RIIGI INFOSÜSTEEMI AMET

OHUHINNANG [1] märts 2022

Enamus lunavararünnakuid sooritatakse kaugtöölaua protokolli (RDP) kaudu

Taust

2021. aastal registreeris CERT-EE 30 Eesti ettevõtete, asutuste ja eraisikute vastu sooritatud lunavararünnakut (rünnakute tegelik arv on kindlasti suurem). Kõigi ründevektorit pole võimalik tuvastada, kuid vähemalt 17 juhul tungis ründaja ohvri süsteemidesse kaugtöölahenduste RDP või TeamViewer kaudu. 2022. aasta jaanuaris registreerisime kuu keskmisest rohkem ehk viis lunavararünnakut, mis kõik toimusid RDP vahendusel.

RDP-ühendused on populaarsed ründevektorid. Üksiküritajad ja rühmitused kaardistavad ööpäevaringselt küberruumi, et leida sealt avatud RDP-ühendusi ja üritavad nende kaudu tungida ohvri süsteemidesse.

Ühe hiljutise intsidendi puhul avas administraator standardpordil ajutise RDP-ühenduse õhtul kell kaheksa, järgmiseks hommikuks olid andmed serveris lunavara poolt krüpteeritud. Teise värske rünnaku puhul avati kaugtööle suundunud töötaja jaoks RDP port 3390. Tema arvuti krüpteeriti mõned päevad hiljem.

Soovitused RDP-ühenduse turvamiseks

Kasuta VPNi ehk virtuaalset privaatvõrku. VPN annab lisakaitse, kuna selle taha pandud RD-pordid pole avalikult leitavad. Lisaks saab VPN-lahendusele lisada kaheastmelise autentimise, mis suurendab turvalisust veelgi.

Luba ühendus vaid kindlatelt IP-aadressidelt. RDP-ühendus ei tohiks olla avatud tervele maailmale, vaid ainult nendele IP-aadressidele, mida kasutavad töötajad või koostööpartnerid, kellele on vaja tagada ligipääs. Kui see lahendus pole rakendatav, tuleks kaaluda regioonipiirangut, mis võimaldab juurdepääsu, näiteks, ainult Eesti IP-aadressidelt. Ehkki selline piirang pole rünnaku vältimiseks piisav, hoiab see eemale suure hulga juhuslikest katsetustest.

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

Piira ebaõnnestunud autentimiskatsete hulka. Kui seadistad tarkvara nii, et näiteks 15 minuti jooksul saab pakkuda kolme parooli, muudad sellega jõurünnaku läbiviimise väga keeruliseks ja aeganõudvaks, kuid see ei päästa olukorras, kus parool on lekkinud.

[1] 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.

Uuenda tarkvara. Veendu, et seadmete tarkvara on uuendatud. 2019. aasta märtsis avalikkuse ette jõudnud BlueKeep haavatavus (CVE-2019-070) võimaldab RDP vahendusel koodi kaugkäivitust. Ehkki turvauuenduse avaldamisest on möödas kolm aastat, on internetti endiselt ühendatud arvuteid, millele pole seda paigaldatud.

Kasuta turvalisi paroole ja uuenda neid regulaarselt. Ründajad kasutavat RDP kaudu ohvri arvutisse tungimiseks kas lekkinud paroole või jõurünnet. Kasuta pikki ja keerulisi paroole ning väldi nende korduvkasutust. Salasõnade loomiseks, salvestamiseks ja uuendamisel on abiks paroolihaldur. Samuti tasub jälgida, et kasutajanimeks pole mõni üldlevinud nimi: user, admin, aministrator vmt.

Seadista ja jälgi logisid. Suuna RDP-logid kas teise Windowsi serverisse, SIEMi või muu logimislahenduse kasutamise korral sellesse. See tagab, et eduka ründe korral logid säilivad ja neid saab hiljem analüüsida.

Seadista monitooring ja teavitused. Anomaaliate korral peaks monitooring saatma välja teavitused ja hoiatused, millele saaks kiirelt reageerida. Näiteks kui kasutaja logib välja 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.

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