Küberkuritegevusest sai epideemia: 2020. aasta levinuimad petuskeemid

5 aastat tagasi - 02.12.2020 Autor: Joosep Truu

2020. aasta statistika saab olema huvitav. Üht me juba teame - oluliselt suurenenud on nii interneti kasutamine kui küberturvalisuse juhtumid. Kindlasti mängib selles suurt rolli COVID-19 pandeemia, kuid lootust, et koos koroonavaktsiiniga kahanevad ka küberohud, paraku pole.

Sel aastal nägime selgelt, et küberkurjategijad oskavad ära kasutada haavatavaid teemasid, olukordi ja sihtrühmi. Viirustõrjet pakkuva ettevõtte Bitdefender hinnangul tõusid maailmas veebruarist märtsini 2020 haiglate vastu suunatud pahatahtlikud rünnakud 475%.

Alles eile kuulsime rünnakutest Eesti riigi IT-taristu vastu, mille tagajärjel varastati terviseametilt 9158 koroonaviiruse diagnoosi saanud inimese andmed.

Laias laastus muutuvad rünnakud aina kavalamaks ja keerulisemaks ning küberkurjategijate sihtrühmad aina laiemaks. Kaitstud pole keegi. Üha keerukamates skeemides kombineeritakse pahavara, andmepüüki, masinõpet, tehisintellekti, krüptoraha ja muud.

Ettevõtete ja asutuste arv, kes intsidentidest teatavad, suureneb, aga tegelikku numbrit me ikka ei tea. Väikeste ja keskmise suurusega ettevõtete juhid eeldavad sageli, et küberkurjategijad jälitavad ainult suuri korporatsioone. Tegelikkuses on aga 43-50% kõigist küberrünnakutest suunatud just väike- ja keskmise suurusega ettevõtete suunas. Neist on saamas eelistatud sihtmärk nimelt seetõttu, et puudub ikka veel teadlikkus ümbritsevatest ohtudest või keeldutakse neid ohte tõsiselt võtma.

Positiivne on see, et ohtudest räägitakse ja konkreetseid hoiatusi jagatakse sotsiaalmeedia kaudu ühe enam. Oma igapäevatööst, meediast ja Riigi Infosüsteemide infokanalitest jäid 2020. aastast enim meelde need levinumad petuskeemid:

Õngitsemine ja kontode kaaperdamised

Suvel kirjutati meedias, et kurjategijatel oli õnnestunud saada ligipääs Eesti ühe spordialaliidu meilikontole, millel toimuvat kirjavahetust mõnda aega jälgiti. Meilivestlusesse sekkuti hetkel, kui tekkis koroonapandeemia tõttu vajadus võistluste osalustasud tagasi maksta. Kelmid palusid pangakontot muuta ja maailma vastav spordiliit saatis kurjategijatele u 4000 euro ulatuses tagasimakseid.

Sarnaseid õnnestunud juhtumeid on kümneid.

> Õppetund: Kui äri e-maili turvaseadistused ning kaheastmeline autentimine on tegemata, on osaval küberkurjategijal võimalus teie ettevõtte alt pettusi teha.

Lunavaraviirused

Häkkerid rakendavad tehnoloogiaid, mis võimaldavad neil sõna otseses mõttes röövida inimese või organisatsiooni andmebaase ja hoida kogu teavet krüptituna kuni lunaraha ära makstakse. Peamiselt levib lunavara viirus e-maili ja veebisaitide teel ja võtab serveris ja arvutis olevad failid n-ö pantvangi. Krüptoviirus proovib pääseda ligi ka kõigile teistele arvutitele ja serveritele, mis on samas domeenis. Andmete lahti krüptimise eest küsitakse lunaraha.

Paralleelselt lunavara rünnakuga võib toimuda andmevargus, millele järgneb väljapressimine.

> Õppetund: ära kliki kahtlastel manustel ja linkidel.

Oktoober 2020: Emoteti ründelaine

Emotet rünnaku ohver saab e-kirja, mis sisaldab PDF-i või Office'i dokumenti, mille avamine käivitas pahavara allalaadimise. Süsteemi pääsedes laeb pahavara ohvri masinasse juba tõsisemat kahju tekitavat lunavara või spioonvara, mis võib varastada arvutis olevat teavet, e-kirju, kontaktiloendeid, paroole, makseteavet ja muid andmeid. Oma olemuselt on Emotet ukseavaja, mis saadab varastatud teabe, sageli e-kirjade sisu, käsuserverisse.

Pahavara võltsib vastuseks juba olemasolevale kirjavahetusele uue e-kirja, mis muudab selle järgmise saaja jaoks usaldusväärseks, kuna ka kirja pealkiri ja sisu on kopeeritud tõelistest sõnumitest.

Võltsõnum sisaldab jälle pahatahtlikku manust. Emoteti tagajärgi on alates märkamatust andmelekkest, kliendilepingute rikkumisest kuni firma arvutisüsteemide täieliku halvamiseni.

> Õppetund: Ära usalda manuseid ka siis, kui need on näiliselt kolleegilt või äripartnerilt.

Pankadega seotud skeemid

Juulis hoiatasid suurimad pangad laialdase petukõnede laviini eest, mis kõlab nagu pangast tehtud kõne, mille eesmärgiks on saada ligipääs inimese pangakontole. “Petturid helistavad näiliselt panga telefoninumbrilt ja väidavad, et tegemist on pangatöötajaga. Kõnes küsitakse pangakaardi numbrit või internetipanga kasutajatunnust, isikukoodi ja palutakse Smart-ID rakendusse sisestada oma kood,” kirjeldas SEB sotsiaalmeedias. Swedbanki klientidele helistati samuti näiliselt panga numbrilt, teavitati pangakaardi kurvitarvitamisest, küsiti kliendi kaardinumbrit ja CVC-koodi.

> Õppetunnid:
>
> - Pettused võivad toimuda igat kanalit pidi.
> - Kurjategijad kasutavad ära tuntud ettevõtete usaldusväärsust.
> - Paradoksaalselt võib ka tõusev teadlikkus küberohtudest olla veeks kurjategijatele veskile.

2020. aasta topelt-löögid

Pandeemiaga seoses on jõudsalt kasvanud pilvelahenduste, digitaalsete müügiplatvormide jm tööriistade kasutamine. Kaugtöö on samuti paljude ettevõtete ja asutuste jaoks pigem uus. See aga loob täiendavaid rünnakupindu, mis suurendab veelgi vajadust turvaliste IT-lahenduste järele.

Nagu viirused, millel on sageli palju tüvesid ja mis pidevalt muunduvad, ei piisa ka küberviiruste takistamisel vaid ühest meetmest, et end nakatumise vastu vaktsineerida.

Enda kaitsmiseks on vaja nii inimest kui tehnoloogiat. Ühekordsetest aktsioonidest ettevõtetes ei piisa. Tegevused inimeste koolitamiseks ja süsteemide testimiseks peaksid toimuma pidevalt.

Turvalisus kui konkurentsieelis?

Praegu viivad küberturvalisuse auditeid ja koolitusi läbi vaid mõni protsent ettevõtteid, kuid see peaks muutuma iga-aastaseks, isegi igakuiseks tegevuseks. Ettevõtja aga ei peaks jääma ootama seadust, mis selle kohtustuslikuks muudab, vaid võtma seda endastmõistetava rutiinina.

Küberturvalisust ei tasuks vaadata ainult kuluna, vaid ka konkurentsi-eelisena. Mujal arvestatakse ettevõtte väärtuse hindamisel ühe tegurina üha enam ka seda, kui hästi ta oma andmeid hoiab, milline on küberturvalisuse olukord ja strateegia.

Lõpetuseks paar soovitust, mis kehtivad nii ettevõtetele kui eraisikutele.

Küberkuritegevus ei piirdu ammu enam vaid e-posti kasutavate petistega, kes lubavad meile saata Nigeeria surnud printsi käest 20 miljonit dollarit. Kuid ligikaudu 90% ründeid jõuavad inimeseni ikka veel läbi e-posti, kuid nad on Nigeeria printsi petuskeemidest palju edasi arenenud! Esimese asjana tuleks peamine ohuvektor maksimaalselt maandada.

Samuti tasub meeles pidada, et küberkurjategijad ei puhka.

Kindlasti mitte pühade ajal!

Joosep Truu on Iteraction OÜ juht ja koolitaja

- Tegijad
- Lahendused

- Turvalisus

Pilt

