# Uzņēmumu vadītājiem skaidri jāapzinās riski, turpinot izmantot Krievijā vai Baltkrievijā ražotu un uzturētu programmatūru 2/16/24

CISA, PMP, IT konsultāciju direktore, PwC Latvija
Dr.dat. Baiba Apine

PwC 2023. gadā veiktajā aptaujā "*Global Digital Trust Insights*" vairāk nekā 70% no 3522 aptaujātajiem uzņēmējdarbības un informācijas tehnoloģiju vadītājiem apgalvoja, ka kopš 2020. gada ir veikuši būtiskus uzlabojumus kiberdrošībā. Vadītāji ir rīkojušies pareizi: pārvērtēti kiberriski, pārstrādāta drošības dokumentācija, uzlabota spēja aizsargāties pret izspiedējvīrusiem, vairota lietotāju apziņa par informācijas drošību. Tomēr gan 2022., gan 2023. kara gads ir izmainījis kibernoziegumu raksturu. 2021. gadā reti kāds sūdzējās par politiski un ideoloģiski motivētiem uzbrukumiem, taču kopš kara sākuma 2022. gadā šādu uzbrukumu īpatsvars ir kļuvis būtisks. Aktoru jeb kiberuzbrucēju, kuri savas zināšanas izmanto politisku vai ideoloģisku motīvu vadīti, aktivitāte ir nemainīgi augsta un salīdzināma ar izspiedējvīrusu un citu komerciāli motivētu uzbrucēju aktivitāti.

Uzņēmumu vadītāji Latvijā bieži padara savus uzņēmumus par aktoru vieglu mērķi, turpinot izmantot Krievijā izstrādātu un uzturētu programmatūru. Piemēram, janvāra sākumā Latvijas medijos parādījās ziņa, ka videonovērošanas kameras, kas izmanto Krievijas programmatūru TRASSIR, tiek plaši pielietotas Ukrainā un var iegādāties arī Latvijā populārās interneta iepirkšanās vietnēs. Taču šī ir tikai maza daļa. Vēl ir 1C grāmatvedība, ģeotelpiskās sistēmas un vēl, un vēl. Aizbildinājumu netrūkst – piegādātājs nav iekļauts sankciju sarakstā, nomaiņa būs dārga, kad izvēlējāmies krievu risinājumu, tas bija divreiz lētāks par Eiropas analogiem, maniem darbiniekiem vieglāk strādāt ar lietotāju saskarni krievu valodā.

Uzņēmumu vadītāji ir atbildīgi, lai uzņēmumu valdījumā esošā informācija tiktu apstrādāta atbilstoši likumiem un droši. Piemēram, neizmantot Krievijai un Baltkrievijai noteikto sankciju sarakstā iekļautu piegādātāju programmatūru, jo ar šādiem piegādātājiem nav iespējams norēķināties. Tas ir labs sākums, bet tas nav pietiekami programmatūras izmantošanas kontekstā. Piegādātāja pārreģistrēšana ārpus Krievijas vai Baltkrievijas maz ko palīdz pēc būtības, jo izstrādātāju komandas joprojām fiziski atrodas diktatūras valstīs, kur tās var tikt ietekmētas, lai izgūtu mūsu datus vai iebūvētu ļaunatūru Latvijā piegādātajā programmatūrā. Ikdienas testēšanā IT speciālisti uzņēmumos nespēj šādus "caurumus" identificēt.

Katram uzņēmuma vadītājam kā rūpīgam saimniekam ir jāidentificē visa uzņēmumā izmantotā Krievijas un Baltkrievijas programmatūra un no tās mērķtiecīgi jāatbrīvojas, negaidot konkrētā piegādātāja iekļaušanu sankciju sarakstā. Droša informācijas apstrāde primāri ir uzņēmuma vadītāja atbildība. Šā gada beigās plānots pieņemt Nacionālās kiberdrošības likumu, kur skaidri noteikts, ka uzņēmuma vadītājam jāizprot kiberriski un jāatbild par kiberdrošību. Mērķtiecīga nulles tolerance Krievijas programmatūrai uzņēmumu vadītājiem būtu jānosaka jau tagad, jo programmatūras nomaiņa ir laikietilpīga. Piemēram, Ukrainas Nacionālā banka ir noteikusi nulles toleranci Krievijas un Baltkrievijas programmatūrai. Lai gan attīrīšanās no tās sākās jau 2014. gadā pēc Krievijas iebrukuma Krimā, šāda programmatūra joprojām ir atrodama.