CERT.LV — jauns instruments Latvijas kiberdrošībai

Taivo Trams

Foto — Normunds Mežiņš.

Jaunais gads iesācies cerīgi arī valsts kiberdrošības jomā — no 1. janvāra CERT.LV jeb Informācijas tehnoloģiju drošības incidentu novēršanas institūcija darbojas Aizsardzības ministrijas (AM) pakļautībā. Laikā, kad kibertelpa kļūst par tikpat ierastu konfliktu zonu kā sauszeme, gaiss un ūdens, tas ir ļoti būtiski.

Jauns intelektuāls un tehnoloģisks resurss

Līdz aizvadītā gada nogalei CERT.LV darbību pārraudzīja Satiksmes ministrija. Pakļautības maiņa ikdienas darbu neietekmē, tieši pretēji — paver jaunas iespējas, lai stiprinātu valsts spējas pretoties apdraudējumiem interneta un informācijas tehnoloģiju vidē.

«Mūsuprāt, CERT.LV iekļaušana valsts aizsardzības sistēmā ir loģisks solis un vienlaikus arī objektīva resursu optimizācija. Skaidrs, ka IT drošības jautājums skar daudzas iestādes un nozares un arvien pieaugošāku lomu tas ieņem arī valsts drošības aspektu kopumā. Esam pārņēmuši šo jautājumu, vienlaikus apņemoties iespēju robežās celt CERT.LV kapacitāti un spējas, jo ir skaidrs, ka šis darba lauks tikai augs un kļūs arvien plašāks,» norāda AM vecākā eksperte — **valsts sekretāra padomniece Ieva Kupce**.

No malas varētu izskatīties, ka CERT.LV darbā tagad nāk klāt kāda īpaša militārā sastāvdaļa. Taču CERT.LV tiek pārņemts ar deleģējuma līgumu — institūcijas darbību turpmāk nodrošina AM. «Likums diezgan precīzi nosaka, kas CERT.LV ir jādara, — un to viņi darīs arī turpmāk. Mēs uz saviem jaunajiem kolēģiem skatāmies drīzāk kā uz tuvāk pieejamu intelektuālu un tehnoloģisku resursu, kas ļaus arī ministrijā padziļināt savas zināšanas un attīstīt IT drošības virzienu. Viņu darbs nemainīsies, bet mēs maksimāli centīsimies izmantot šo tagad pieejamo jauno kapacitāti,» atzīst I. Kupce.

Arvien sarežģītākas un vieglāk pieejamas tehnoloģijas

Būtiskākais CERT.LV uzdevums ir darbs ar IT drošības incidentiem, palīdzot gan valsts un pašvaldību iestādēm, gan privātajām institūcijām. «Ja resurss atļauj, cenšamies neatteikt un palīdzēt visiem,» stāsta **CERT.LV vadītāja Baiba Kaškina**. Līdztekus CERT.LV aktīvi darbojas arī citās jomās. Daudz pūļu tiek veltīts sabiedrības izglītošanai — pagājušajā gadā dažādos pasākumos apmācīti ap 2000 cilvēku. CERT.LV speciālisti organizē informatīvos pasākumus, kuru galvenā mērķauditorija ir valsts un pašvaldību iestāžu par IT drošību atbildīgās personas, pārstāvji no interneta pakalpojumu sniedzējiem un citi cilvēki, kuru darbs ikdienā saistīts ar IT drošību. CERT.LV eksperti ir bieži viesi arī skolās, lielu interesi par viņiem izrāda arī komercuzņēmumi. «Bieži vien valsts iestāžu atbildīgās personas vēršas pie mums un lūdz nākt un stāstīt par šiem drošības apsvērumiem — pret mums klausītāji jūt lielāku respektu,» pasmaida B. Kaškina.

Būtiska preventīvā darba daļa ir kopējā stāvokļa uzraudzīšana valsts IT drošībā, lai problēmas varētu paredzēt jau iepriekš. Un šajā jomā situācija kļūst arvien sarežģītāka. Tehnoloģijas top aizvien komplicētākas — ikdienas lietotājam ir faktiski neiespējami izsekot līdzi to attīstībai, pat ekspertiem tas prasa pamatīgas pūles. Vienlaikus tehnoloģijas kļūst arvien plašāk un vieglāk pieejamas, uzsver I. Kupce. Arvien palielinās arī tehnoloģiju un interneta lietotāju skaits, tātad — pieaug potenciālo upuru skaits, savukārt atzīst B. Kaškina. CERT.LV novērojumi liecina arī par to, ka palielinās uzbrukumu sarežģītība kibertelpā, līdz ar to šo noziegumu atklāšanā ir jāiegulda vairāk resursu.

No izrādīšanās līdz politiskiem uzbrukumiem

Laika gaitā mainās arī uzbrukumu motīvi. Interneta aizsākumos galvenokārt varēja runāt par uzbrukumiem, kuru mērķis bija parādīt to īstenotāju prasmi, ļaujot palielīties ar uzlauztajām mājaslapām un nodarīto kaitējumu, bet pēdējos piecos gados vadošā tendence ir nauda — jebkurš veids, kā var nopelnīt. Un dažu pēdējo gadu laikā strauji pieaug arī politiski motivēti uzbrukumi internetā. «Nauda nekur nav pazudusi, bet tai līdzās tikpat aktīvs motīvs ir spiegošana, mērķēti uzbrukumi valsts iestādēm, arī mērķēti uzbrukumi komerciestādēm, lai iegūtu informāciju, ko var tālāk izmantot komerciāli,» stāsta B. Kaškina. Incidentus IT vidē var arī iedalīt divās pavisam lielās grupās — uzbrukumos, kas domāti visiem, un uz tiem parasti uzķeras ap 3—5% lietotāju, no kuriem ļaundari var iegūt kādu labumu, un uzbrukumos, kas domāti tieši vienai konkrētai personai vai uzņēmumam. Šie uzbrukumi ir rūpīgi izplānoti un ar visai augstu iespēju, ka uzbrukuma upuris patiešām iekritīs. «Ja kāds zina, ka šim cilvēkam vai organizācijai ir informācija, ko var izmantot tālāk vai pārdot, tiek mērķtiecīgi strādāts, lai piekļūtu pie datoriem, e-pasta sarakstes, failu glabātavām,» skaidro CERT.LV vadītāja.

Latvija — interesanta vieta kiberļaundariem

Latvija ir salīdzinoši interesanta vieta dažādu interneta ļaunprātību veikšanai, un te ir vairāki faktori, kas to veicina. Mēs esam *NATO* un ES sastāvdaļa, līdz ar to cilvēkiem un organizācijām aiz mūsu

valsts robežām, protams, ir interese arī par mūsu virtuālo pasauli. Otrs svarīgs faktors ir Latvijas IT jomas un interneta augstais attīstības līmenis pasaules mērogā. «Esam interesanti ar to, ka mums ir salīdzinoši ātrs internets. Mēs ar to ļoti lepojamies, bet tā ir arī ļoti laba vide eksperimentiem, piemēram, lai kāds hakeris patestētu savas spējas,» norāda I. Kupce. Pēc «Eirobarometra» datiem, Latvijā ir procentuāli daudz lietotāju, kas internetā izmanto dažādus valsts piedāvātus pakalpojumus. Uz lielo un t.s. veco Eiropas valstu fona mūsu sabiedrība ir salīdzinoši neliela un moderna, taču vienlaikus pieaug arī riski. Jo vairāk iedzīvotāji, uzņēmumi un valsts institūcijas sniedz pakalpojumus caur internetu un izmanto tos, jo lielāka vērība jāpievērš drošības aspektiem. Intereses pieaugumu par IT drošību mūsu valstī noteikti vairos arī gatavošanās Latvijas prezidentūrai ES.

Labi speciālisti un sakārtoti likumi

Savukārt Latvijas lielais pluss ir sakārtotā likumdošana — IT drošības likums visumā precīzi un skaidri apraksta gan atbildības, gan kompetences šajā jomā strādājošajiem. «Ir diezgan maz valstu, kurās ir pieņemts un darbojas šāds IT drošības likums. Valstij tas ir ļoti būtiski, jo ļauj nozares drošības uzraugiem rīkoties un darīt to, kas jādara nepieciešamības gadījumā. Daudzās valstīs ir šī problēma — vietējiem CERT vienkārši nav pilnvaru, nav tiesību saņemt informāciju utt.,» paskaidro Baiba Kaškina.

Liels pluss ir arī salīdzinoši daudz labu IT nozares drošības speciālistu. «Protams, vienmēr var vēlēties labāk un vairāk, bet zinoši cilvēki mums ir gan CERT.LV komandā, gan daudzās valsts un privātajās institūcijās,» atzīst CERT.LV vadītāja. Protams, ir daudzas lietas, kas jāsakārto un jāuzlabo — krīze atstājusi savas pēdas arī IT drošības jomā.

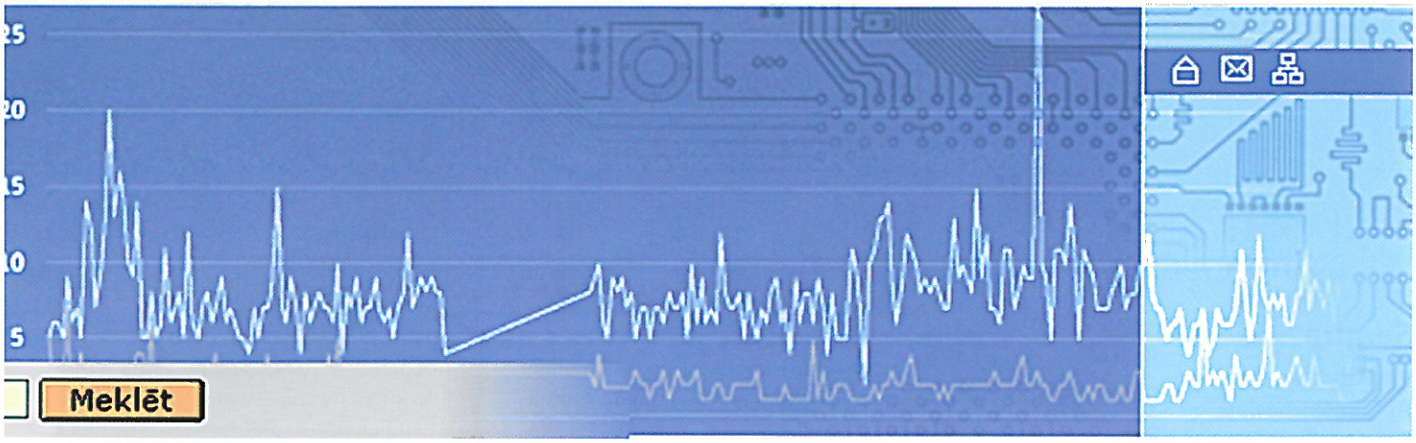
«Drošības situācija Latvijā ir līmenī. Jaunākais «*Microsoft*» IT drošības pārskats parādīja, ka drošības incidentu skaits valstī patiešām ir samazinājies. Pēc viņu datiem, mēs esam stabilā vidējā Eiropas līmenī,» saka I. Kupce.

IT drošībai par labu noteikti nāks arī topošā IT drošības stratēģija 2013.—2018. gadam, kas sakārtos dažādu valsts institūciju sadarbību kiberdrošības jomā. «IT drošības jautājumi skar daudzus sektorus — te ir gan izglītība un e-pārvalde, gan iekšlietu un tieslietu resori utt. Līdz ar to šis dokuments saliedētu visus minētos elementus kopējam darbam, noteiktu prioritātes, un katrs IT drošības jomā iesaistītais skaidri redzētu savu darba daļu, kas tam darāma,» stāsta I. Kupce. Satiksmes ministrijas vadībā un sadarbībā ar Nacionālo IT drošības padomi pašlaik norit darbs pie dokumenta izstrādes.

Top «kiberzemessardze»

Līdz ar CERT.LV nonākšanu AM pārziņā tiek attīstītas arī jaunas iestrādes. Viena no būtiskākajām, par ko pašlaik notiek aktīvas diskusijas, ir t.s. kiberzemessardzes projekts jeb Kiberaizsardzības vienība Zemessardzes sastāvā. «Tā varētu būt atsevišķa vienība Zemessardzē, kas strādātu tieši ar IT drošības jautājumiem un būtu gatava reaģēt lielāku drošības apdraudējumu gadījumā, kuri, es ceru, nepienāks,» skaidro I. Kupce. IT drošības ekspertu grupas izveide Zemessardzes paspārnē dotu tai juridisko platformu — darbības principus, tiesības un atbildību, kā arī iespēju piesaistīt vai mobilizēt speciālistus no nevalstiskā jeb privātā sektora krīzes situācijās.

Šīs vienības kodols būtu cilvēki, kas jau strādā šajā jomā un nepieciešamības gadījumā iesaistās IT incidentu risināšanā. «Būtībā tie ir brīvprātīgie, kas nepieciešamības gadījumā jau sniedz atbalstu arī CERT.LV. Daļa no viņiem varētu būt gatavi vairāk sadarboties ar valsti, uzņemties pastāvīgāku iesaisti drošības incidentu risināšanā valsts līmenī. Protams, ir cerība, ka mēs tagad varētu piesaistīt arī plašāku speciālistu loku un, izmantojot jau esošo speciālistu kodolu, ar viņu palīdzību apmācīt jaunus cilvēkus, kuriem būtu interese, bet pagaidām nav šo specifisko zināšanu,» stāsta CERT.LV vadītāja.



Brīvprātīgo vienību izveide IT drošības veicināšanai pēdējā laikā ir visai aktuāls jautājums ne tikai Latvijā. «Piemēram, briti par to aktīvi diskutē un domā par šādu rezervistu vienību izveidi. Šajā jomā viņiem jau ir uzkrāta sava unikālā pieredze saistībā ar olimpiskajām spēlēm,» saka I. Kupce. Līdzīgu ceļu gatavojas iet arī vairākas citas valstis.

Uzskatīt, ka situācija IT drošības jomā uzlabosies pati, noteikti nav pamata, tādēļ jāstrādā, lai saglabātu līmeni, kurā potenciālo apdraudējumu skaits nepieaug. «Potenciālie riski jāanalizē un jāidentificē apsteidzoši. Un jādara viss iespējamais, lai tos nevarētu viegli īstenot,» uzsver vecākā eksperte I. Kupce. Ar ierobežotajiem valsts finansiālajiem resursiem vērienīgas investīcijas CERT.LV tuvākajā laikā nav paredzamas, taču AM strādās pie pakāpeniska resursu pieauguma, kā arī vienlaikus piedāvās sava resora ietvaros pieejamās izaugsmes iespējas — ciešāku starptautisko sadarbību, aktīvāk iesaistot CERT.LV sadarbības projektos gan ar *NATO*, gan ASV un reģiona partnervalstīm.

Nespeciālistam tas varētu šķist pārsteidzoši, taču Latvijas kibertelpā vērā ņemami incidenti notiek katru dienu. «Ļoti nopietni incidenti, par laimi, ir retāki — kādas pāris, varbūt trīs reizes nedēļā,» saka CERT.LV vadītāja. Līdz ar CERT.LV nonākšanu valsts aizsardzības sistēmā ir pamatotas cerības, ka mēs būsim labāk sagatavoti potenciālajiem apdraudējumiem. «CERT.LV noteikti iederas valsts aizsardzības un drošības sektorā! Manuprāt, tagad ļoti daudzi elementi beidzot ir sastājušies savā vietā un ir gatavībā darbam,» rezumē Ieva Kupce.