iTIESĪBAS

Intelektuālais īpašums 07:00, 25. Mar. 2019

Kibernoziedzības uzvaras gājiens

Viktorija Jarkina, ZAB "SORAINEN", zvērināta advokāte, Dr.iur.

https://www.itiesibas.lv/raksti/komercdarbiba/intelektualais-ipasums/kibernoziedzibas-uzvaras-gajiens/14748

Ik dienu pasaulē vairāk nekā miljons cilvēku kļūst par kibernoziegumu upuriem. Kibernoziedzinieku darbības lauks ir plašs, sākot ar kredītkaršu informācijas un identitātes zādzībām un bērnu seksuālu izmantošanu un beidzot ar masveida uzbrukumiem iestādēm un infrastruktūrām.

Kibernoziedzība ir viens no ienesīgākajiem noziedzīgi iegūto ienākumu veidiem. Pasaulē katru gadu kibernoziegumu rezultātā upuri zaudē apmēram 388 mljrd. Amerikas Savienoto Valstu dolāru, kas kibernoziedzību padara "pelnošāku" (noziedzīgā kārtā iegūtas naudas apmēra ziņā) par tirdzniecību ar marihuānu, kokaīnu un heroīnu, norādīts Eiropas Komisijas paziņojumā padomei un Eiropas Parlamentam "Vēršanās pret noziedzību mūsu digitālajā laikmetā: Eiropas kibernoziedzības centra izveide" (Paziņojums).

Kibernoziegumi attīstās ļoti strauji. Kibernoziedzības izplatīšanās ātrumu veicina trīs tendences:

- arvien vairāk cilvēku ikdienā izmanto internetu;
- arvien biežāk internetu lieto dažādās ierīcēs;
- arvien biežāk ierīces izmanto, lai veiktu tādus uzdevumus kā iepirkšanās un internetbankas pakalpojumi, kas rada risku, ka tiek nodota informācija par personas datiem un naudas līdzekļiem.

Turklāt saskaņā ar statistikas datiem pasaulē kopumā atklāj ne vairāk par 10% kibernoziegumu.

Kibernozieguma definīcija

Pirmo reizi starptautisko tiesību jomā kibernoziegumu regulējums radās jau 2001.gadā Eiropas Padomes Konvencijas par kibernoziegumiem (Konvencija) ietvaros. Tomēr Konvencijā nav sniegta jēdziena "kibernoziegums" definīcija. Šāda definīcija nav atrodama arī Eiropas Savienības tiesību aktos (skat., piemēram, Eiropas Parlamenta un Padomes Direktīvu 2013/40/ES par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI). Arī Latvija nav izņēmums, un kibernozieguma definīcija nav sniegta arī mūsu tiesību aktos.

Kā norāda Starptautiskā Kriminālpolicijas organizācija jeb Interpols, pasaulē nav vienotas kibernozieguma definīcijas. Kibernoziegumi ir īpaši ātri augoša noziegumu sfēra. Strauja tehnoloģiju attīstība, jaunie datorvīrusi un paņēmieni padara neiespējamu rādīt vienotu, globālu un aktuālu kibernoziegumu definīciju.

Arī Latvijas krimināltiesību zinātnieki uzskata, ka kibernoziegumu definīcija nevar būt noslēgta, tajā jāiekļauj elementi, bez kuriem nav iespējams veikt nevienu nodarījumu elektroniskā vidē, proti, aktīva darbība, kas saistīta ar automatizētu datu apstrādes sistēmu un automatizētu datu apstrādi, kā arī tiešs vai netiešs nodoms.

Kibernoziegumu regulējums Krimināllikumā

Kā jau norādīts, Latvijas tiesību aktos, tostarp Krimināllikumā (KL), nav paredzēta kibernozieguma definīcija. Turklāt KL šāds jēdziens vispār nav lietots. Tomēr tas nenozīmē, ka Latvijā nav noteikta krimināltatbildība par kibernoziegumiem.

Kopumā KL iespējams izdalīt astoņus noziedzīga nodarījuma sastāvus, kas var būt saistīti ar automatizēto datu apstrādes sistēmu, proti, KL 144., 177.[1], 193.[1], 241.-245.pants. Jānorāda, ka kibernoziegumi Latvijā var aptvert dažādus noziedzīga nodarījuma grupas objektus, proti, noziedzīgi nodarījumi pret personas pamattiesībām un pamatbrīvībām, īpašumu, noziedzīgi nodarījumi tautsaimniecībā, kā arī noziedzīgi nodarījumi pret vispārējo drošību un sabiedrisko kārtību.

KL 144.pantā paredzēta atbildība par korespondences, pa telekomunikāciju tīkliem pārraidāmās u.c. informācijas noslēpuma pārkāpšanu (viens no piemēriem varētu būt e-pasta korespondences grozīšana, pieslēgums svešam e-pastam). Konkrētais noziedzīgais nodarījums vērsts pret personas privātas dzīves un korespondences noslēpumu, aizliedzot patvaļīgi piekļūt automatizētai datu apstrādes sistēmai.

KL 177.[1]pantā paredzēta atbildība par krāpšanu automatizētās datu apstrādes sistēmā jeb "datorkrāpšanu". Šis pants ietver personas apzinātu rīcību ar datorsistēmu. Līdz ar to datorkrāpšanas fokusā ir datorsistēma, nevis cilvēks (kā tas ir krāpšanā, par kuru krimināatbildība paredzēta KL 177.pantā).

KL 193.[1]pantā paredzēta krimināatbildība par datu, programmatūras un iekārtu iegūšanu, izgatavošanu, izplatīšanu, izmantošanu un glabāšanu nelikumīgām darbībām ar finanšu instrumentiem un maksāšanas līdzekļiem. Šim pantam atbilst, piemēram, nelikumīgi izmantots kodu kartes numurs, internetbankas lietotāja numurs, paroles, maksājuma kartes numurs u.tml.

KL 241.pantā noteikta krimināatbildība par patvaļīgu piekļūšanu automatizētai datu apstrādes sistēmai, savukārt KL 243.pantā paredzēta krimināatbildība par automatizētas datu apstrādes sistēmas darbības traucēšanu un nelikumīgu rīcību ar tajā iekļauto informāciju.

KL 244.pantā paredzēta krimināatbildība par nelikumīgām darbībām ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm. Savukārt KL 244.[1]pantā paredzēta atbildība par datu, programmatūras un iekārtu iegūšanu, izgatavošanu, izmainīšanu, glabāšanu un izplatīšanu nelikumīgām darbībām ar elektronisko sakaru tīklu iekārtām.

Kibernoziegumu veidi

Attīstoties tehnoloģijām, kibernoziegumi tiek izdarīti arvien ātrāk, globālāk un efektīvāk. Rodas jauni noziegumu veidi, no kuriem šobrīd biežāk sastopamie ir pikšķerēšana un inficēšana ar datorvīrusu.

Pikšķerēšana

Šis termins radies no vārda "makšķerēšana" (jeb angļu valodā - "*phishing*", kas, savukārt, radās no vārda "*fishing*"). Akadēmiskajā terminu datubāzē pikšķerēšana definēta kā neapdomīgu lietotāju aizvilināšana uz tīmekļa vietnēm, kas atdarina reālu organizāciju vietnes. Šādas "makšķerēšanas" nolūks ir iegūt no klientiem viņu paroles, kredītkaršu informāciju, ziņas par sociālo apdrošināšanu vai citus personas datus, kurus zaglis pēc tam varētu ļaunprātīgi izmantot.

Praksē pikšķerēšana ir krāpnieciska darbība tiešsaistē, kas ar e-pasta vai mobilā telefona starpniecību tiek vērsta pret konkrētu personu, krāpniekam uzdodoties par "leģitīmu" datu

apstrādes institūciju (banku, apdrošināšanas kompāniju, sadarbības partneri u.c.), lai tiktu atklāta personiskā informācija, ar kuras palīdzību krāpnieks varētu, piemēram:

- citas personas vārdā pieteikties un saņemt kredītu;
- iztukšot svešu bankas kontu un iztērēt kredītkaršu limitus;
- izņemt naudu no svešiem kontiem;
- izmantot debetkartes kopiju, lai izņemtu svešu naudu jebkurā pasaules valstī.[1]

Pikšķerēšanas piemēru ir daudz. Kibernoziedznieki var izveidot viltus vietni, kas izskatās identiska bankas vai kādas citas interneta maksājumu sistēmas vietnei. Pēc tam lietotājus aicina apmeklēt šo vietni un tur ievadīt savus konfidenciālos datus.

Parasti lietotājus viltotajā vietnē ievilina ar masveidā sūtītām e-pasta vēstulēm it kā no bankas vai citas reālas finanšu iestādes, šajās vēstulēs ievietojot viltotās vietnes hipersaiti. Ja lietotājs uz tās uzklikšķina, viņš nonāk krāpnieku izveidotajā interneta lapā, kur viņam pieprasa ievadīt savus datus. Bieži pikšķerēšanas vēstulēm ir tāds pats noformējums kā īstiem bankas sūtījumiem, un arī adrese hipersaitē ir līdzīga reālajai bankas interneta adresei. Turklāt bieži vien paziņojumā lietotāju uzrunā vārdā – kā to varētu sagaidīt īstā vēstulē no bankas. Vēstulē parasti ir minēts ticams iemesls, kāpēc lietotājam jāievada savi dati "bankas vietnē".

Pikšķerēšanas pētījumi apstiprina, ka cilvēki kļūst arvien neuzmanīgāki, viņu uzticēšanās pieaug, tāpēc pikšķerēšanas upuru skaits arvien palielinās. Piemēram, 2017.gadā pikšķerētāji izsūtīja krāpnieciskus e-pastus par 2018. gada FIFA Pasaules kausa izcīņu futbolā, norādot, ka e-pastu saņēmēji ir laimējuši loterijā un ieguvuši brīvbiļetes uz minēto pasākumu. Šādas ziņas izsūtītas, lai izkrāptu no cilvēkiem naudu vai personisko informāciju. Pētījumos norādīts, ka, salīdzinot 2016.gadu ar 2017.gadu, pikšķerēšanas uzbrukumu skaits ir pieaudzis. Pretpikšķerēšanas sistēma "Kaspersky Lab" lietotāju datoros tikusi aktivizēta 246 231 645 reizes, kas ir gandrīz par 59% vairāk nekā 2016. gadā.

Jāatzīmē, ka starp Eiropas Savienības dalībvalstīm ir novērojamas ievērojamas atšķirības krāpniecisku e-pastu vai telefona zvanu upuru skaita ziņā. Vairāk nekā puse no aptaujātajiem iedzīvotājiem Dānijā (66%), Nīderlandē (64%), Zviedrijā (61%), Apvienotajā Karalistē (57%) un Francijā (52%) ir piedzīvojuši šādas krāpnieciskas darbības. Savukārt tikai nedaudz vairāk par 10% respondentu ir cietuši no šāda kaitējuma Slovākijā un Horvātijā (abās 14%), un Portugālē (11%). Latvijā un Lietuvā (27%), bet Igaunijā (42%) aptaujāto kļuvuši par krāpnieciska e-pasta vai telefona zvana upuriem, interesanti, ka

Igaunijā tikai (38%) iedzīvotāji izteica bažas par iespēju kļūt par krāpnieciskās darbības upuriem, liecina Eirobarometra dati.

Datorvīrusi

Praksē dažkārt kibernoziegumi tiek īstenoti, cilvēkiem pašiem aktivizējot inficētus failus, kas saņemti e-pastā. Ar kaitnieciskās programmas palīdzību iespējams pārķert tekstu, kas ievadīts ar datora klaviatūru. Dažas kaitnieciskās programmas pat spēj iekļūt klienta datora interneta pārlūkprogrammā un tad, kad klients sāk darbu internetbankā, tiek parādīta viltota forma, kurā tiek piedāvāts ievadīt autorizācijas kodus, lai it kā apstiprinātu drošības sertifikātu.

Pazīmes, kas datorvīrusu atšķir no parastās programmas:

- tas aktivizējas bez lietotāja ziņas un veic nevēlamas darbības;
- spēj inficēt vai mainīt citas datnes;
- pavairo sevi un var izplatīties uz citām datnēm vai sistēmām.

Pastāv dažādai datorvīrusu veidi, piemēram:

- "tārpi" – tie izplata sevi citos tīklos, bet nebojā datnes;
- "trojas zirgi" – maskējās par citām datnēm un pēc to lejupielādes instalē vīrusus;
- spiegprogrammatūra – slepeni vāc datus, informāciju par lietotāju, izmantojot tā pieslēgumu internetam. Iegūtā informācija var tikt nodota ieinteresētajām personām vai organizācijām.

No kiberuzbrukumiem un datorvīrusiem nav pasargāts neviens. To pierāda 2018.gada 19.janvāra ziņa, ka Lietuvā noticis kiberuzbrukums ziņu portālam "TV3.lt", publicējot viltus ziņas par Lietuvas aizsardzības ministru un izsūtot ministrijām, vēstniecībām un citiem adresātiem vēstuli ar datorvīrusu. Tiek norādīts, ka kibernoziedzinieku IP adrese izsekota līdz Sanktpēterburgai.

Savukārt 2017.gadā visā pasaulē tika veikti masveida "ransomware"" (jeb "izspiedējvīrusa") uzbrukumi. Tā ir viena no visbīstamākajām datorprogrammu formām, kas sekundes laikā spēj ietekmēt jebkura veida operētājsistēmu un jebkuru pārlūku. Tiek apgalvo, ka vairāk nekā miljards "Windows" datoru 2017.gadā ir inficējušies ar šo vīrusu. Kibernoziedzinieks paziņo datora lietotājam: lai atgūtu piekļuvi pie datorā esošajiem datiem un failiem, jāsamaksā noteikta naudas summa.

Lielākais "izspiedējvīrusa" uzbrukumu skaits 2017.gadā notika Krievijā. Kopumā izspiedējvīruss skāra 74 valstis. Uzbrukuma skaita ziņā Latvija ieņēma 12.vietu, apsteidzot, piemēram, Brazīliju, Honkongu, Spāniju.

Viedtālruņi un planšetdatori

Interneta lietošana mūsdienās neaprobežojas tikai ar datoriem. Arvien vairāk izmantojam arī viedtālruņus – kompaktas ierīces, kas aprīkotas ar savu operētājsistēmu un programmatūru. Tas paplašina arī kibernoziedznieku darbību iespējas.

2017.gadā notika viens no līdz šim lielākajiem kiberuzbrukumiem caur viedtālruni - "Mobile banking Trojans". Šī uzbrukuma ietvaros no mobilo sakaru lietotāju bankas kontiem ar viedtālruņu banku lietotņu starpniecību tika nozagta nauda. Lietotāji paši lejupielādēja "Mobile banking Trojans", jo kibernoziedzinieki rada viltotas banku lietotnes. Informācija par šīm lietotnēm nereti tiek nosūtīta ar īsziņu palīdzību, tomēr novēroti pat gadījumi, kad šīs lietotnes bija iespējams lejupielādēt oficiālajā "Google play" veikalā.

2017.gadā valstu sarakstā ar vislielāko "Mobile banking Trojans" uzbrukumu skaitu Latvija ierindojās 7.vietā, apsteidzot Kirgizstānu, Moldovu un Kazahstānu, bet vislielākais uzbrukumu skaits bija Krievijā, Austrālijā un Turcijā.

Secinājumi

Kibernoziegumi ir 21.gadsimta pasaules mēroga problēma. Neskatoties uz to, ka kibernoziegumi ir kriminalizēti, katrai fiziskai un juridiskai personai ir jābūt uzmanīgai. Lai mazinātu uzbrukumu risku, jālieto antivīrusa programmas, jāatturas no aizdomīgu interneta vietņu apmeklēšanas un aizdomīgu e-pastu pielikumu atvēršanas, jālieto pretpikšķerēšanas sistēmas, kā arī jāveic citi piesardzības un drošības pasākumi. Būtiski ir arī ziņot par kibernoziegumiem Informācijas tehnoloģiju drošības incidentu novēršanas institūcijai (CERT.LV), kuras uzdevums ir informācijas tehnoloģiju drošības Latvijā veicināšana un ekonomisko noziegumu apkarošanas pārvalde.

[1] Aizsardzība pret pikšķerēšanas shēmām un citiem tiešsaistes krāpšanās veidiem.