JURISTA PADOMS

Pamatdokumenti veiksmīgai kiberdrošības pārvaldībai

Attālināts darbs un pastiprināta informācijas tehnoloģiju izmantošana un paļaušanās uz tām ir kļuvusi par mūsu ikdienas neatņemamu sastāvdaļu, īpaši iepriekšējos mēnešos piedzīvotās ārkārtējās situācijas laikā. Līdzīgi kā rūpēm par veselības stāvokli, arī uzņēmumu kiberdrošībai, tai skaitā kiberhigiēnai, ir jābūt prioritārai, un nepieciešams tai pievērst pastiprinātu vērību. Lai nodrošinātu efektīvu kiberdrošības pārvaldi, katram uzņēmumam ir nepieciešams ieviest kiberdrošības pārvaldības sistēmas, kas atbilst tā darbības specifikai un risku līmenim.

Kiberdrošības sistēmu visbiežāk raksturo šādi pamatdokumenti:

(1) informācijas tehnoloģiju un sistēmu pārvaldes politika, kas balstīta uz drošības risku izvērtējuma,
(2) kārtība, kādā rīkoties informācijas tehnoloģiju drošības incidenta gadījumā,
(3) vadlīnijas drošam attālinātam darbam un
(4) kārtība darbinieku informēšanai un apmācībām par aktuālajām kiberdrošības un kiberhigiēnas prasībām.

Normatīvie akti pašlaik paredz pienākumu izstrādāt informācijas tehnoloģiju drošības pārvaldības dokumentus institūcijām un juridiskām personām, kuras tiek noteiktas saskaņā ar Informācijas tehnoloģiju drošības likumu (ITDL). Tomēr jebkurai organizācijai būtu jāparedz šādu dokumentu izstrāde un sistēmu ieviešana, jo to ieviešana praksē ir preventīvi pasākumi un nodrošinājums informācijas tehnoloģiju incidentu gadījumiem.

Informācijas tehnoloģiju pārvaldības politika

Veiksmīgai kiberdrošības pārvaldībai katrai organizācijai neatkarīgi no tās lieluma būtu jāapzina savi informācijas tehnoloģiju (IT) resursi un potenciālie riski tās IT drošībai. Politiku izstrādā atbildīgā persona par IT sistēmu drošību un apstiprina vadība. Politika ir visaptverošs dokuments, kura ietver IT sistēmas pārvaldības un drošības politikas mērķus un pamatnostādnes; IT sistēmas raksturojumu, analīzi un risku novērtējumu; pārvaldības organizācijas principus (t.sk. atbildīgās personas iecelšana un pienākumi, piekļuves veidi un līmeņi, personāla pienākumi un apmācības); sistēmas drošības atbilstību normatīvajiem aktiem un standartiem. Politika būtu regulāri jāpārskata un jāatjauno atbilstoši izmaiņām IT sistēmās un to pārvaldībā.

Pārvaldības politikā būtu jāparedz arī īpašas vadlīnijas attālināta darba veikšanai. Uzņēmumam ir jāizvērtē potenciālie riski, ko rada attālināts darbs. Īpaša uzmanība ir jāpievērš darbinieku drošai piekļuvei uzņēmuma sistēmām un datiem, izmantojot tikai drošu interneta pieslēgumu un VPN (virtuālo privāto tīklu), kā arī rīcību kad tiek veikts darbs ar uzņēmuma datoriem un ierīcēm, gan arī kad ir nepieciešams veikt darbu, izmantojot privātas ierīces, kas nav uzņēmuma pārziņā un kuras līdz ar to nav konfigurētas atbilstoši uzņēmuma IT drošības politikai. Svarīgi ir informēt darbiniekus gan par darba, gan personīgo iekārtu kiberhigiēnu (regulāra paroļu, operētājsistēmu un programmatūru atjaunošana, nevērt vaļā aizdomīgas vai nezināmas saites, pievērst uzmanību aizdomīgiem e–pastiem un izvairīties no dažādu multivides datņu lejupielādes).

Ilustrācija: pikisuperstar – www.freepik.com

AGNESE GERHARDE

zvērinātu advokātu biroja *Cobalt* juriste

Svarīgi ir apzināt uzņēmuma darbības veidam atbilstošos riskus un paredzēt rīcību gan IT drošības incidenta gadījumā, gan drošības nepilnības konstatēšanā.

Rīcības plāns drošības incidenta gadījumā

Līdz ar strauji pieaugušo attālināto darbu strauji ir audzis arī kiberuzbrukumu skaits. Lai kiberuzbrukums nepārsteigtu nesagatavotu un pēc iespējams novērstu iespējamo kaitējumu, papildus vispārējai IT drošības pārvaldībai ir nepieciešams izstrādāt rīcības plānu drošības incidenta gadījumā. Šāds rīcības plāns ir atkarīgs no uzņēmuma darbības veida un vai tas ir ieguvis pakalpojumu sniedzēja statusu, kuram tiek piemērotas papildu prasības ziņošanai par drošības incidentiem saskaņā ar normatīvajiem aktiem. Svarīgi ir apzināt uzņēmuma darbības veidam atbilstošos riskus un paredzēt rīcību gan IT drošības incidenta gadījumā, gan drošības nepilnības konstatēšanā.

Rīcība drošības incidenta vai nepilnības konstatēšanas gadījumā

Informācijas tehnoloģiju drošības incidents ir kaitējošs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte[1].

Savukārt informācijas tehnoloģiju drošības nepilnība ir būtiska IT sistēmas vai elektronisko sakaru tīkla izveides, uzturēšanas vai pārveidošanas gaitā tīši vai nejauši radīta sistēmiska vājība, kuras rezultātā var tikt apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte[2].

Būtiski ir paredzēt ziņošanas mehānismu atbilstoši konstatētajam drošības incidentam vai nepilnībai. Jebkurš var informēt CERT (Informācijas tehnoloģiju drošības incidentu novēršanas institūciju), bet noteiktiem komersantiem (kā skaidrots turpmāk rakstā) ir pienākums nekavējoties informēt CERT vai citu atbildīgo institūciju par drošības incidentu, kuram ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību vai digitālā pakalpojumu sniegšanu saskaņā ar normatīvajos aktos[3] noteiktajiem kritērijiem, vai arī tas ir kritiskās infrastruktūras īpašnieks vai pārvaldnieks.

Rīcība personas datu pārkāpuma gadījumā

Papildus ir nepieciešams izstrādāt vadlīnijas rīcībai, ja drošības incidents skar personas datus, kad tiek piemērota Vispārīgā datu aizsardzības regula (VDAR). Datu pārzinim ir jābūt sagatavotam šādām scenārijam, jo uz personas datu incidentu ir jāreaģē nekavējoties.

Saskaņā ar VDAR 4. panta 12. daļu personas datu aizsardzības pārkāpums ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

Darbības pēc personas datu pārkāpuma ietver:

1) pārkāpuma apstākļu konstatēšanu un seku novēršanu – pārkāpuma izvērtēšanu var veikt saskaņā ar 29. panta Datu aizsardzības darba grupas pieņemtajām pamatnostādnēm[4],
2) Datu valsts inspekcijas informēšanu (72 stundu laikā),
3) datu subjektu iespējamu informēšanu.

Būtiski ir sekot līdzi incidentu fiksēšanai un VDAR prasību ievērošanai, jo VDAR noteikumu pārkāpumu gadījumā ir iespējami sodi līdz 10 000 000 eiro vai 2% no uzņēmuma vai uzņēmuma grupas gada apgrozījuma.

1 Informācijas tehnoloģiju drošības likuma 6. panta pirmā daļa.

2 Informācijas tehnoloģiju drošības likuma 6.[1] panta pirmā daļa.

3 Kritērijus ziņošanai regulē šādi normatīvie akti: 2019. gada 15. janvāra Ministru kabineta noteikumi Nr. 15 „Noteikumi par drošības incidenta būtiskuma kritērijiem, informēšanas kārtību un ziņojuma saturu"; 2019. gada 15. janvāra Ministru kabineta noteikumi Nr. 43 „Noteikumi par nosacījumiem drošības incidenta būtiski traucējošās ietekmes noteikšanai un kārtību, kādā piešķir, pārskata un izbeidz pamatpakalpojuma sniedzēja un pamatpakalpojuma statusu"; Informācijas tehnoloģiju likuma 6. panta 2. punkts.

4 Pārkāpuma izvērtēšanu var veikt saskaņā ar 29. panta Datu aizsardzības darba grupas pieņemtajām „Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde „varētu radīt augstu risku" regulas 2016/679 izpratnē", savukārt ziņošanas pienākuma izvērtēšanu var veikt saskaņā ar 29. panta Datu aizsardzības darba grupas pieņemtajām „Pamatnostādnes par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar regulu 2016/679".

Foto no *Cobalt* arhīva

Obligātas prasības izstrādāt kiberdrošības pamatdokumentus

Lai gan visiem uzņēmumiem būtu vēlams izstrādāt un ieviest pamatdokumentus kiberdrošības pārvaldībai, ITDL un 2019. gada 15. janvāra grozījumi Ministru kabineta noteikumos Nr. 442 „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" noteic obligātas prasības izstrādāt un nodrošināt IT sistēmu atbilstību minimālajām drošības prasībām, tai skaitā ieviešot pamatdokumentus katrai sistēmai, šādām personām:
(1) valsts un pašvaldību institūcijām,
(2) informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem un
(3) pamatpakalpojumu sniedzējiem un digitālā pakalpojuma sniedzējiem.

Pamatpakalpojumu sniedzēji un digitālā pakalpojumu sniedzēji

Kopš 2018. gada oktobra Latvijā ir ieviesti divi jauni tiesību subjekti – pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji, uz kuriem tiek attiecinātas papildu IT drošības prasības, tai skaitā obligātu kiberdrošību regulējošu dokumentu sastādīšana un ieviešana. Šīs prasības izriet no Eiropas Parlamenta un Padomes 2016. gada 6. jūlija direktīvas (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (NIS direktīva), kura Latvijā tika ieviesta ar grozījumiem ITDL.

Pakalpojumu sniedzēju statusu nosaka ITDL ietvertie nosacījumi un atbilstības kritēriji. Pamatpakalpojumu statusu piešķir attiecīgās nozares atbildīgā valsts institūcija pakalpojumu sniedzējam, ja tas atbilst ITDL 3.[1] panta pirmās daļas kritērijiem[5]. ITDL 3.[1] panta pirmā daļa noteic, ka pamatpakalpojuma sniedzējs ir valsts vai pašvaldības institūcija vai juridiskā persona, kas veic saimniecisko darbību Latvijā un sniedz:
1) finanšu pakalpojumus Kredītiestāžu likuma izpratnē un finanšu tirgus infrastruktūras pakalpojumus, dzeramā ūdens piegādes vai izplatīšanas pakalpojumus, interneta plūsmas apmaiņas punkta pakalpojumus, domēnu nosaukumu sistēmas pakalpojumus, augstākā līmeņa domēna nosaukumu reģistra pakalpojumus vai pakalpojumus enerģētikas, transporta vai veselības nozarē kādā no ES dalībvalstīm;
2) pakalpojumus, kuru sniegšana ir atkarīga no informācijas tehnoloģijām;
3) pakalpojumus, uz kuru sniegšanu būtiski traucējošu ietekmi var radīt informācijas tehnoloģiju drošības incidents.

Savukārt gadījumā, ja digitālo pakalpojumu sniedzējs atbilst ITDL 3.[1] panta otrās daļas kritērijiem, tad pretēji pamatpakalpojuma sniedzēja statusa iegūšanai un prasību piemērošanai, normatīvo aktu prasības digitālo pakalpojumu sniedzējiem tiek automātiski piemērotas bez īpaša valsts pārvaldes lēmuma par statusa piešķiršanu. Tādējādi katra uzņēmuma pienākums ir izvērtēt, vai tas ir digitālā pakalpojuma sniedzējs ITDL izpratnē.

Saskaņā ar ITDL 3.[1] panta otro daļu digitālā pakalpojuma sniedzējs ir juridiskā persona, kas atbilst vienai no šādām pazīmēm:
1) veic saimniecisko darbību Latvijā un sniedz tiešsaistes tirdzniecības vietas, tiešsaistes meklētājprogrammas vai mākoņdatošanas pakalpojumu (turpmāk — digitālais pakalpojums) kādā no ES dalībvalstīm;
2) veic saimniecisko darbību ārpus ES un digitālo Latvijā sniedz ar pilnvarota pārstāvja starpniecību.

Ne visi uzņēmumi tiek automātiski uzskatīti par digitālā pakalpojuma sniedzējiem, kaut arī tie sniedz digitālos pakalpojumus. Lai juridiska persona tiktu atzīta par digitālā pakalpojuma sniedzēju ITDL izpratnē, papildus digitālā pakalpojuma sniegšanai uzņēmumam ir jābūt vairāk kā 50 nodarbinātajiem un gada apgrozījumam vai bilances kopsummai jāpārsniedz 10 miljonus eiro.

Katra uzņēmuma pienākums ir izvērtēt, vai tas ir digitālā pakalpojuma sniedzējs Informācijas tehnoloģiju drošības likuma izpratnē.

Pienākums izstrādāt informācijas tehnoloģiju drošības dokumentus

Pamatpakalpojumu sniedzējiem un digitālā pakalpojuma sniedzējiem, tāpat kā valsts un pašvaldību institūcijām un informācijas tehnoloģiju kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem, ir **pienākums izstrādāt šādus pamatdokumentus katrai sistēmai, kā arī nodrošināt tajos noteikto prasību izpildes uzraudzību un kontroli**:
(1) sistēmas drošības politika;
(2) sistēmas drošības iekšējie noteikumi;
(3) sistēmas lietošanas noteikumi;
(4) sistēmas drošības riska pārvaldības plāns;
(5) sistēmas darbības atjaunošanas plāns[6]. Prasības dokumentu saturam un pārvaldei izriet no MK noteikumiem Nr. 442[7].

Secinājums

Lai gan ne visiem komersantiem ir noteikts pienākums izstrādāt pamatdokumentus IT drošības sistēmu pārvaldībai, paaugstinātie kiberuzbrukumu riski rada nepieciešamību pēc preventīviem pasākumiem katrā uzņēmumā. Tādēļ ikviens ir aicināts izveidot kiberdrošības sistēmas un regulāri atjaunot pamatdokumentus un informēt darbiniekus par labu kiberdrošības un kiberhigiēnas pārvaldību neatkarīgi no tā, vai šādas prasības nosaka likums. BJP

5 Saskaņā ar 2019. gada 15. janvāra Ministru kabineta noteikumiem Nr. 43 „Noteikumi par nosacījumiem drošības incidenta būtiski traucējošās ietekmes noteikšanai un kārtību, kādā piešķir, pārskata un izbeidz pamatpakalpojuma sniedzēja un pamatpakalpojuma statusu".

6 MK noteikumu Nr. 442 „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8. punkts.

7 MK noteikumi Nr. 442 „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām".