Vai Latvijā tagad ir kiberkarš un kas būtu jādara? 1/30/24

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

Dr.dat. Baiba Apine, CISA, PMP, PwC Latvija IT konsultāciju direktore
Foto: Gatis Dieziņš, Latvijas Republikas Aizsardzības ministrija

Plašsaziņas līdzekļos aktīvi izmanto jēdzienu "kiberkarš". Šā gada festivālā "Lampa" piedalījos Aizsardzības ministrijas organizētā diskusijā "Vai esam gatavi kiberkaram?". Šobrīd nespējam novilkt skaidru līniju starp kiberkaru, kur jāreaģē militāri vai kuru jāuzskata par uzbrukumu Krimināllikuma ietvarā. Latvijā šobrīd dzīvojam kiberkarā, un uzņēmumiem jārēķinās, ka rūpīgi jāseko līdzi savai kiberdrošībai.

Savā 2023. gada pārskatā CERT atzīst, ka kopš 2022. gada Krievijas pilna mēroga iebrukuma Ukrainā DDoS uzbrukumus Latvijai, Eiropas Savienības un NATO alianses valstīm visbiežāk organizē ar Krieviju saistīti grupējumi – haktīvisti. To darbības, iespējams, tiek koordinētas un finansētas Krievijas iekšpolitisko un ārpolitisko ietekmes operāciju mērķu realizēšanai. Uzbrukumi – veiksmīgi vai neveiksmīgi – tiek plaši reklamēti kā lieli panākumi, jo internets pacieš jebko.

Ikdienā uzņēmumi nespēj nošķirt, vai kiberuzbrucējs ir militārs haktīvists vai parasts krāpnieks, un jebkurš uzbrukums būtu jāvērtē kā kriminmāls noziegums.

No 2019. gada līdz 2023. gada pavasarim Ukrainā vadīju Oschadbank padomi. Tā ir valsts banka, otra lielākā Ukrainā, universāla banka, kas apkalpo gan uzņēmumus, gan privātpersonas visos kanālos. Bankai karš sākās 15. februārī ar neaptveramas, nebijušas jaudas kiberuzbrukumiem. Zinājām, ka pasaules plānotā reakcija būs sankcijas, un aicinājām tās uzsākt. Neveiksmīgi, jo kiberkarš nav redzams. Tas domāts haosa radīšanai, lai atvieglotu karadarbību "uz zemes". Haktīvistu uzbrukumu veids mainījās diezgan ātri: jau 2022. gada rudenī dominējošie atkal bija krāpnieki un zagļi, kā ziņoja regulators. Karadarbībai "uz zemes" ievelkoties, finansēt augstu kiberkara jaudu ir grūti.

Uzņēmumiem Latvijā jābūt gataviem nepārtraukti strādāt kiberkara apstākļos. Manā ieskatā minimālais

darbību saraksts ir vienkāršs:

1. centralizēta uzņēmumu informācijas sistēmu arhitektūra, kur datus glabā centralizēti;
2. datiem un programmatūrai ir rezerves kopijas. Uzņēmuma informācijas tehnoloģiju speciālisti ir pamēģinājuši atjaunot sistēmas no rezerves kopijām;
3. uzņēmumā jābūt skaidri nodefinētam kritiskajam personālam darbam krīzes situācijā, un šiem cilvēkiem jāzina, ka tieši viņi iesaistīti nepārtrauktā darbībā;
4. jāatbrīvojas no Krievijā un Baltkrievijā izstrādātas un uzturētas grāmatvedības, ģeotelpiskās informācijas apstrādes programmatūras u.c.

PwC informācijas tehnoloģiju speciālisti labprāt izskatīs jūsu uzņēmuma IT infrastruktūru un pārvaldību ar mērķi identificēt riskus nepārtrauktai darbībai un izstrādās precīzu rīcības plānu risku mazināšanai, nodrošinot, ka investīcijas kiberdrošībā ir optimālas.