Ettevõtte IT turvalisus e-äri tähtsuse tõusu ajal – kõigi, aga eelkõige juhi asi

6 aastat tagasi - 15.04.2020 Autor: Joosep Truu

Kaubandus ja äritegevus kolivad praegu üha enam Internetti. Meie maailm on iga päevaga digitaalsem, mobiilsem, kliendikesksem, pilvepõhisem. Seoses käimasoleva eriolukorraga kasutatakse e-teenuseid nii töötamiseks, õppimiseks, ostude tegemiseks kui vaba aja veetmiseks veelgi enam. Selles pole midagi ohtlikku, kui me ei unusta ära, et arvuti- ja sidevõrgud on sama haavatavad, nagu on inimeste immuunsus-süsteemid. Neis toimuvad tuhanded muutused sekundis loovad häkkeritele võimalusi pääseda võrkudesse, seadmetesse ja süsteemidesse

Tehnoloogiate kiire areng muudab ettevõtete IT halduse aina keerulisemaks ja üha enam laiali pillutatuks. Kui jätta IT turvalisus vaid IT osakonna asjaks, saab tugevaks vaid üks nurgakividest – tehnoloogia. Kuid sellest ei piisa.

Puudulik küberhügieen mõjutab kõiki

Tehnoloogiaga saab maandada paljusid riske, kuid protsessid, iga töötaja teadlikkus ja küberhügieen pole vähem olulised. On rõõmustav, et juhtide teadlikkus võimalikest ohtudest on viimastel aastatel suurenenud. Kuid unustada ei tohi ka personali.

Täna registreeritakse iga paari minuti tagant mõni veebileht, mis on seotud COVID-19 petuskeemiga, mis kasutab ära inimeste paanikat. Samuti on registreeritud tuhandeid domeene, mille nimes sisaldub näiteks konverentskõnede tarkvara Zoom nimi. Eks ikka selleks, et populaarse tööriista pahaaimamatute kasutajate ja ettevõtete andmetele ligi pääseda.

Kui töötajad ei ole ohtudest teadlikud, avatakse teadmatusest manuseid, klikitakse seal, kus pole vaja ning loovutatakse oma sisselogimisandmeid. Väiksemas ettevõttes on intsidendile lihtsam kiiresti ja paindlikult reageerida. Mida suurem on ettevõte, seda kriitilisem on tõsta infuturbe alast üldist teadlikkust ja oskusi, sest piisab vaid ühest nõrgast lülist.

Näiteks kui ettevõtte meilikontode hulgas on vaid üks eriti nõrga parooliga kasutaja, võib sellest piisata, et saada serverisse sisse, seal juba edasi toimetada ning ka ülejäänud ettevõtte IT-taristu juurde edasi liikuda. Kontoandmete

kaitsmine on täna olulisem kui kunagi varem. Aga oma käed peab ikka igaüks ise ära pesema.

Ka isikliku mobiiltelefoni kaudu võib ettevõtte andmed ohtu seada

Ettevõtte kaitsmiseks ei piisa enam ainult tulemüürist jms tehnoloogiast. Mobiilsusega on paradigma muutunud ja uus perimeeter küberrünnaku kaitsmisel on just konto.

Me kasutame oma mobiiltelefonides üha enam äppe. Kuigi Apple ja Google kaitsevad oma operatsioonisüsteeme hästi, on kolmandate osapoolte rakenduste turvamine endiselt suur väljakutse. Küberkurjategijad kasutavad turvaauke rakendustes seadmetele kaugjuurdepääsuks. Mida rohkem nutitelefoni tööks kasutatakse, seda enam laienevad riskid ka ettevõtte rakendustele, andmebaasidele ja andmetele. Esmalt tõmmatakse üle töökontaktid ja telefoninumbrid, siis juba eemaldatakse andmeid, installitakse pahavara, pommitakse lunavara.

IT turvalisus ei too raha sisse

Tõsi, IT turvalisus maksab raha ja ei too midagi sisse. Küll aga viib välja, kui pihta saadakse. Alles tõsine intsident paneb ettevõtjate väärtusi ümber hindama. Sageli ei piisa isegi sellest, sest alati ei väljendu kahju otseselt või kohe rahas. Visalt, kuid vaikselt siiski, on näha suhtumise muutust, sest 2019 pakkus rikkalikult näiteid neist, kellele tegemata töö läks kalliks maksma. Riigi Infosüsteemide Ameti andmetel tuleb 10 000- või 20 000-eurose kahjusummaga juhtumeid ette keskmiselt korra nädalas. Samuti kaotavad ettevõtted kliente ja käivet nendel päevadel, kui nad parasjagu lunavaraintsidentide tõttu oma andmeid taastavad.

IT turvalisus hakkab juhtidest

Enamasti on turvalisuse ja andmelekke intsidendid seotud juhtkonna, mitte IT-poiste tegemata tööga. Kui juhtkond ei ole enda äriga seotud küberohtudega kursis ning ei pea seda teemat ka väga kriitiliseks, siis peegeldub see ka küberkaitsetehnoloogiate valikus ning kogu personali ohutunnetuses.

Jah, ettevõtetel on praegu kriisijuhtimisega tegemist. Paraku on nii, et praegune olukord majanduses, kodukontorites töötamine ning ebakindlus inimeste isiklikus elus on ideaalne pinnas küberkuritegevuse laialdasele levikule. Ettevõtjad, palun koolitage oma juhte ja töötajaid ja andke neile ajakohane teave

küberturvalisusest!

Joosep Truu
Müügijuht ja koolitaja, Iteraction OÜ

- Tegijad
- Lahendused

- Turvalisus

Pilt