Nāks jaunas nepatikšanas, vecās aizmirsīsies 1/6/25

Direktore IT konsultāciju nodaļā, PwC Latvija
Dr.dat. Baiba Apine

Aplūkojot detalizētāk 2024. gadā veiktās PwC klientu aptaujas par uzņēmumu kibernoturību (Global Digital Trust Insights Survey) rezultātus, var secināt, ka būtiskas bažas uzņēmējos raisa kiberuzbrukumu iespējamās izmaksas. Tās ietver iespējamo izpirkuma maksu izspiedējvīrusa gadījumā, sistēmu darbības atjaunošanas izmaksas un iespējamās kompensācijas klientiem par uzņēmuma nespēju piegādāt preces vai sniegt pakalpojumus kiberuzbrukuma seku likvidācijas laikā. Šādas izmaksas var izrādīties "nepaceļamas" mazajiem uzņēmumiem.

Atbilstoši CERT 2023. gada darbības ziņojumam Latvijā visaktīvākie kiberuzbrucēji ir haktīvistu grupējumi. Ziņojumā var izlasīt to pašu grupējumu nosaukumus, kuri darbojās Ukrainā kiberuzbrukumos pirms oficiālā kara sākuma. Ukrainā haktīvistu uzbrukumu veids mainījās diezgan ātri – jau 2022. gada rudenī atkal dominēja krāpnieki un zagļi, kā ziņoja Ukrainas Nacionālā banka. Šī pati tendence vērojama arī Latvijā – pie nemainīgi augsta haktīvistu uzbrukumu līmeņa izspiedējvīrusi un krāpnieki arvien biežāki ir ļaundari mūsu uzņēmumos.

Lai nenonāktu šādā neapskaužamā situācijā, katrā uzņēmumā ir nepieciešamas divējādas kontroles jeb pasākumu kopumi: pārvaldības kontroles un tehnoloģiskās kontroles.

Attiecībā uz pārvaldības kontrolēm ir būtiski, lai organizācijā būtu darbinieki, kuri katrs savā jomā atbild par kiberdrošību. Uzņēmuma vadītājs personīgi ir atbildīgs par efektīvām kiberdrošības kontrolēm, turklāt uzņēmuma vadībai jāsaprot, vai uzņēmums ir būtisko un svarīgo pakalpojumu sniedzējs vai arī atrodas būtisko un/vai svarīgo pakalpojumu sniedzēja piegādes ķēdē atbilstoši Nacionālās kiberdrošības likumam, un atbilstoši jāievieš likumā noteiktās kontroles. Pat ja uzņēmums nav šā likuma subjekts, tajā noteiktās kontroles ir nepieciešamas un mazinās iespēju kļūt par kibernoziedznieka upuri. Risku vadītājam vajadzētu nodrošināt, ka kiberrisku pārvaldība nav atsevišķi no kopējās uzņēmuma risku pārvaldības, proti, kiberriski un to mazināšanas kontroles ir vienā sarakstā ar ģeopolitiskajiem un ekonomiskajiem riskiem. Finanšu direktoram jābūt pilnīgai skaidrībai par kiberdrošībai nepieciešamajām investīcijām, to apmēru un potenciālajiem zaudējumiem, t.i., cik nāktos maksāt, ja piemeklētu izspiedējvīruss, vai uzņēmumam nepieciešama kiberrisku apdrošināšana. Savukārt, jurista uzdevums ir nodrošināt, ka uzņēmums saprot kiberdrošības likumvidi un realizē pasākumus, lai nodrošinātu atbilstību tai. Tāpat juristam būtu laikus jāapgūst kiberincidenta rezultāta dokumentēšana apdrošināšanas un policijas vajadzībām. Uzņēmuma informācijas tehnoloģiju (IT) vadītājs ir atbildīgs par efektīvām tehniskajām kontrolēm IT infrastruktūrā un sistēmās (piekļuves tiesību kontroles, programmatūras testēšana pirms uzstādīšanas, tīkla datu plūsmas uzraudzība u.c.). Savukārt iekšējam auditoram jāpārliecinās, vai visas šīs kontroles darbojas un vai uzņēmums ir labi pasargāts no incidentiem.

Mazā uzņēmumā var nebūt visu iepriekšminēto darbinieku. Tādā gadījumā šie uzdevumi jāpilda uzņēmuma vadībai, ja nepieciešams, konsultējoties ar ārpakalpojumu sniedzēju. Piemēram, vismaz vienreiz būtu nepieciešama kiberdrošības pārbaude, ko veiktu ārpakalpojuma sniedzējs. Ideāli, ja tādas pārbaudes veiktu reizi gadā.

Šodienas kiberriski ir ar lielāku varbūtību un dārgākām sekām nekā iepriekš – jāatjauno darbība, iespējams, jāmaksā izspiedējam, jāmaksā sodi klientiem par preču un pakalpojumu līgumu neizpildi. Atskatoties uz analogām kiberdrošības aptaujām, piemēram, 2018. gadā, būtisks risks bija sods par fizisko personu datu aizsardzības pārkāpumu.

Lai gan fizisko personu datu aizsardzības regulējums un spiediens uz nosacījumu ievērošanu nav mazinājies, sodi saglabājušies un pat tiek piemēroti, bažu īpatsvars uzņēmēju vidū ir mazinājies salīdzinājumā ar krāpšanu un zādzībām kibertelpā.