valstīm ir iespēja kopīgiem spēkiem mazināt kiberdraudu izplatību, meklēt labākos politiskos un tehniskos risinājumus atbildot uz pieaugošajiem kiberdrošības izaicinājumiem, kā arī stiprināt kopējās kiberaizsardzības spējas.

Kiberdrošības jautājumi arvien lielāku nozīmi ieņem arī ES un NATO darbakārtībā, un Latvija iesaistās abu šo organizāciju iniciatīvās attiecībā uz drošības līmeņa paaugstināšanu gan praktiskos treniņos un mācībās, gan politikas veidošanā. Ņemot vērā Baltijas un Ziemeļvalstu reģiona līdzīgi augsto tehnoloģisko attīstību un sabiedrību plašo izpratni par e-iespējām, ciešāka reģionālā sadarbība ar šīm valstīm dotu visskaidrākos kibertelpas drošības stiprināšanas rezultātus pārskatāmā nākotnē. Šogad Baltijas valstis plāno noslēgt konkrētas vienošanās par praktisko sadarbību gan kibertelpas drošības stiprināšanai starp Baltijas CERT vienībām, gan izmēģināt pirmo e-pakalpojumu sistēmu saslēgšanu. Šādu iniciatīvu tālāka attīstība celtu ne tikai kopējo Baltijas kibertelpas drošības līmeni, bet arī būtu ieguvums lielai sabiedrības daļai, īpaši uzņēmējiem, kuriem ērtā un mūsdienīgā veidā būtu iespēja veikt dažādas birokrātiskās procedūras tuvējās kaimiņvalstīs.

Sadarbība starptautiskajā jomā nav iespējama bez ciešas privāto partneru iesaistes. No vairākām valstīm kā, piemēram, Apvienotās Karalistes, ir vairāki konkrēti sadarbības piedāvājumi, un šajā gadā Latvija grib tos izmantot, dodot iespēju industrijas uzņēmumiem iesaistīties gan praktiska līmeņa apmācībās, tādējādi ceļot savu tehnisko kapacitāti, gan daloties labās prakses piemēros dažādos divpusējos formātos. Padome 2014.gadā tiks stiprināta kā platforma, kur privātā un nevalstiskā sektora pārstāvjiem ir iespēja saņemt informāciju par aktuālāko Latvijas kiberdrošības jomā, iespējām iesaistīties dažādos starptautiskos projektos, piesaistot finansējumu savas institūcijas kiberspēju kapacitātes celšanai, tādējādi stiprinot arī kopējo Latvijas kibertelpas drošību.

2014.gads – izaicinājumi tikai priekšā

Latvijā jau šobrīd ir attīstījusies spēcīga informācijas sabiedrība, kur nozīmīgi spēlētāji ir gan valsts, gan privātais sektors. Tāpat, ir attīstītas būtiskas kibertelpas drošības stiprināšanas iniciatīvas un radīti labās prakses piemēri abos sektoros. Tomēr Latvijā gan institūcijām, gan indivīdiem vēl joprojām nepieciešams mācīties, lai kļūtu par atbildīgiem un apzinīgiem globālās kibertelpas pilsoņiem.

Riski kibertelpā vēl joprojām netiek apzināti adekvātā līmenī, un valsts sektoram vispirms jau ar savu piemēru būtu jādemonstrē skaidra izpratne, ka kiberdraudi ir nevis nākotnes izaicinājums, bet šodienas realitāte.

Kibertelpas drošības stiprināšanai var izvirzīt neskaitāmas prioritātes, sākot no akadēmisko zināšanu veicināšanas tehniskā, politiskā un tiesiskā jomā, IKT drošības speciālistu sagatavošanas, sabiedrības vispārējās izpratnes līmeņa celšanas līdz kibernoziegumu mazināšanai un valsts sagatavotībai kiberkrīzes situācijās. Visi šie jautājumi ir būtiski Latvijai, tomēr izvirzītās trīs prioritātes, lai arī aptver plaša spektra jautājumus, fokusējas uz svarīgāko – kļūt drošākiem kibertelpā, veidojot atbildīgu valstisko pieeju kiberdrošības jautājumiem. Tas palīdzēs augstā līmenī novadīt gaidāmo prezidentūru ES un, rādot piemēru, izglītot gan privāto sektoru, gan sabiedrību kopumā. Tai pašā laikā jāapzinās, ka drošas nacionālās kibertelpas attīstība nav iespējama bez starptautiskās sadarbības, kurā plaši tiek iesaistīta gan valsts, gan industrija.