NR. 6 (498) 2023. GADA JŪNIJS BILANCE

Kas katram uzņēmumam ir jāzina par kiberdrošību

Līdz ar Covid–19 vīrusa uzliesmojumu ir pieaudzis kibernoziegumu skaits — kibernoziedzība vēršas plašumā visā pasaulē un arī Latvijā. Par kibernoziedznieku upuri var kļūt jebkurš uzņēmums un ikviens indivīds. Kibernoziegumu radītie zaudējumi veido 0,8% no pasaules iekšzemes kopprodukta (IKP), skaitļos tie ir 600 miljardi ASV dolāru. Kā uzņēmumam un katram indivīdam sevi pasargāt no kiberincidentiem?

Zvērinātu advokātu biroja *Sorainen* vebinārā «APDROŠINĀŠANA PRET KIBERUZBRUKUMIEM — KAS JĀZINA UZŅĒMĒJIEM?» tika sniegts ieskats par to, kādi ir būtiskākie kiberdraudi mūsdienās un kādus aspektus ir būtiski dokumentēt, ja uzņēmums ir cietis no kiberuzbrukuma.

Ievainojams bezvadu tīkls

Possible Security Latvijā tirgū darbojas jau desmit gadus un nodarbojas ar ielaušanās testiem un auditiem — apmeklē klientus, kas pasūta šādu pakalpojumu, uzlauž viņu datorsistēmas, atrodot vājās vietas un konsultē, kas būtu jādara, lai hakeri nevarētu izdarīt tieši to pašu, vebinārā stāstīja IT drošības uzņēmuma *Possible Security* vadītājs, viens no vadošajiem kiberdrošības ekspertiem Latvijā, *Mg. sc. comp., Mg.phys.* **KIRILS SOLOVJOVS**.

Viņš arī aprakstīja trīs dažādas situācijas, kuras ir notikušas reālajā dzīvē.

Pirmā situācija: uzņēmumam pieder rūpnīca, kurā ir ievainojams bezvadu IT tīkls, tam ir konfigurācijas problēmas, kuras uzbrucēji var izmantot savā labā. Netālu no

Ilustrācija: © Andrei Hasperovich – stock.adobe.com

KIRILS SOLOVJOVS,
Mg. sc. comp., Mg.phys.
IT drošības uzņēmuma *Possible Security* vadītājs

uzņēmuma rūpnīcas tika izvietota iekārta, kas izlikās par kāda darbinieka ierīci. Uzņēmums bija parūpējies šajā tīklā par tā drošību, tāpat tika izmantota arī MAC adrešu filtrēšana[1].

Tomēr MAC adrešu filtrēšana nepalīdzēja, jo it kā kāds darbinieku visu laiku slēdzās klāt pie uzņēmuma bezvadu IT tīkla. Līdz ar to tika iegūta piekļuve rūpnīcas finanšu informācijas sistēmām un veikts ievērojams pārskaitījums — nodarītie zaudējumi bija ap 200 000 eiro.

Ko vajadzētu darīt? Viens veids, kā speciālists var palīdzēt, ir novērtēt bezvadu IT tīkla un datortīkla konfigurāciju kopumā, saprast, vai tā ir atbilstoša un vai tā tehniskā līmenī spēj mazināt ielaušanās riskus.

Ne mazāk svarīga ir atbilstošas drošības politikas izveide, lai visi iesaistītie zina, kas viņiem ir jādara, kādi ir uzņēmuma drošības mērķi. Svarīgs ir arī monitorings. Ja uzņēmumam, kuram pieder rūpnīca, būtu bijis monitorings un komersants regulāri to izmantotu, ielaušanās gadījums tiktu pamanīts, pirms par to informē finanšu direktors.

Ko darīt, ja zog datus

Otra situācija: *Possible Security* klients bija saņēmis e–pastu: nozagām jūsu datus, samaksājiet četrus bitkoinus, lai šos datus nepublicētu. Šajā gadījumā ir tikai viena pareizā atbilde: ņemot vērā, ka noziedzniekiem uzticēties nevar, maksāt neko nevajadzētu. Izrādījās, ka klients jau iepriekš bija maksājis izpirkuma maksu noziedzniekiem, cerot, ka šāda situācija neatkārtosies un tiks atrisināta. Atkārtots gadījums tikai praktiskā līmenī parāda, ka maksāt hakeriem nav nekādas jēgas.

Ko darīt šādā situācijā? Jaśķiet, ka dati jau ir nozagti, ir jāpārliecinās, ka tā tas tiešām ir noticis. Internetā ir daudz krāpniecības, tajā skaitā arī noziedznieki, kuri izliekas, ka ir uzlauzuši uzņēmuma IT sistēmu.

Šajā konkrētajā gadījumā uzņēmums pārliecinājās, ka dati ir nozagti: palūdza izspiedējiem atsūtīt daļu datu, ko viņi arī izdarīja. Datiem bija sensitīvs raksturs.

Ja dati ir nozagti, *Possible Security* vienīgā rekomendācija ir strādāt ar juristiem un sabiedriskajām attiecībām, lai attiecīgi paziņotu uzraugošajām iestādēm un ietekmētajiem klientiem, un sagatavotu sabiedrību, ka drīzumā varētu notikt šādu datu neatļauta publicēšana.

Šajā gadījumā reputācijas kaitējums un soda naudas uzņēmumam, ko nodarīja hakeri, tika novērtēts uz 700 000 eiro.

Kāds uzlauž datoru, jo nav uzlikti atjauninājumi, kāds darbinieks var uzinstalēt nepareizo IT programmu. Visbīstamākais uzņēmumam ir ļaunprātīgs darbinieks. Tas ir grūti risināms jautājums.

Datu rezerves kopijas

Trešā situācija: kāda neliela reklāmas aģentūra neveidoja datu rezerves kopijas. Tās darbinieki strādāja pie projektiem, katram bija savs dators, kur arī glabājās visa informācija. Aparatūras problēmu dēļ viens no šiem datoriem neilgi pirms projekta nodošanas sabojājās. Līdz ar to arī visi projekta faili uz šī datora nebija pieejami. Projekts bija 30 000 eiro vērts, un bija svarīgi to pabeigt laikā.

Possible Security atrisināja reklāmas aģentūrā radušos situāciju — tika piedāvāta datu atgūšana no bojātiem datu nesējiem. Nākotnei ieteikts padomāt par rezerves kopiju izgatavošanu un izstrādāt plānu dažādu katastrofu gadījumā.

K. Solovjovs uzsvēra, ka katrai svarīgai informācijas vienībai ir jābūt trijos eksemplāros: diviem no tiem jāglabājas uzņēmumā, bet vienam no tiem, piemēram, mākonī. Protams, glabājot datus mākonī, ir jāpadomā par šifrēšanu, lai dati nenoplūst un kāds tiem nepiekļūst.

Kāpēc nepietiek ar to, ka dokumenta oriģināls ir datorā un blakus diskā? Reizēm gadās lielas nelaimes, piemēram, ugunsgrēks vai zādzība, un var tikt aiznesti vai sabojāti abi — dators un disks. Tāpēc ir svarīgi, ka trešais eksemplārs glabājas kaut kur citur.

Kiberdrošība

Ko darīt, lai mazinātu iespēju saskarties ar kiberincidentiem? Kiberdrošība ir konkrētas kibertelpas daļas aizsardzības pasākums. Ar ko kibertelpa atšķiras no uzņēmuma datortīkla? Kibertelpa ir dinamiska. Ja darbinieks aiziet atvaļinājumā un paņem līdzi arī darba datoru, kibertelpa paplašinās un ir jāaizsargā visas IT sistēmas, arī tās, kas uz brīdi fiziski neatrodas uzņēmumā.

Kādiem uzbrukumiem visbiežāk ir pakļauti uzņēmumi Latvijā? Pirmais ir informācijas noplūde. Tā var notikt dažādos veidos — kāds uzlauž datoru, jo nav uzlikti atjauninājumi, kāds darbinieks var uzinstalēt nepareizo IT programmu. Visbīstamākais uzņēmumam ir ļaunprātīgs darbinieks. Tas ir grūti risināms jautājums, piebilda K. Solovjovs.

Pastāv arī ļaunatūra. Tā ir programmatūra, ko izmanto, lai apzināti noziedzīgos nolūkos inficētu datorus, viedtālruņus u. tml. ierīces, piemēram, traucējot to darbību, piekļūstot privātām datorsistēmām, bojājot tās. Kā no tā izvairīties? Ļoti svarīgi ir neapdomīgi neklikšķināt uz aizdomīgāk saitēm.

Ir arī jāizlasa paziņojumi, kas izlec datorlodziņā, pirms to apstiprināšanas.

Bieži vien datoruzbrukumi ir veiksmīgi, jo ir nedrošas paroles.

1 MAC filtrēšana ir drošības funkcija, kas bezvadu tīkla maršrutētāja vai bezvadu tīkla piekļuves punkta vajadzībām konfigurē sarakstu ar ierīču adresēm (sauktas arī par MAC adresēm), kas drīkst piekļūt tīklam, izmantojot attiecīgo maršrutētāju — red.).

Ražotāja «sētas durvis»

Var būt gadījumi, kad gan pēc pasūtījuma izstrādātās, gan gatavās datorprogrammāsražotājs ir ievietojis tādas kā sētas durvis, lai viņš vēlāk varētu piekļūt informācijai.

K. Solovjovs savā 2015. gadā pētījumā konstatēja, ka visās dārgajās, Ķīnā ražotajās kamerās, ražotājs ir iestrādājis divus speciālus veidus, kā var piekļūt kamerai jebkurā vietā pasaulē, un trīs nejaušus veidus, kā to izdarīt.

Svarīgi uzņēmumā ir arī uzbrukumi IT tīklam, kuru novēršana ir datorspeciālistu jautājums. Ja nav laba ugunsmūra vai arī nav atjauninātas tīkla servisu programmatūras versijas, uzbrucējs var uzbrukt tīkla iekārtām, neiesaistot uzņēmuma darbiniekus.

Vēl pastāv arī ļaundabīgas ierīces, kuras cilvēks var neuzmanības dēļ pievienot savam datoram. Piemēram, tās var būt iekārtas, kas izskatās kā USB atmiņas kartes vai lādēšanas iekārtas, bet īstenībā tās tādas nav. Mācība būtu: nevajag spraust svešas ierīces savās datoriekārtās, tās nav iespējams vizuāli atšķirt no labdabīgām.

IT sistēmas var sabojāt arī fiziskie apdraudējumi, piemēram, ugunsgrēks, kura gadījumā visi dati var būt pazuduši.

Nopietns apdraudējums ir, ja no biroja nozog darbinieku datorus, tie tādējādi kļūst nepieejami vai dati nonāk uzbrucēju rokās. Tad ar tiem var veikt ļaunprātīgas darbības.

Būtisks apdraudējums ir arī sociālā inženierija, kas informācijas drošības kontekstā nozīmē cilvēka psiholoģisku manipulēšanu, lai panāktu noteiktu darbību veikšanu vai konfidenciālas informācijas izpaušanu. Tas ir uzticēšanās trika veids ar mērķi savākt informāciju, apkrāpt, vai iegūt piekļuvi sistēmai.

Dažādi hakeru veidi

Pasaulē ir dažādi hakeru veidi, K. Solovjovs akcentēja trīs no tiem. Ir noziedznieki, kas savu mērķi izvēlas nejauši, tā saucamie «bērneļi» (angl. *script–kiddies*). Šie cilvēki nesaprot, ko viņi dara, bet viņiem ir hakera gēns — interese, kā uzlauzt IT sistēmas. Turklāt internetā ir brīvi pieejami dažādi kiberieroči. Līdz ar to kiberuzbrukumi var notikt ar jebkuru. Tiesa, «bērneļi» ir ļoti neizglītoti, un līdz ar to uzbrukumi ir triviāli atvairāmi.

SVARĪGĀKIE PADOMI

- Viedtālrunim ir jābūt šifrētam, ir jāizmanto drošs kods. Jāizsver iespēja izmantot papildu autorizāciju.
- Tiek izmantota biometrija — pirkstu nospiedumi, sejas vai acs attēls, kas ir publiska nenomaināma parole. To lietot paroļu vietā nav pārāk droši, taču ir vērtīgi to lietot papildu parolēm.
- Programmas *Find my iPhone/Find my Device* palīdzēs atrast, ja iekārta ir nozagta.
- Iesaka izslēgt analītiku.
- Nevērt vaļā nepazīstamus pielikumus.
- Obligāti ir jāuzstāda atjauninājumi, jo tādējādi varam gūt labumu no tā, ka ražotājs ir novērsis iepriekš atklātās drošības problēmas.
- Par jebkādiem IT incidentiem darbiniekam ir jāziņo uzņēmuma IT daļai.

Cita riska grupa ir augstas vērtības mērķi, kuriem uzbrukumi tiek organizēti speciāli. Šādos gadījumos pamatā uzbrūk uzņēmuma konkurenti, lai iegūtu biznesa informāciju. Vēl šajā sadaļā ietilpst organizētās noziedzības grupas, kas speciāli mēģina piekļūt uzņēmumam, kuram ir liels apgrozījums vai ir kādas citas intereses.

Ir valstis, kas mēģina veikt šādus uzbrukumus kādai trešajai valstij, un vietējais uzņēmums var tikt izmantots kā uzbrukuma nesējs.

Aizsardzība dziļumā

Kad uzbrucējs ierodas pēc informācijas, viņam būtu jāpārvar noteikti šķēršļi. Piemēram, uzņēmumam ir datu bāze un, lai to iegūtu, ir nepieciešams zināt paroli. Uzbrucējam tā ir jāuzlauž.

Savukārt aizsardzība dziļumā nozīmē, ka uzņēmums ir parūpējies par vairākiem aizsardzības mehānismiem. Ir jārūpējas par to, ka katrai svarīgai informācijas vienībai ir vairākas drošības kontroles. Piemēram, var aizsargāt IT sistēmu ar ugunsmūri, savukārt servera telpu — ar speciālām pieejas kartēm u.c. Uzņēmumam būtu jābūt regulējumam, iekšējiem normatīviem aktiem, kas norāda, kā rīkoties darbiniekiem, IT nodaļai. Tādējādi pat tad, ja viena kontrole nenostrādās, tiks uzlauzta vai apieta, uzbrucēju atturēs pārējās drošības kontroles.

Kiberhigiēna

Kiberhigiēna ir rutīnu kopa, kas samazina uzbrukuma piedzīvošanas risku, līdzīgi kā higiēna ikdienā mazina iespēju iedzīvoties veselības problēmās un palielina mūsu dzīves ilgumu. Pirmkārt, ir vajadzīga droša parole, ugunsmūris, kas neļauj pieslēgties caur IT tīklu un sākt uzbrukumu. Standartā no rūpnīcas gan uz *Windows* datoriem, gan uz *iPhone* telefoniem ugunsmūris ir jau iestrādāts.

«*Windows* datoriem ir uzstādīta arī antivīrusa programma *Windows Defender*. Ar to pilnīgi pietiek, ja tiek izmantoti atjauninājumi,» teica K. Solovjovs. «Tomēr pirmais aizsardzības valnis ir uzņēmuma darbinieki — lai viņi saprot, ko dara,» piebilda eksperts.

Runājot par uzglabāto datu šifrēšanu, K. Solovjovs norādīja, ka *Google*, kas ražo *Android* sistēmu, un *Apple*, kas ražo *iPhone*, šo ražotāju iekārtās tas notiek automātiski. Ja telefons ir izslēgts, dati ir nošifrēti un tos nevar atšifrēt bez koda. Protams, liels izaicinājums ir tas, ka viedtālrunis parasti ir ieslēgts.

Informācija IT sistēmās ir jāaizsargā ne tikai tad, kad to izmanto, bet jau no tās radīšanas brīža. Ir jāpatur prātā gan arhivēšana, gan iznīcināšana, gan arī informācijas saņemšana, klasificēšana, nodošana, un, protams, lietošana — arī šo darbību laikā ir svarīgi garantēt informācijas drošību — konfidencialitāti, integritāti un pieejamību.

Nozīmīga ir arī sekošana jaunumiem IT drošības jomā To var izdarīt tīmekļvietnē www.esidross.lv, arī informācijas tehnoloģiju drošības incidentu novēršanas institūcijas *Cert.lv* mājaslapā.

Kas ir jādokumentē kiberincidenta gadījumā

Ja ir noticis kiberincidents, kādi aspekti ir jādokumentē un kurām valsts iestādēm par to ir jāziņo? Kādi ir attiecīgie termiņi un informācija, kas jāiekļauj attiecīgajos ziņojumos? *ZAB Sorainen* vecākā juriste **JŪLIJA TERJUHANA** vebinārā dalījās pieredzē, kā risināt kiberincidentu no ziņošanas viedokļa. Šis aspekts attiecas uz visiem komersantiem.

«Ja uzņēmumā ir skarti personas dati, tas nozīmē, ka iestājies tas 72 stundu termiņš, kura laikā ir jāpaziņo par incidentu,» skaidroja J. Terjuhana.

Kāpēc ir svarīgi ievērot termiņu — 72 stundas un ziņot? Tāpēc, ka, gadījumā, ja uzņēmums kavējies vai vispār ignorējis paziņošanas pienākumu, Vispārīgā datu aizsardzības regula paredz sodu līdz pat 10 miljoniem eiro vai 2% no visas grupas pasaules apgrozījuma. Tas nozīmē: ja esat grupas uzņēmums, jums ir jāpārliecinās, vai un kādas jurisdikcijas ir skartas, un jāpaziņo attiecīgi tajās juridikcijās par notikušo incidentu.

Kad ir obligāti jāziņo

Kad ir jāziņo par datu noplūdi? Tas nav jādara visos gadījumos, bet tad, kad iestājas juridiska situācija, kad pastāv risks indivīda tiesībām un brīvībai. Tas nozīmē, ka ar konkrēta cilvēka personas datiem un iesaistītajām personām var notikt kaut kas negatīvs. Piemēram, var notikt identitātes zādzība, datiem noplūstot internetā, var rasties finanšu zaudējumi.

Šādi gadījumi ir arī tad, ja kredītkartes dati nonāk ļaundaru rokās, vai no bankas konta tiek pārskaitīta nauda bez personas piekrišanas. Arī, noplūstot datiem par politisko piederību, personas veselības rādītājiem vai citām sensitīvām darbībām, tāpat var rasties reputācijas apdraudējums. Šādos gadījumos noteikti būtu jāziņo Datu valsts inspekcijai, bet šis saraksts nav izsmeļošs.

Iekšējā izmeklēšana

«Visiem uzņēmumā ir jāzina, kā rīkoties. Tas nozīmē, ka darbiniekiem ir jābūt informētiem, kā izskatās incidents un ko darīt. Svarīgi, vai uzņēmumā kiberincidenta gadījumā ir iekšējā procedūra, noteikti jāziņo IT daļai un tiešajam priekšniekam. Ir jāveic izmeklēšana, jāsaglabā pierādījumi un jāveic notikušā analīze, lai saprastu, kas ir noticis un vai ir jāziņo uzraugošajai iestādei — Datu valsts inspekcijai,.» klāstīja J. Terjuhana.

Iekšējā izmeklēšanā ir jānoskaidro vairāki faktori. Tas ir vajadzīgs, lai aizpildītu paziņojuma formu un uzņēmums noskaidrotu, kas ir noticis. Informācijas apkopojumā, kuru iesniedz uzraugošai iestādei, raksta, kas ir noticis, kad, cikos un kā incidents ir attīstījies.

Piemēram, incidents ir noticis pirms trim nedēļām — ir uzlauzta

JŪLIJA TERJUHANA, Zvērinātu advokātu biroja *Sorainen* vecākā juriste

Savukārt Lietuvā uzraugošā iestāde jau ir piemērojusi sodus par kavēšanos sniegt ziņojumu; par to, ka uzņēmums nav veicis pietiekamas darbības, novēršot incidentu vai pirms incidenta iestāšanās nav piemērojis pietiekamus tehniskos risinājumus, kas atbilstu tehnoloģijas stāvoklim, prezumējot, ka tādiem būtu jābūt.

Svarīgi, lai uzņēmumā kiberincidenta gadījumā ir iekšējā procedūra, noteikti jāziņo IT daļai un tiešajam priekšniekam. Ir jāveic izmeklēšana, jāsaglabā pierādījumi un jāveic notikušā analīze, lai saprastu, kas ir noticis un vai ir jāziņo uzraugošajai iestādei.

IT sistēma, bet uzņēmums to ir pamanījis aizvakar. Pirmajās stundās ir novērsti kaut kādi trūkumi un turpinās darbs pie izmeklēšanas. Tas viss ir jānorāda ziņojumā Datu valsts inspekcijai. Ir visas iespējas tālāk uzraugošai iestādei nosūtīt papildinājumus. Piemēram, *Sorainen* nesen Datu valsts inspekcijai nosūtīja papildu informāciju par incidentu uzņēmumā, kas notika pirms gada.

Ir jāzina, cik personas incidentā ir skartas, kādi personas dati, kādas ir iestājušās vai potenciāli ir iespējamas negatīvās sekas. Ir jānorāda, kas ir darīts pirms tam, lai tas nenotiktu, kādas procedūras ir veiktas, vai ir informēti darbinieki, kas ir darīts, lai novērstu negatīvās sekas.

Lietuvā uzraugošā iestāde ir aktīvāka

Kāda situācija ir ar ziņojumu iesniegšanu par kiberincidentu ir Latvijā? «Neesam savā praksē un no publiski pieejamās informācijas uzzinājuši, ka uzraugošā iestāde — Datu valsts inspekcija — būtu strikti piemērojusi kādu sodu. Bet tā noteikti var paprasīt paskaidrojumu, ja uzņēmums kavējas ar kiberincidenta ziņojumu un, to iesniedzot, uzdot papildu jautājumus,» teica juriste.

Visbiežāk uzraugošā iestāde pieņem ziņojumu zināšanai. Taču, ja ir kādi aspekti, kas sevišķi interesē iestādi, tad var tikt uzdoti precizējoši jautājumi.

«Lietuvā uzraugošā iestāde ir daudz aktīvāka nekā Latvijā,» rezumēja J. Terjuhana. «Kad notiek incidents, nekavējoties nāk papildu jautājumi, kas precizē notikušo. Līdz ar to varam sagaidīt, ka nākotnē šādu tendenci varētu novērot arī Latvijā.»

Paziņošanas uzdevumi

Vēl juriste norādīja uz uzņēmumu pienākumu izsūtīt paziņošanas uzdevumu ne vien uzraugošai iestādei, bet arī visām skartajām personām. Gadījumos, kad iesaistīti vairāki desmiti vai tūkstoši klientu, ir jāvērtē, cik liels ir viņu tiesību apdraudējums un, ja ir skartas sevišķās datu kategorijas, piemēram, medicīnas dati, reliģiskie uzskati, tad ir jāziņo arī visiem iesaistītiem cilvēkiem.

Tas nozīmē vai nu masveida e–pastu izsūtīšanu, vai individuālu paziņojumu sagatavošanu, vai speciālas mājaslapas izveidošanu, lai detalizēti aprakstītu, kas noticis, un lai komersantu pasargātu turpmāk.

Kādas kiberincidenta gadījumā var būt sekas uzņēmumam? «Tas visbiežāk ir uzņēmuma reputācijas apdraudējums,» atbildēja J. Terjuhana. «Ja uzlauzts personas iecienītais interneta veikals vai banka, kuras klients viņš ir, indivīds var vērsties tiesā, lai piedzītu kompensāciju.»

Vebināra atziņas pierakstīja
INESE HELMANE