

Strādājot attālināti, pieaug "kiberhigiēnas" nozīme

Autors: Uldis Semeiks

Arvien straujākā viedierīču un interneta plašā pieejamība ļauj cilvēkiem strādāt 24 stundas diennaktī, kā arī piekļūt gan saviem, gan uzņēmuma datiem praktiski no jebkuras vietas.

Kā liecina tehnoloģiju kompānijas „Citrix” veiktie pētījumi, 90% darbinieku, kas strādā attālināti un paši var plānot savu laiku, ir apmierinātāki nekā cilvēki, kas strādā noteiktu laiku konkrētā vietā. Turklāt "mobilie darbinieki" mēdz retāk mainīt darbavietas, tas savukārt nozīmē, ka uzņēmumam nav jātērē resursi jaunu cilvēku meklēšanai un apmācībai.

Ja raugāties uz to no personālvadības viedokļa, darbs no mājām var būt pozitīvā ziņā motivējošs faktors darbiniekiem. Savukārt uzņēmējam tas rada papildu riskus, jo tieši biznesa vide jeb uzņēmumi ir kibernetizācijas mērķis. Ja iepriekš uzņēmuma dati tika glabāti kādā konkrētā vietā (serveri u.c.), tagad, strādājot attālināti, informācija tiek glabāta pārnēsājamās ierīcēs, kas rada lielākus datu drošības draudus.

Te vēl nozīmīgāka kļūst "kiberhigiēnas" ievērošana, sākot ar pamatlietām - antivīrusu instalēšana un regulāra atjaunināšana, drošu paroļu izveidošana, datu dublēšana, beidzot ar jau sarežģītākiem drošības procesiem - attiecīgu programmatūru ieviešana ikdienas procesos, kas ļauj gan strādāt ārpus darba vietas, gan pašam uzņēmējam nodrošina lielāku drošības garantiju.

Uzņēmumi arvien vairāk izmanto "Citrix" lietotņu virtualizāciju, kas nodrošina datora darba virsmas glabāšanu serverī, nevis fiziskajā datorā. Attiecīgi tiek realizēta centralizēta pārvaldība, kas ļauj lietotnes ātrāk atjaunot un mainīt programmatūru. Tāpat tiek nodrošināts augsts drošības līmenis - gala ierīces nozaudēšanas vai defekta gadījumā dati netiek pazaudēti. Lietotājam piekļūstot savai lietotnei, datu savienojumi tiek droši šifrēti, tāpēc nav iespējama datu noplūde, jo fiziski dati netiek pārsūtīti.

Viens no uzņēmēju mērķiem allaž bijis par zemākām izmaksām palielināt produktivitāti. Lietotņu virtualizācijas procesu ātrdarbību un veiktspēju nodrošina datu centra centralizēti serveri, nevis lietotāja gala ierīce, jo tā nodrošina tikai pieslēgumu serverim. Turklāt nav nepieciešama regulāra "uzņēmumu" datoru parka atjaunošana, jo var izmantot lētākas ierīces, kas aprīkotas ar mazu veiktspēju un jebkuru operētājsistēmu. Tāpat ir iespējams ietaupīt arī uz programmatūras licencēm.

Ļoti daudz runājam par to, ka tendences par IT rīku izmantošanu uzņēmējdarbībā uzrāda augšupejošu līkni, taču vēl aizvien manāma visai konservatīva reakcija no uzņēmēju puses. Jāsaprot, ka IT risinājumi uzņēmumam dod jaunu skatījumu biznesā - kā samazināt izdevumus, jaunus veidus, kā optimizēt savu biznesu. Tāpat tas sniedz spēcīgu augsni inovāciju radīšanā un eksportspējas veicināšanā.

Kad dzirdam vārdu "kiberrisks", visbiežāk mums nāk prātā hakeris, kas sēž pagrabā pie datora un virtuāli ielaužas datoros vai banku mājas lapās. Noteikti tas ir ļoti virspusējs skatījums.

No uzņēmējdarbības viedokļa ar kiberrisku būtu jāsaprot ne tikai ārējs apdraudējums, bet arī visi tie potenciālie riski, kas var rasties kompānijas iekšienē, proti, biznesa risku pārvaldībā ar terminu cyber apzīmē pilnīgi visus uzņēmuma procesus, kas ir jebkādā veidā saistīti ar datiem un to drošību. Uzņēmumos ir gan pašu darbinieki, kas strādā ar datu bāzēm, grāmatvedības un citām programmām, kā arī servisa uzņēmumi un ārpakalpojumu sniedzēji, kas ierodas apkopt datorus, vai arī, piemēram, kāda darbinieka bērns, kas nejauši piesēdies pie datora. Visas minētās situācijas ir potenciāls kiberrisks uzņēmumam, kas radies no iekšienes, t.i., risks nozaudēt datus nav saistīts tikai ar datorvīrusiem vai kiberuzbrukumu.

Ikdienā uzņēmumu vadītāju lielākās bažas saistās tikai ar klientu datiem un biznesa pārtraukumu - nespēju veikt pasūtījumus vai saņemt naudu. Šī nepilnīgā izpratne piemīt ne tikai Latvijas uzņēmējiem, kiberrisks ir vēl nenovērtēts lielā daļā Eiropas vidējo un mazo kompāniju.

Pēc "Marsh" kiberrisku pētījuma datiem, 79% Eiropas uzņēmumu labākajā gadījumā ir pamata izpratne par riskiem, 68% uzņēmumu nav novērtējuši iespējamus finanšu zaudējumus kiberriska gadījumā, bet 43% Eiropas kompāniju vispār nav identificējuši pat vienu iespējamo kiberriska scenāriju, kas varētu būtiski ietekmēt uzņēmuma darbību.

Latvijā vispār lielākā daļa uzņēmumu ir mazie un vidējie, kuriem ir savas nelielas klientu vai sadarbības partneru datu bāzes, un arī pie mums darbojas klasiskā atruna - mums uzņēmumā nav nekādas sensitīvas informācijas. Bet vai ir padomāts, kas notiek, ja iziet no ierindas programmas un uzņēmums nevar mēnesi veikt aprēķinus un piestādīt rēķinus? Vai arī, kāds haoss iestājas, ja pilnībā "pazūd" programma un dati ir jāievada no jauna? Nerunājot jau par tādām nozarēm kā transports un loģistika, kurās visi procesi mūsdienās darbojas kodu sistēmās.

Atšķirībā no virknes Eiropas valstu, Latvijā pagaidām nav likumdošanā iestrādātu normu, kas paredzētu konkrētu soda naudu un rīcību, kādai uzņēmumam ir jāseko datu noplūdes/zaudēšanas gadījumā. Amerikā un "vecajās" Eiropas valstīs likumdošana paredz kompānijām noteiktus soļus, kas, protams, attiecīgi saistās ar izmaksām: piemēram, uzņēmumam jānosūta katram klientam vēstule, personīgi jāsavana un jāpārlicinās, ka paroles ir nomainītas, jāveic pēcnolikuma situācijas monitorings u.tml.

Aprēķināts, ka šāds process Lielbritānijas kompānijai vidēji izmaksā ap 50 mārciņām par vienu vienību. Nav grūti aprēķināt, kādas ir kiberriska iestāšanās finansiālās sekas, ja uzņēmumam ir vairāki tūkstoši klientu. Papildus, iestājoties zaudējumiem, kas saistīti ar trešajām pusēm, kompānijai ir jāaprēķinās vēl arī ar potenciālām tiesāšanās izmaksām. Visi šie faktori veicina pieprasījumu darījuma kiberrisku apdrošināšanas, kas pašreiz ir aktualitāte tieši šajās valstīs.

Nevienam nav noslēpums, ka arī Latvijas uzņēmumi regulāri cieš zaudējumus, kas iestājušies dažādu kiberdraudu dēļ - tie ir gan datorvīrusi, gan iekšējo IT sistēmu nobrukumi, bet diemžēl pašreizējā prakse rāda, ka uzņēmumi izvēlas negadījumus noklusēt, nevis pret tiem nodrošināties un tādejādi veicināt klientu uzticamības pieaugumu.

NSA programma, kurai dots nosaukums PRISM, tika izveidota 2007.gadā un kopš tā laika ir ievērojami paplašinājusies, kļūstot par produktīvāko avotu slepenajiem izlūkošanas ziņojumiem, kas ik dienu tiek iesniegti personīgi prezidentam.

PRISM dod iespēju NSA un ASV Federālajam Izmeklēšanas birojam (FIB) sekot līdzi personas klātbūtnei globālajā tīmeklī, analizējot videomateriālus, fotogrāfijas un e-pastus.

Sabiedrībā šī programma, visticamāk, izsauks pretrunīgus vērtējumus, tomēr kāda augsta ASV administrācijas amatpersona norādīja, kā tā ir saskaņota ar Kongresu un to uzrauga Ārējās izlūkošanas uzraudzības tiesa (FISC).

"Tā ietver plašas procedūras, ko specifiski apstiprinājusi tiesa", lai nodrošinātu, ka novērošanai tiek pakļautas tikai personas ārpus Savienotajām Valstīm, norādīja anonīmais avots, piebilstot, ka tādejādi tiek līdž minimumam samazināta iespēja, ka var tikt iegūta, saglabāta un izplatīta nejauši iegūta informācija par ASV pilsoņiem un iedzīvotājiem.

Mediji vēsta, ka interneta kompānijas, kuru serveri novēroti, labprātīgi sadarbojušās, tomēr vairums uzņēmumu apgalvo, ka neko par to nav zinājuši.

Anonīmā ASV administrācijas amatpersona aizstāvēja programmu, sakot, ka tā sniedz svarīgu un vērtīgu informāciju un tiek izmantota, lai pasargātu Savienotās Valstis no daudziem un dažādiem draudiem.