Foto: Boriss Koļesnikovs

Foto: Boriss Koļesnikovs

Dr. sc. ing. **Rūta Pirta-Dreimane**
Rīgas Tehniskās universitātes docente

Prof. Dr. sc. ing. **Jānis Grabis**
Rīgas Tehniskās universitātes Informācijas tehnoloģijas institūta direktors

Informācijas drošība digitalizācijas laikmetā: izaicinājumi un risinājumi

Digitalizācija ir viena no aktuālākajām sabiedrības attīstības tendencēm. To virza ne vien organizāciju vēlme radīt jaunus produktus, pakalpojumus un palielināt to pievienoto vērtību, bet arī sociālekonomiskās, kulturālās pārmaiņas un ārējās vides ietekme. Šogad Covid-9 ietekmē digitālo transformāciju pieredzējušas nozares, kas iepriekš skeptiski vērtējušas darbu digitālajā vidē (piemēram, izglītība un kultūra). Digitalizācijas radītās pārmaiņas ietekmē informācijas drošību un īpaši kiberdrošību, radot gan jaunus draudus, gan paverot iespējas. Masveidīga pāreja uz attālinātu darbu, studijām un telemedicīnu ļaundariem pavērusi iespējas apdraudēt uzņēmumu un organizāciju datortīklus un citas informācijas tehnoloģijas. Tajā pašā laikā iedzīvotāju, studējošo un strādājoša starpā ir strauji augušas digitālās prasmes. Digitalizācijas turpmākās attīstības gaitā ir svarīgi padziļināt digitālās prasmes drošības jomā un novērst ļaundaru iespējas paralizēt attālināto pakalpojumu lietošanu.

Digitalizācija

Digitalizācija ir digitālo tehnoloģiju izmantošana jaunu pakalpojumu un pievienotās vērtības radīšanai. Tā palīdz risināt uzņēmumu un organizāciju aktuālās biznesa vajadzības, rada jaunus paņēmienus un pieejas problēmu risināšanai un lieto jaunākās digitālās tehnoloģijas. Raksturīgās digitalizācijas tendences organizācijās ir: biznesa procesu automatizācija, datu analītika, inovatīvo tehnoloģiju (mākslīgais intelekts, roboti, lietu internets u.c.) izmantošana procesos produktos, pakalpojumu, kā arī digitālo pakalpojumu ekosistēmu izveide.

Digitalizācija virza organizāciju darbības modeļu izmaiņas. Biznesa procesus arvien vairāk pilda tehnoloģijas (uzņēmumu lietotnes, fiziskie vai loģiskie roboti u.c.), lēmumu pieņemšana tiek balstīta datos, pakalpojumi tiek personalizēti atbilstoši klientu vēlmēm un fiziskajām vajadzībām. Uzņēmumiem ir jābūt elastīgiem un spējīgiem ātri piemēroties pārmaiņām (tai skaitā normatīvo aktu pārmaiņām).

Digitalizācijas turpmākās attīstības gaitā ir svarīgi padziļināt digitālās prasmes drošības jomā un novērst ļaundaru iespējas paralizēt attālināto pakalpojumu lietošanu.

Digitalizācija ietekmē ne vien organizāciju darbības modeļus, bet arī sociālekonomisko un kulturālo vidi. Mainās profesijas un lomas, normatīvā vide, kā arī organizāciju klientu, darbinieku un sadarbības partneru gaidas. Ieinteresētās puses labāk apzinās savas tiesības uz privātumu un informācijas aizsardzību. Privātums un drošības nodrošināšana tiek sagaidīta pēc noklusējuma, piemēram, integrētā privātuma aizsardzība.[1]

1 Cavoukian A. Privacy by Design: The 7 Foundational Principles, 2009. Pieejams: *https://www.ipc.on.ca/wp-content/uploads/Resources/7foundational principles.pdf*

Informācijas drošības izaicinājumi digitalizācijas kontekstā

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV informācijas drošību definē kā "informācijas un informācijas sistēmu aizsargāšanu no neautorizētas piekļuves, izmantošanas, publiskošanas, tās pieejamības traucēšanas, pārveidošanas vai iznīcināšanas".[2] Digitalizācijas kontekstā raksturīgie izaicinājumi ir saistīti ar elektroniski pieejamas informācijas integritātes, konfidencialitātes un pieejamības nodrošināšanu, ko apdraud organizāciju iekšējās un ārējās vides faktori. Tipiski organizatoriskā rakstura apdraudējumi ir organizāciju darbinieku brīvprātīga vai piespiedu atteikšanās no lojalitātes, sociālā inženierija un pikšķerēšana. Tehnoloģiskā un tehniskā rakstura apdraudējumi ir ļaunatūra, piekļuves lieguma uzbrukumi (DoS, DDoS), kā arī tīši vai netīši IT infrastruktūras vai gala iekārtu bojājumi.

Informācijas drošības pārvaldība

Informācijas aizsardzību veido pārvaldības procedūru un tehnoloģiju kopums, kas nodrošina korektas informācijas pieejamību īstajai personai īstajā laikā un īstajā vietā. Informācijas drošības nodrošināšanas vadlīnijas sniedz dažādi standarti un metodoloģijas, piemēram, ISO 27000 grupas standarti, ISF standarts, COBIT un ITIL labākās prakses apkopojumi. Standarti un metodoloģijas sniedz rekomendācijas informācijas drošības pārvaldības procesiem, drošības organizācijas izveidei, drošības dokumentācijai, kā arī konkrētu kontroļu ieviešanai organizācijās. ISO 27001 standarta rekomendācijām atbilstošie kontroļu kopumi ietver: drošības politiku un drošības organizācijas izveidi un ieviešanu, informācijas aktīvu pārvaldību, piekļuves kontroli, biznesa nepārtrauktības vadību, incidentu drošības pārvaldības ieviešanu un citus. Rekomendācijas drošības prasībām sniedz arī starptautiskas organizācijas, piemēram, Ekonomiskās sadarbības un attīstības organizācija (OECD) un Eiropas Savienības Kiberdrošības aģentūra (ENISA). OECD rekomendē ievērot vairākus principus – risku novērtējumu, drošības pārvaldību, atbildību, apzināšanos un citus.[3] ENISA uzsver riska pārvaldības kultūras nozīmību un rekomendē ieviest drošības prasības kā juridisku pienākumu.[4]

Informācijas drošības prasības nosaka vairāki normatīvie akti: Informācijas tehnoloģiju drošības likums, Fizisko personu datu apstrādes likums, Informācijas atklātības likums, Valsts informācijas sistēmu likums un Informācijas sabiedrības pakalpojumu likums. Informācijas tehnoloģiju drošības likuma mērķis ir uzlabot informācijas tehnoloģiju drošību, nosakot svarīgākās prasības, lai garantētu tādu būtisku pakalpojumu saņemšanu, kuru sniegšanai tiek izmantotas informācijas tehnoloģijas. Likumam pakārtoti vairāki Ministru kabineta noteikumi, tostarp Ministru kabineta noteikumiem Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām". Noteikumi nosaka: (1) valsts un pašvaldību institūciju informācijas un komunikācijas tehnoloģiju minimālās drošības prasības un kārtību, kādā valsts un pašvaldību institūcijas un informācijas tehnoloģiju kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji nodrošina informācijas un komunikācijas tehnoloģiju sistēmu atbilstību minimālajām prasībām; (2) valsts informācijas sistēmu vispārējās drošības prasības un (3) informācijas tehnoloģiju drošības prasības privāto tiesību juridiskajām personām, kas ir pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji.

Jauni informācijas drošības izaicinājumi

Digitalizācijas rada vairākus jaunus informācijas drošības izaicinājumus, kuru piemēri sniegti nākamajās sadaļās.

Inovatīvo tehnoloģiju radītie izaicinājumi

Inovatīvās tehnoloģijas kļūst organizācijām arvien pieejamākas. Organizācijas izmanto mākslīgā intelekta risinājumus intelektuālā darba automatizēšanai (autonomās sistēmas, inteliģentie roboti, tirdzniecības aģenti u.c.), rutīnas uzdevumiem tiek izmantoti roboti, tiek veidotas viedās ekosistēmas un izmantots lietu internets (IoT). Mērogojamības nodrošināšanai un IT resursu efektivizācijai organizācijas izvēlas mākoņdatošanas pakalpojumus. Inovatīvās tehnoloģijas tiek kombinētas, lai klientam palielinātu produktu un pakalpojumu pievienoto vērtību un paaugstinātu uzņēmumu darbības efektivitāti. Eiropas Komisija uzsver dažādu tehnoloģiju sinerģijas nozīmību, īpaši akcentējot augstas veiktspējas datošanas, mākslīgā intelekta un kiberdrošības tehnoloģiju kombinēšanu inovatīvo produktu un pakalpojumu izveidei.[5] Palielinoties inovatīvo tehnoloģiju izmantošanai organizāciju ikdienas darbā, palielinās arī saistītie informācijas drošības riski. Papildus jau zināmajiem apdraudējumiem inovatīvo tehnoloģiju izmantošana rada jaunus, vēl neizpētītus apdraudējumus.

5G ir piektā mobilo sakaru tehnoloģiju paaudze, kuras izmantošana pasaulē un Latvijā arvien palielinās. Eiropas Komisija paredz, ka 5G tīkli nākotnē būs daļa no sevišķi svarīgas infrastruktūras, kas tiks izmantota svarīgu sabiedrisko un ekonomisko funkciju uzturēšanai.[6] Līdz ar minēto nozīmīgi izstrādāt visaptverošu risku analīzē

2 CERT informācijas drošības izpratnes programma, 2012.

3 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.

4 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

5 Eiropas Savienības programmas "Digitālā Eiropa", 2018.

6 Eiropas Padome. Secinājumi par 5G nozīmi Eiropas ekonomikā un nepieciešamību mazināt ar 5G saistītos drošības riskus, 2019.

sakņotu pieeju, ko piemērot 5G drošības nodrošināšanai, sākot ar tehnoloģiju piegādātāju atlasi, turpinot ar tīkla elementu izveidi un tīklu ekspluatāciju. Savlaicīgi ir jāizstrādā pasākumi, lai kontrolētu drošības risku, kas rodas uz 5G izstrādātos risinājumos (piem., mobilā virtuālā un paplašinātā realitāte).

Mākslīgā intelekta radītās iespējas izmanto ne vien organizācijas intelektuālā darba automatizēšanai, bet arī kibernoziedzinieki jaunu uzbrukumu veidu plānošanai un izpildei. Tas tiek izmantots profilēšanā, pikšķerēšanā, tīkla analīzē un cilvēktestu (*captcha*) atšifrēšanai.[7] Uzbrukumiem tiek izmantoti kontrolēti robotu tīkli, dabiskās valodas apstrādes algoritmi un autonomās sistēmas. Industrijas eksperti rekomendē izmantot mākslīgo intelektu arī šādu uzbrukumu draudu mazināšanai ("mašīna pret mašīnu" pieeja). Mākslīgā intelekta risinājumi bieži tiek izmantoti sensitīvu datu apstrādei (piemēram, veselības dati), līdz ar to nozīmīga ir arī personas datu aizsardzība.

Mākslīgā intelekta radītās iespējas izmanto ne vien organizācijas intelektuālā darba automatizēšanai, bet arī kibernoziedzinieki jaunu uzbrukumu veidu plānošanai un izpildei. Tas tiek izmantots profilēšanā, pikšķerēšanā, tīkla analīzē un cilvēktestu atšifrēšanā.

Mākoņdatošanas pakalpojumu izmantošana faktiski nozīmē, ka informācija tiek glabāta ārpus organizācijas telpām un tās aizsardzība ir pakalpojuma sniedzēja atbildība. Līdz ar to samazinās informācijas aizsardzības caurskatāmība un pakalpojumu saņēmēji zaudē kontroli pār savu informāciju. Nozīmīgi ir formāli atrunāt pušu pienākumus un atbildību līgumos. Mākoņdatošanas risinājumu izmantošanas apjoms ar katru gadu būtiski palielinās ne vien privātajā sektorā, bet arī publiskajā pārvaldē, līdz ar to ir apzināta nepieciešamība izveidot publiskās pārvaldes datu glabāšanas politiku mākoņdatošanas risinājumos.[8]

Risku un apdraudējumu ekosistēmas

Organizācijas veido un sadarbojas digitālajās pakalpojumu ekosistēmās, kas apvieno dažādus pakalpojumu sniedzējus un piegādātājus. Organizācijas ekosistēmās pērk un pārdod pakalpojumus, integrē biznesa procesus un pakalpojumus un rada jaunu vērtību klientiem. Ekosistēmas nodrošina lietotājorientētu pieeju, personalizētus pakalpojumus, un to izmantošana vairumā gadījumu samazina katra individuālā komersanta izmaksas par digitālo pakalpojumu sniegšanu. Ekosistēmu pamatā ir vienota informācijas telpa, kas rodas, savietojot lielu apjomu organizāciju datus no dažādiem avotiem. Tipiski organizācijas dalās ar pakalpojumu, produktu, klientu un piegādātāju datiem. Vienota informācijas telpa ir pievilcīgs kiberuzbrukumu mērķis.

Organizāciju sadarbības rezultātā veidojas arī vienotas risku un apdraudējumu ekosistēmas. Salīdzinot ar "tradicionālo" pakalpojumu sniegšanu vienas organizācijas ietvaros, riski digitālajās ekosistēmās ir daudz augstāki. "Tradicionālajos" modeļos katra organizācija pārvalda savus riskus. Digitālajās ekosistēmās risku pārvaldība ir kopīgs process, organizācija nav spējīga pilnībā kontrolēt drošības aspektus, atbildība par informācijas drošības nodrošināšanu ir jāuzņemas katram sadarbības partnerim.

Ekosistēmu dalībnieki nereti ir ne vien sadarbības partneri, bet arī konkurenti. Līdz ar to jaunus riskus rada ne vien trešās puses (kiberuzbrucēji), bet arī paši ekosistēmu dalībnieki.

Risku mazināšanai organizācijām pirms sadarbības uzsākšanas ieteicams veikt padziļinātu sadarbības partneru izpēti un trešo pušu risku novērtējumu. Uzsākot sadarbību, iesaistītajām pusēm jāveido kopīgi ekosistēmu risku novērtējumi un jāievieš atbilstoši drošības pasākumi (datu apmaiņas aizsardzība, piekļuves kontroles u.c.). Tāpat kopīgi plānojama ekosistēmu darbības nepārtrauktība un atjaunošana.

Ekosistēmās aktuāli ir arī personas datu apstrādes atbilstības aspekti, ņemot vērā vienoto informācijas telpu un dalīšanos ar datiem.

Jauni informācijas aizsardzības risinājumi

Inovatīvās tehnoloģijas rada ne vien drošības draudus, bet arī paver jaunas iespējas informācijas aizsardzības jomā, piemēram, digitālās identitātes un mākslīgā intelekta izmantošana.

Inovatīvo tehnoloģiju radītie risinājumi

Kiberuzbrukumu veidi katru gadu mainās, līdz ar to ir nozīmīgi nodrošināt atbilstošu fizisko un loģisko aizsardzību. Līdz ar jauniem uzbrukumu veidiem tiek izstrādāti un attīstīti arī jauni IT drošības risinājumi.

Ņemot vērā apdraudējumu pieaugumu, viena faktora autentifikācija vairs nav pietiekama vērtīgu informācijas resursu aizsardzībai. Stingrās autentifikācijas nepieciešamību atsevišķos gadījumos, piemēram, maksājumu veikšanai internetā, nosaka arī normatīvie akti.[9] Autentifikācijas un autorizācijas infrastruktūra pēdējos gados attīstās, nodrošinot elektroniskas informācijas aizsardzību, kā arī klientorientētu pieeju – tiek izmantota biometrija, sejas

7 Zouave E., Bruce M., Colde K., Jaitner M., Rodhe I., Gustafsson T. Artificially intelligent cyberattacks, 2020.

8 Aizsardzības ministrija. Informatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022. gadam", 2019.

9 Maksājumu pakalpojumu direktīva (PSD2).

un balss atpazīšana. Inovatīvās autentificēšanās metodes ietver uzvedības biometriju, kas analizē cilvēka paradumus un uzvedību, piemēram, roku kustības, gaitu, sirds ritmu.[10]

Mākslīgais intelekts tiek izmantots ne vien jaunu uzbrukumu plānošanai, bet arī jaunu aizsardzības risinājumu radīšanai. Mākslīgā intelekta un mašīnmācīšanās tehnoloģijas tiek izmantotas draudu un ievainojamību identificēšanai, piemēram, incidentu vēsturisko datu analītikai un draudu identificēšanai, ļaunatūras identificēšanai. Mākslīgajā intelektā sakņots tīklu monitorings un analīze palīdz organizācijām ātrāk identificēt drošības notikumus un incidentus. Mākslīgais intelekts apvienojumā ar datu analītiku palīdz organizācijām identificēt aizdomīgas IT resursu lietotāju darbības. Piemēram, uzlabojot IT pārvaldības procesus un ieviešot mākslīgā intelekta risinājumus draudu atklāšanā, Rīgas Tehniskajā universitātē izdevās trīs reizes samazināt kritisko drošības incidentu skaitu.[11]

Kiberdrošība kā stratēģiska digitālā spēja

Kiberdrošība Eiropas līmenī ir nosaukta par stratēģisko digitālo spēju. Kiberdrošības jomā ir vērojams būtisks speciālistu trūkums, kas neapmierina speciālistu pieprasījumu. Līdz ar to organizācijās ir grūtības nodrošināt kiberdrošības spējas. Spēju paaugstināšanai tiek celtas kiberdrošības prasmes organizāciju darbiniekiem, kā arī tiek veidoti zināšanu apmaiņas tīkli. Speciālistu sagatavošanā un spēju paaugstināšanā nozīmīga loma ir augstākās izglītības un zinātniskās pētniecības iestādēm un to sadarbībai ar uzņēmumiem. Latvijā pieejamas kiberdrošības studiju programmas gan pamatstudiju, gan maģistrantūras līmenī Rīgas Tehniskajā universitātē, Banku augstskolā un Vidzemes Augstskolā. Zināšanu ātrākai ieviešanai praktiskās darbības vidē sevišķi nozīmīgas ir profesionālās tālākizglītības studiju programmas, kas ir pieejamas šādās jomās: 1) personas datu aizsardzība un IT drošība un 2) IT pakalpojumu un infrastruktūras pārvaldības procesu organizēšana un uzturēšana. 90 % datu drošības incidentu rada cilvēku kļūdas. Kiberdrošības nozīmīguma apzināšanās un atbilstošas zināšanas ir efektīvākais apdraudējumu novēršanas veids.[12]

Mākoņdatošanas risinājumu izmantošanas apjoms ar katru gadu būtiski palielinās ne vien privātajā sektorā, bet arī publiskajā pārvaldē, līdz ar to ir apzināta nepieciešamība izveidot publiskās pārvaldes datu glabāšanas politiku mākoņdatošanas risinājumos.

Valsts pētījumu programmas "Covid-19 seku mazināšana" ietvaros Rīgas Tehniskās universitātes vadībā ir apvienojušās piecas Latvijas augstākās izglītības iestādes, lai īstenotu pētījumu "Perspektīvās tehnoloģijas noturīgiem un drošiem servisiem", kurā tiek risinātas problēmas, kas saistības ar drošu e-studiju, telemedicīnas un attālināta darba pakalpojumu nodrošināšanu. Strauja digitalizācija šajās jomās ir radījusi drošības apdraudējumus, kas raksturīgi vāji kontrolējamai IT videi, un atsevišķajām organizācijām pietrūkst spējas apzināt un novērst šos drošības apdraudējums. Tāpēc tiek izmantoti digitālo pakalpojumu digitālie dvīņi visaptverošu strestestu veikšanai un servisu pārraudzībai, kā arī nepieciešama drošības incidentu risināšanas zināšanu apmaiņa institūciju starpā.

Pašlaik informācijas drošības nodrošināšana uzņēmumiem rada būtiskus izdevumus. Ja informācijas drošības pasākumi un digitālās prasmes kļūst par digitālo risinājumu neatņemamu sastāvdaļu, tad nākotnē šie izdevumi būtiski samazinātos. ■

10 Giorgi G. Behavioral Analysis For a Continuous User Authentication, 2019.

11 Minkevics V., Kampars J. IS Security Governance Capability Design for Higher Education Organization. In: Proceedings of 59th International Scientific Conference on Infor-mation Technology and Management Science of Riga Technical University, ITMS 2018.

12 Skat.: *https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/*