Kibernoziegumi Latvijā

16.10.2017.

http://www.itiesibas.lv/raksti/komercdarbiba/komerctiesibas/kibernoziegumi-latvija/12443

AUTORS
Viktorija Jarkina
ZAB "Sorainen"
zvērināta advokāte, Dr.iur.

Internets, neapšaubāmi, kļuvis par sabiedrības dzīves, darba un ekonomikas neatņemamu sastāvdaļu. Vienlaikus internets ir arī viens no bīstamākajiem ieročiem noziedzībā. Ņemot vērā informācijas tehnoloģiju (IT) straujo attīstību, pat piesardzīgākais interneta lietotājs un drošākās IT sistēmas un datu bāzes var kļūt par nozieguma upuriem. Kibernoziegumi ir starptautiska mēroga problēma.

Kibernozieguma jēdziens

Pirmo reizi starptautisko tiesību jomā kibernoziegumu regulējums parādījās jau 2001.gadā Eiropas Padomes Konvencijas par kibernoziegumiem ietvaros. Konvencijā nav sniegta jēdziena "kibernoziegums" definīcija, paredzot to noregulēt valstu nacionālajos tiesību aktos. Aktuāls ir jautājums, vai aptverošu un nemainīgu definīciju, ņemot vērā nepārtrauktu IT tehnoloģiju attīstību, vispār ir iespējams sniegt.

Konvencijas ietvaros var izdalīt šādus noziedzīgus nodarījumus:

- nodarījumi pret informācijas sistēmu drošību (patvaļīga piekļuve, pārtveršana, datu traucēšana, sistēmu traucēšana, kaitīgās ierīces);
- ar datoriem saistīti noziegumi (datorkrāpšana);
- noziegumi pret autortiesībām un blakustiesībām;
- nelikumīgas informācijas aprites noziegumi (rasu naida, genocīda, kara kurināšana, bērnu pornogrāfijas aprite).

Latvijas tiesību normās jēdziens "kibernoziegums" nav atsevišķi definēts, kas tomēr nenozīmē, ka šie noziegumi Latvijā nav kriminalizēti. Arī Latvijas judikatūrā un tiesību doktrīnā nav vienotas kibernozieguma definīcijas. Viena no kibernozieguma definīcijām raksturo kibernoziegumus kā noziedzīgus nodarījumus pret automatizētas datu apstrādes sistēmas drošību – pret konfidencialitāti, pieejamību un integritāti.

Lai gan par kibernozieguma definīciju ir dažādi viedokļi un vairākas diskusijas, tomēr nav šaubu – par kibernoziegumiem atzīstami tikai tādi nodarījumi, kas izdarīti tiešsaistē (*on-line*).

Krimināllikuma regulējums

Latvijas Krimināllikumā (KL) kibernoziegumiem ir veltīti vairāki panti. Piemēram, KL 144.pantā paredzēta atbildība par korespondences, pa telekomunikāciju tīkliem pārraidāmās informācijas un citas informācijas noslēpuma pārkāpšanu (viens no piemēriem varētu būt e-pasta korespondences grozīšana, pieslēgums svešam e-pastam). Konkrētais noziedzīgais nodarījums ir vērsts pret personas pamattiesībām un brīvībām.

Datorkrāpšana ir regulēta KL 177.^{1}pantā. Jānorāda, ka datorkrāpšanu nevajag jaukt ar parastu krāpšanu, par kuru atbildība ir paredzēta KL 177.pantā. Datorkrāpšanai ir atšķirīgs noziedzīgā nodarījuma apdraudējuma objekts. Datorkrāpšanas "mērķis" ir datorsistēma, nevis cilvēks kā tradicionālajai krāpšanai. Datorkrāpšana, līdzīgi kā parasta krāpšana, arī ietilpst noziedzīgo nodarījumu pret īpašumu grupā.

KL 193.^{1}pantā paredzēta krimināltbildība par datu, programmatūras un iekārtu iegūšanu, izgatavošanu, izplatīšanu, izmantošanu un glabāšanu nelikumīgām darbībām ar finanšu instrumentiem un maksāšanas līdzekļiem. Tas ir noziedzīgs nodarījums tautsaimniecībā.

Saskaņā ar KL 241.pantu ir noteikta krimināltbildība par patvaļīgu piekļūšanu automatizētai datu apstrādes sistēmai. Savukārt KL 243.pantā ir paredzēta krimināltbildība par automatizētas datu apstrādes sistēmas darbības traucēšanu un nelikumīgu rīcību ar šajā sistēmā iekļauto informāciju. KL 244.pantā paredzēta krimināltbildība par nelikumīgām darbībām ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm. Savukārt KL 244.^{1}pantā – par datu,

programmatūras un iekārtu iegūšanu, izgatavošanu, izmainīšanu, glabāšanu un izplatīšanu nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām. Būtiski norādīt, ka KL 241.-244.[1]pantā kā noziegumu grupas objekts ir nodarījums pret vispārīgo drošību un sabiedrisko kārtību.

Atbildīgās iestādes

Latvijā kiberznoziegumu izmeklēšanu veic Valsts policijas Ekonomisko noziegumu apkarošanas pārvaldes (ENAP) Kibernoziegumu apkarošanas nodaļa. Latvijā darbojas arī Informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV, kas ir Latvijas Universitātes Matemātikas un informātikas institūta struktūrvienība un darbojas Latvijas Republikas Aizsardzības ministrijas pakļautībā Informācijas tehnoloģiju drošības likuma ietvaros.

Galvenie CERT.LV uzdevumi ir:

- uzturēt un aktualizēt informāciju par IT drošības apdraudējumiem;
- sniegt atbalstu valsts institūcijām IT drošības jomā;
- sniegt atbalstu IT drošības incidentu novēršanā jebkurai fiziskai vai juridiskai personai, ja incidentā iesaistīta Latvijas IP adrese vai LV domēns;
- organizēt informatīvus un izglītojošus pasākumus gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem, gan citiem interesentiem.

Kad un kam ziņot

Valsts un pašvaldības Iestādes IT drošības pārzinim jāziņo par incidentu, ja ir noticis ārējs vai iekšējs uzbrukums iestādes IT infrastruktūrai un šī uzbrukuma rezultātā notikusi svarīgu resursu atteice, kā arī apgrūtināta iestādes normāla darbība vai būtisku pakalpojumu sniegšana.

Incidenta gadījumā nekavējoties jāveic visas tā novēršanai nepieciešamās darbības (īpaši izpildot CERT.LV rekomendācijas par vēlamo sākotnējo rīcību attiecīgajā situācijā), kā arī tūlīt jāinformē par notikušo CERT.LV. Drošības incidenta gadījumā CERT.LV vienojas ar drošības incidenta pieteicēju par atbalsta sniegšanu drošības incidenta novēršanā. IT drošības pārzinim jānodrošina pierādījumu saglabāšana un jāreģistrē incidents drošības incidentu žurnālā.

Ja ir noticis noziedzīgs nodarījums vai ir pamats uzskatīts, ka kāds mēģina to izdarīt, iespējamam cietušajam būtu jāziņo ENAP Kibernoziegumu apkarošanas nodaļai.

Raksta 2.daļā pievērsīšos Latvijā izplatītākajiem kibernoziegumiem un to novēršanas iespējām.