2026. aasta viis küberohtu, millega peab arvestama iga ettevõte

3 kuud tagasi - 19.01.2026 Autor: AM

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) juhib koos oma liikmetega tähelepanu viiele küberohule, mis mõjutavad 2026. aastal üha enam ettevõtete juhtide vastutust, et äriliselt jätkusuutlik olla. Küberturvalisus puudutab kõiki sektoreid ning eeldab teadlikke otsuseid juhatuse ja nõukogu tasandil.

„Küberohud on tihedalt seotud tehnoloogia kiire arenguga. Tehnoloogia ise ei ole halb – vastupidi, see loob majandusele ja ühiskonnale uusi võimalusi. Paraku kasutavad samu tööriistu üha oskuslikumalt ka kurjategijad. Seetõttu ei piisa enam üksnes tehnilisest kaitsest, vaid määravaks saab juhtkonna otsustusvõime, rollijaotus ja valmisolek kriisiolukorras tegutseda," selgitab ITLi juhatuse liige ja CybExer Technologies OÜ Nõukogu esimees Lauri Almann, „küberintsidentide puhul ei piisa üksnes tehnilisest reageerimisest. Olulised on otsused, mida tehakse info puudulikkuse tingimustes: kas ja kuidas suhelda klientide ja avalikkusega, millal intsident raporteerida, milline on juhatuse vastutus ning kuidas tagada oma äri jaoks kriitiliselt oluliste andmete säilimine."

Almann rõhutab, et ITLi liikmed ei ole pelgalt tehnoloogiate arendajad ja teenusepakkujad, vaid ka Eesti digiruumi toimimise ja turvalisuse haldajad, see tähendab vastutust nii enda organisatsioonide, klientide kui ka laiemalt ühiskonna ees.

Küberohtude määratlemiseks kogunesid ITLi liikmesettevõtete juhid koos valdkonna ekspertidega, kelle hulgas olid Kalev Pihl (SK ID Solutions), Toomas Vaks (Swedbank), Andre Visse (Telia Eesti), Vahur Verte (Riigiprokuratuur) ja Veikko Raasuke (CERT-EE). Arutelu keskendus realistlikele stsenaariumitele ning juhtide praktilistele otsustele, misjärel leiti olulisimad probleemid, millest ükski ettevõtte juht mööda vaadata ei tohiks.

Eksperdina arutelus telekomide esindajana osalenud ITLi juhatuse liige ja Telia Eesti AS tegevjuht Andre Visse selgitab, et küberruumi toimimine ei ole ammu enam pelgalt IT meeste mure ega tehniline probleem – see on osa majandusest, kriitilisest taristust ja igapäevaelust, „küberturvalisuse eest ei saa vastutada ainult IT-juht või infoturbe spetsialist. Soovitan ettevõtetel käsitleda küberturvalisust pideva juhtimisprotsessina, mitte ühekordse projektina. Vajalik

on luua ja regulaarselt harjutada kriisiplaane, investeerida andmete varundamisse ja turvalisse autentimisse, tõsta töötajate teadlikkust ja oskusi ning teha koostööd usaldusväärsete tehnoloogiapartneritega," selgitas Visse.

IT-ettevõtete juhid stsenaariumide läbimängul. Foto: Priit Jõesaar

ITLi hinnangul TOP 5 küberohtu 2026. aastal

AI ründetööriistana ja AI-põhised õngitsusründed

Tehisintellekt võimaldab ründajatel luua väga usutavaid, sihitud petusõnumeid ja -kõnesid. Ennustuste kohaselt kasutatakse 2027. aastaks tehisintellekti ligi 17% küberrünnakutest. Samal ajal on AI ka oluline kaitsevahend – küsimus on, kumb pool suudab kiiremini kohaneda.

Õngitsemine ja petukõned

Pettused on jätkuvalt üks suurima mõjuga küberkuritegevuse vorme. Eestlased kaotasid mullu kelmidele ligi 29 miljonit eurot, millest suurima osa moodustasid pangapettused ja ärikirjapettused. Ohuks ei ole mitte ainult rahaline kahju, vaid ka maine ja usaldus.

Andme- ja identiteedilekked

Andmete hulk ja väärtus kasvavad kiiresti. Ainuüksi Eestis on viimastel aastatel lekkinud miljoneid paroole. Andmelekked võivad tekkida nõrkade paroolide,

õngitsuste või tarneahela rünnete kaudu ning mõjutada otseselt ettevõtte tegevusvõimet ja vastutust klientide ees.

Tarneahela ründed
Ründajad otsivad teadlikult nõrgimat lüli. Üha sagedamini saadakse ligipääs ettevõtte süsteemidele just partnerite või teenusepakkujate kaudu. Tarneahela turvalisus on seetõttu juhatuse tasandi risk, teadlik koostööpartnerite valik muutub järjest olulisemaks.

Lunavara
Lunavararünnakud on jätkuvalt ühed enim levinud ja kulukamad küberintsidendid Euroopas. Need on muutunud ärimudeliks, kus rünnakuid pakutakse teenusena ning kahju võib ulatuda ettevõtte tegevuse seiskumiseni.

- Tegijad
- Uudised

- Lahendused
- Turvalisus

Pilt