



Lunavararünded toimuvad jätkuvalt kaugtöölaua protokoll (RDP) kaudu

Taust

Kuigi möödunud aastal registreeris CERT-EE vähem Eesti ettevõtete, asutuste ja eraisikute vastu sooritatud lunavararündeid, kui varasematel aastatel, ei ole need siiski ära kadunud. Usume, et tegelik rünnakute arv on suurem, kui meid teavitatakse. Aastate jooksul oleme ikka ja jälle siinsamas Eestis näinud, et tihti toimuvad lunavararünded läbi RDP (*remote desktop protocol*) ehk kaugtöölaua rakenduse, mis on internetis avalikult kättesaadav. Teine levinud variant on vananenud või uuendamata tarkvaraga võrguseadmed. Need võivad olla seadmed, mis on juba jõudnud kasutusea lõppu ja millele ei pakuta enam turvauuendusi, või lihtsalt uuendamata tarkvaraga võrguseadmed.

2025. aasta esimese kolme kuuga oleme registreerinud juba neli lunavararünnakut, mis suure tõenäosusega toimusid kõik just RDP vahendusel. RDP-ühendused on jätkuvalt populaarsed ründevektorid. Üksiküritajad ja rühmitused kaardistavad ööpäevaringselt küberruumi, et leida sealt avatud RDP-ühendusi ja üritavad nende kaudu tungida ohvri süsteemidesse. Samamoodi skaneeritakse ka turvanõrkuste tõttu olemasolevaid seadmeid.

Sel aastal toimunud lunavararünnete täpsemad asjaolud on veel selgitamisel, kuid ühe juhtumi puhul nägime, et kasutati internetis avalikult kättesaadavat kaugtöölaua ühendust ja nõrka parooli.

Soovitused RDP-ühenduse turvamiseks ja lunavararünde ennetamiseks

Kasuta VPNi ehk virtuaalset privaatsvõrku. VPN annab lisakaitse, kuna selle taha pandud RDP pordid pole avalikult leitavad. Lisaks saab VPN-lahendusele lisada kaheastmelise autentimise, mis suurendab turvalisust veelgi. Vajadusel ja võimalusel võib kaaluda ka Zero Trust lahenduste (ZTNA) rakendamist.

Luba ühendus vaid kindlatelt IP-aadressidelt. RDP-ühenduse võimalust ei tohiks kindlasti pakkuda kõikidele, teisisõnu tervele maailmale, vaid ainult nendele IP-aadressidele, mida kasutavad töötajad või koostööpartnerid, kellele on vaja tagada ligipääs.

Kasuta kaheastmelist autentimist. Tavapärasest paroolist ja kasutajanimest tõhusama kaitse annab mitmeastmeline autentimine, mida on võimalik rakendada ka RDP-ühenduse puhul.

Kasuta unikaalseid turvalisi paroole. Ründajad kasutavad RDP kaudu ohvri arvutisse tungimiseks kas lekkinud paroole või jõurünnet. Vahel katsetatakse ka enamlevinud paroole, mis on internetis lihtsalt leitavad, näiteks: password, 123456, qwerty.



Kasuta pikki ja tugevaid parooli ning väldi nende korduvkasutust. Salasõnade loomiseks ja salvestamiseks on abiks paroolihaldur. Samuti tasub jälgida, et kasutajanimeks pole mõni üldlevinud nimi: user, admin, administrator vmt.

Piira ebaõnnestunud autentimiskatsete hulka. Kui seadistad teenusesse ligipääsemise nii, et näiteks 15 minuti jooksul saab pakkuda kolme parooli (juhul, kui autentimine toimub parooliga), muudad sellega jõurünnaku läbiviimise väga keeruliseks ja aeganõudvaks, kuid see ei päästa olukorras, kus parool on lekkinud.

Uuenda regulaarselt tarkvara. Veendu, et seadmete tarkvara on uuendatud. Kui seadmele enam ei pakuta turvauuendusi, siis tuleks see välja vahetada mõne uuema vastu. Ründajad kasutavad tihti just turvapaikamata tarkvara süsteemidesse ligipääsu saamiseks. Soovitame paigaldada turvauuendused esimesel võimalusel ja jälgida RIA [blogi](#), kus avaldame igal nädalal infot olulisemate turvanõrkuste kohta.

Näiteks tuli 2024. aasta oktoobris avalikuks turvanõrkus (CVE-2024-43533), mis võimaldab RDP vahendusel koodi kaugkäivitust.

Seadista ja jälgi logisid. Suuna RDP-logid kas eraldisesvasse logimislahendusse, teise Windowsi serverisse, SIEMi või muusse taolisse lahendusse. See aitab tagada, et eduka ründe korral logid säilivad ja neid saab hiljem analüüsida.

Seadista monitooring ja teavitused. Anomaaliatega korral peaks monitooring saatma välja teavitused ja hoiatused, millele saaks kiirelt reageerida. Näiteks, kui kasutaja logib sisse piirkonnast, kus ta seda tavapäraselt ei tee, võiks monitooring juhtida sellele tähelepanu. Samuti tuleks jälgida õnnestunud ja ebaõnnestunud logimisi – see aitab rünnet ära hoida või seda kiirelt tuvastada.

Tee regulaarselt varukoopiaid ja testi neist taastatavust. Juhul, kui arvuti nakatub lunavaraga ning failid krüpteeritakse, on võimalik kahju ära hoida regulaarse varukoopia tegemisega. Varukoopia tegemisel on oluline veenduda, et varukoopia pole nakatunud arvutiga ühenduses selliselt, et ka varukoopia oleks võimalik ära krüpteerida. Hoida varukoopiat näiteks välisel kõvakettal, mis ei ole arvutiga ühendatud. Võimalusel testi regulaarselt varukoopiate taastatavust – varukoopia, millest ei ole võimalik midagi taastada, on kasutu.

Koolita töötajaid küberohtude teemadel. Koolitused võiksid hõlmata nii teoreetilist kui ka praktilist osa. Võimalusel võiksid organisatsioonid enda vastu teha ka reaalse rünnete simulatsioone – see tähendab, et näiteks korraldatakse juhatuse nõusolekul ja teadmisel ettevõttele simuleeritud õngitsuskampaania. Õngitsuse tulemusi tuleks töötajatele esitleda koos praktiliste soovitusetega ja rääkida, kuidas end selliste kampaaniatega eest kaitsta. Lisaks on RIA loonud Kübertesti, mis on e-õppe koolituskeskkond. Selle eesmärgiks on tõsta ja hoida asutuse või ettevõtte töötajate küberturbeteadlikkust. Rohkem infot Kübertesti ja sellega liitumise kohta leiad RIA [kodulehelt](#). Häid soovitusi ja juhendeid leiad ka [IT-vaatliku](#) lehelt.

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