



Teenusetõkestusrünnete oht Eesti riigiasutustele ja ettevõtetele püsib

Olukord

Alates 2022. aasta algusest on mitmekordistunud teenusetõkestusrünnete arv Eesti ettevõtete ja asutuste vastu. Käesolev aasta näitab trendi jätkumist ja ründeid viiakse läbi lainetena, nende maht on kohati suur. Viimane suurem laine algas 23. jaanuaril finants- ja kindlustussektori vastu ning selle järelmid veel kestavad.

Sihtmärkideks on aasta vältel olnud riigiasutuste veebilehed, pangad, transpordiettevõtted, telekommunikatsiooniettevõtted, meediaportaalid, mõnedel juhtudel ka energiaettevõtted ning kindlustusettevõtted. Rünnete kasv on seotud Vene sõjategevusega Ukrainas ning nende taga on enamasti erinevad häktivistide rühmitused, kes väljendavad oma meelsust, rünnates endi jaoks ebasõbralikke riike.

Samalaadsetest ründelainetest on teada andnud ka teised riigid. Mõnikord on neil avaldunud kõrvalmõju Eesti ettevõtetele – näiteks kui ettevõtte peakontor asub parajasti ründe all olevas riigis või on osa teenuseid majutatud ettevõtte teiste riikide harukontorites.

Senine kogemus nii Eestis kui teistes riikides näitab, et ründed hoogustuvad sageli konkreetsete poliitiliste sündmuste või otsuste ajendil. Nii näiteks võivad eelseisvad Riigikogu valimised kaasa tuua järjekordse laine.

Rünnete iseloomustus ja mõju

Suurem osa viimase aasta jooksul aset leidnud teenusetõkestusrünnetest on rakenduskihi ründed, mis tähendab, et rünnatakse otse veebilehti. Lihtsalt selgitatuna pannakse veebilehe suunas teele miljoneid päringuid ja loodetakse sellega leht üle koormata. Päringute tegemiseks kasutatakse nii üle võetud robotvõrgustikke kui ka muid seadmeid, samuti kompromiteeritud veebilehti.

Need ründed on enamasti olnud mõjuta või väga lühiajalise mõjuga - ettevõtete või asutuste veebilehtede ja teenuste kasutajate jaoks toimib kõik tavapäraselt. Seda põhjusel, et rünnatud ettevõtted on osanud seda ohtu ette näha ning rakendanud tehnilised kaitsemeetmed. Riigivõrgus olevate asutustele rakendub riigi poolt keskselt pakutav DDoS kaitse ning vastavalt ohupildile on CERT-EE riigi jaoks olulistel veebilehtedel aidanud üles seada ka täiendavad kaitsekihid.

Viimaste lainete tähelepanekud

Viimaste ründelainete puhul on siiski märgata, et ründajad püüavad seniste rünnete ebaedust järeldusi teha ning ründeviise mitmekesistada. Näiteks on proovitud rünnata veebilehte majutavaid servereid või veebilehe teatud funktsionaalsusi. Katsetatakse ka ründemahtude varieerimisega.

¹ 1 KüTS'i paragrahv 12: (3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.



Vältimaks levinud kaitsemeetet, mis seisneb teistest riikidest tuleneva liikluse piiramises (lubatakse ligipääs vaid Eestist), on viimasel ajal hakatud rünneteks kasutama ka Eesti VPN-ühendusi.

Selliste rünnetega toimetulek eeldab mitmekihilist kaitset ning veebilehete või teenuste haldajatelt täpset käsitsi administreerimist, mistõttu on olnud juhtumeid, kus teenused või veebilehed on olnud mõne tunni vältel kättesaamatud või toimunud tavapärasest aeglasemalt.

Ehkki paljud sihtmärgid korduvad lainest lainesse, satub nende hulka aeg-ajalt ka juhuslikke sihtmärke (näiteks kui veebilehe või teenuse nimi viitab elutähtsale või olulisele valdkonnale).

RIA soovitused teenuste ja veebilehete omanikele²:

1. Ole valmis, et ka sinu teenus või veebileht võib osutada teenusetõkestusründe sihtmärgiks. Hinda, kuidas võimalik rünne mõjutaks sinu äritegevust ja millised oleks optimaalsed kaitsemeetmed.
2. Uuri oma internetiteenusepakkujalt ja veebimajutajalt, millised kaitsemeetmed on nende poolt keskselt rakendatud ning mida nad ründe korral saavad täiendavalt teha.
3. Tunne oma veebilehe või teenuse funktsionaalsust – kas ja millele on otstarbekas lasta ligipääsu piirata, kui satud ründe alla. Ole teadlik, et riigipõhistest piirangutest ei pruugi abi olla.
4. CERT-EE tehniliste meetmete juhendi teenusetõkestusrünnete ennetamiseks ja lahendamiseks leiad [siit](#).

Kui soovid olla kursis Eesti küberruumis toimuvaga, jälgi RIA [kuukokkuvõtteid](#) ja [kvartaliülevaateid](#).

Ohuhinnangu koostas RIA analüüsi- ja ennetusosakond koostöös CERT-EE-ga.

² Antud soovituste fookuses ei ole elutähtsate ja riigi jaoks kriitiliste teenuste pakkujad, kes on CERT-EE kõrgendatud tähelepanu all ja saanud spetsiifilisemaid juhiseid.