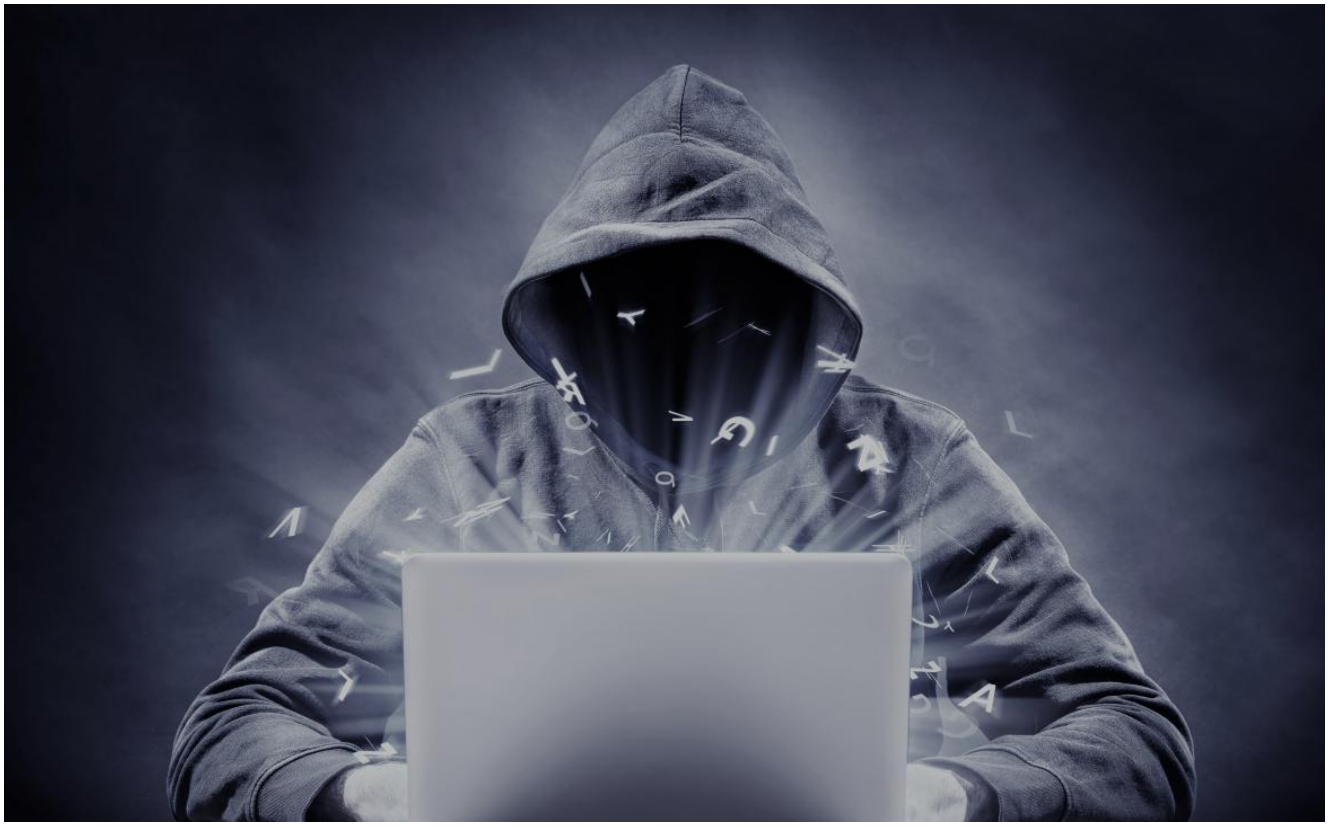
7 näpunäidet ettevõtjale küberturvalisuse tagamiseks

Küberrünnakuid võib nende eesmärgi alusel jaotada aktiivseteks ja passiivseteks. Aktiivsete rünnakute eesmärgiks ongi just konkreetselt sinu ründamine. Passiivsete rünnakute puhul heidavad pahatahtlike kavatsustega isikud laia võrgu ning loodavad tõenäosusele, et keegi jääb ikka sinna kinni.



Kas on olemas mingid meetmed, mis aitaksid küberintsidentide korral vähendada tekkivat kahju ning võiks päästa ka passiivse rünnaku võrgust? Juhul, kui tegemist on aktiivse rünnakuga, on väga tõenäoline, et mingi turvaauk ikka leitakse, kustkaudu siseneda. Kui oled siiski 100% veendunud, et sinu ettevõtte küberturvalisuse süsteem on läbistamatu, siis on selle testimiseks kasulik tellida pen-test (ehk simuleeritud rünnak sinu ettevõtte vastu). Järgnevalt toome välja mõned meetmed, millest võiks küberintsidendi poolt põhjustatud kahju ulatuse piiramisel kasu olla ning mis võivad päästa passiivse rünnaku võrgust.

Hoolsusmeetmed

1. **Personaalse küberhügieeni rakendamine**

Personaalse küberhügieeni all mõeldakse enamasti inimeste rutiinset käitumist oma seadmetes ning internetis. Sarnaselt käte pesemisele viiruste vastu võitlemisel, on korraliku küberhügieeni abil võimalik oma arvutisüsteemide nakatumist vältida (või vähemalt vähendada nakatumise tõenäosust).

Personaalse küberhügieeni hulka kuulub näiteks:

· tugeva parooli kasutamine – sealjuures ei ole hea idee kasutada sama parooli mitme konto jaoks. Eriti tuleks vältida sama parooli kasutamist töö- ja eraelus.

· kaheastmeline autentimine (2FA) – isegi, kui sinu parool ära arvatakse, ei pääse pahatahtlike kavatsustega isikud sinu informatsioonile ligi.

· oskus tunda ära õngitsuskirju – tüüpilisemad õngitsuskirja tunnused on näiteks kui kirja saatja nimi ja meiliaadress ei klapi omavahel; e-kirja tekstis olevad hüperlingid viivad võõrale veebilehele (seda saab kontrollida ilma lingile klikkimata, hoides kursorit lingi kohal); või lugematud kirjavead e-kirjas, mille peaks olema saatnud justkui ametlik ettevõte.

· tarkvara korrapärane uuendamine – uuenduste pidev edasilükkamine tähendab, et ka sinu seadmete turvasüsteemid ei ole uuendatud. Vanemate versioonide kasutamine tähendab, et häkkeritel on olnud rohkem aega kasutatavas süsteemiversioonis turvaaukude leidmiseks.

Ettevõtte küberhügieeni hulka kuulub ka töötajate koolitamine, et töötajad suudaksid potentsiaalseid ohumärke ära tunda ning ei muutuks kogemata nö „nõrgaks lüliks", mille kaudu on pahatahtlikel isikutel võimalik ettevõtte sisesüsteemidesse tungida.

Muidugi on ettevõtte küberhügieen parem, kui töötajad ei kasutagi oma töist meiliaadressi eraelulisteks toiminguteks nagu Amazoni või Netflixi kontole logimine. Sellisel juhul tekitab väidetavalt Amazonist saabunud kiri töömeilile kohe kahtlust ning reeglina ei asuta seal erinevatele hüperlinkidele klikkima – inimesed ei lase reeglina kutsumata külalist oma koduuksest sisse.

2. **Ettevõtte ja selle turvariskide tundmine**

Ettevõtte juhina on oluline teada, millised on sinu ettevõtte turvariskid ning milline informatsioon võib pahatahtlikele isikutele atraktiivne tunduda.

Andmete atraktiivsuse puhul tasub näiteks analüüsida, millised andmed võivad tekitada ettevõttele kõige rohkem kahju. Sellisteks andmeteks võivad olla näiteks tööstussektori ärisaladused, meditsiiniettevõtte kogutud patsientide terviseandmed või klientide finantsandmed. Isegi kui küberrünnaku eesmärk ei ole nende andmete varastamine, võib ka teatud andmetele ligipääsu piiramine ettevõttele kahju tuua.

Lisaks väärtuslike andmete tuvastamisele on oluline ka nende kaitsmine. Turvariskide puhul tasub näiteks analüüsida, kas ettevõtte sisevõrgus olevale informatsioonile pääsevad ligi kõik või on kehtestatud juurdepääsupiirangud. Hetkel levinuima küberintsidendi liigi – lunaraharünnaku – potentsiaalset kahju aitab vähendada oma andmete varundamine. Rohkem infot küberriskide analüüsimise kohta on võimalik lugeda ka SIIT.

Ideaalmaailmas on kõigil töötajatel kõige modernsemad ning nõuetekohaselt uuendatud turvasüsteemid, kust ei pääse läbi ükski pahalane, ning kogu ettevõtte informatsioon on võrdselt ja täiuslikult kaitstud. Kuid piiratud ressurssidega reaalses maailmas on oluline prioritiseerimine. Seega tulekski ettevõtte juhtidel tunda oma ettevõtte-spetsiifilisi riske ning esmajärjekorras tegeleda suurema kahjupotentsiaaliga ohtudega.

3. **Regulaarne kontroll**

Kas sinu ettevõtte küberturvalisuse jälgimine toimub regulaarselt või alles siis, kui kahju avalikuks tuleb? Isegi kui ettevõttel ei ole mõistlik palgata küberturvalisusega tegelema eraldi spetsialisti, aitab proaktiivne lähenemine kahju tõenäosust ning ulatust oluliselt vähendada. Suuremate ettevõtete puhul võib siiski olla vajalik reaalajas toimuva kontrolli võimekusega programmidesse investeerimine. See võimaldab reeglina toimunud rünnet kiiremini tuvastada ning võib tänu sellele tekkiva kahju ulatust vähendada.

Oma ettevõtte küberturvalisusele tuleks ideaalis tähelepanu pöörata juba teenust arendades ning ettevõtte kulutustesse juba aegsasti ka küberkulutusi planeerida. Regulaarne riskide hindamine ning vajaliku tarkvara ning tegevusplaanide uuendamine aitab paremini rakendada ka eelnevalt mainitud hoolsusmeetmeid.

Küberintsident siiski toimus – mida teha?

4. **Teavita CERT-i**

CERT-EE abistab Eestis asutusi küberintsidentide asjus ning pakub tehnilist tuge intsidentide lahendamisel. Samuti koordineerib CERT samaaegselt toimuvate intsidentide puhul neile reageerimist. CERT-i kohta saad rohkem lugeda SIIT.

Kui küberintsidendi tulemusena lekkisid mh isikuandmed, võib lisaks CERTi teavitamisele olla vajalik ka Andmekaitse Inspektsiooni teavitamine.

5. **Dokumenteeri maksimaalselt**

Küberintsidentidega seonduvaid andmeid võib hiljem vaja minna – näiteks millal intsident toimus, milline oli selle iseloom, kuidas süsteemidesse sisse pääseti. Isegi kui selle info abil küberintsidendi korraldajat ei leita, võib see aidata samaliigilisi rünnakuid vältida. Samuti on see info abiks ettevõtte turvasüsteemi tugevdamisel.

6. **Hinda võimalikku õiguslikku vastutust**

Kui küberintsidendi tagajärjel koguti sinu andmebaasidest konfidentsiaalset infot või isikuandmeid, võib tagajärjeks olla ka tsiviilõiguslik vastutus koostööpartnerite, klientide või töötajate ees. See ei tähenda automaatselt kohtusse mineku vajadust, kuid õiguseksperte kaasamine juba intsidendist teadasaamise hetkel aitab efektiivsemalt edasisi tegevusi planeerida ning võimaliku kahju ulatust hinnata. Olukorra õiguslik analüüs aitab teha kindlaks ka seda, kas hoopis sinul võib olla nõue mõne oma teenusepakkuja või koostööpartneri vastu.

Kindlasti ei ole hea lahendus probleemi eiramine ilma seda analüüsimata, sest ettevõttel võib tulenevalt omavahel sõlmitud lepingust või Euroopa Liidu isikuandmete kaitse üldmäärusest (GDPR) olla kohustus toimunud küberintsidendist oma koostööpartnereid või kliente teavitada.

7. **Mine tagasi hoolsusmeetmete rakendamise juurde**

Küberintsident näitas, kus sinu ettevõtte turvasüsteemides on auk. See on võimalus turvasüsteemid paremaks teha ning hoolsusmeetmeid täiendada.

(Autor: Gerda Grauberg)

LIISI JÜRGEN
VANDEADVOKAAT, PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE