RIIGI INFOSÜSTEEMI AMET

OHUHINNANG[1] 25 jaanuar 2022

Ukraina vastased küberründed ja võimalik mõju Eestis

13. jaanuaril tabas Ukraina valitsuse veebilehti ulatuslik küberrünnak. Eri allikate kohaselt näotustati kuni kaheksakümmend valitsusasutuse veebilehte, nende seas välisministeeriumi, haridus- ja teadusministeeriumi, julgeoleku- ja kaitseministeeriumi ning valitsuskabineti veebid, aga ka nt vaktsineerimissertifikaate säilitava portaali avaleht.

Näotustamise kõrval toimub ka teine tõsisem operatsioon: 15. jaanuaril avaldas Microsofti küberohte ja –ründeid analüüsiv üksus, et on leidnud juhtumis tõendeid andmeid kustutava pahavara kohta. Pahavara, mida tuntakse *WhisperGate* nime all, käitub pealtnäha nagu lunavara, kuid sellel puudub andmete taastamise mehhanism – seega erinevalt lunavarast on eesmärk andmete kustutamine ning seadmete kasutuskõlbmatuks muutmine. Kõnealust pahavara on Microsofti teatel leitud nii Ukraina valitsusasutuste, MTÜ-de kui ka IT-asutuste võrkudest.

Mille kaudu ründed toime pandi

Uurimine käib, kuid senistel andmetel:

1. Kompromiteeriti Ukraina IT-ettevõte Kitsoft, mis pakub teenust paljudele Ukraina valitsusasutustele. Kitsofti esindaja on kinnitanud, et on leidnud oma võrkudes Microsofti viidatud andmeid hävitavat pahavara. Kuna rünnati teenusepakkuja kaudu, on ohus kõik Kitsofti kliendid (ka koostööpartnerid teistes riikides, juhul kui Kitsoftil neid on).
2. Kasutati ära paikamata turvanõrkust CVE-2021-32648 veebilehtede sisuhaldussüsteemis CMS October. (Selle turvanõrkuse paik on olemas ja avaldati augustis 2021). On ka viiteid, et kasutati ära ka VMWare turvanõrkust CVE-2021-22045.
3. Kasutati ära Log4Shell logimisfunktsiooni turvanõrkusi. Log4Shell turvanõrkus avaldub üle maailma miljonites seadmetes ja rakendustes, sealhulgas ka Eestis. Loe lähemalt RIA blogist.
4. Kasutati ära juba mitu kuud varem saadud ligipääsusid süsteemidesse (lekkinud paroolid jm).

Mõju Eestis

Sama käekirjaga ründeid praegu Eestis näha ei ole olnud.

Samas soovitab RIA olla valvas oma infosüsteemide turvalisuse osas, eriti kui ettevõttes või asutuses on kasutusel Ukraina päritolu või Ukrainas laialt kasutusel olevad tarkvaratooted või on muu IT-alane seos Ukrainaga.

[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.

Nii 2017. aasta NotPetya rünnak, mis tehti raamatupidamistarkvara MeDOC uuenduste kaudu, kui ka praegune rünnak, milleks kasutati IT-teenuse pakkujat Kitsofti, on oma olemuselt tarneahelaründed. Sihtmärgist sõltumata võib tarneahelarünnetel olla kõrvalmõju ka teistele riikidele, sealhulgas Eestile.

Soovitused asutuste ja ettevõtete infoturbejuhtidele

Ukraina-põhiste sõltuvuste olemasolul:

1. Soovitame isoleerida Ukraina poolega suhtlevad süsteemid teistest võrkudest selliselt, et liiklus oleks vaid ühesuunaline ning välise osapoolega suhtlevad süsteemid ei saaks luua ühendusi sisevõrkudega.
2. Sama kehtib Ukrainaga seotud tarkvaralahendusi kasutavate teenuste ja serverite puhul.

Üldised soovitused:

1. Kaugtööks tuleb kasutada mitmikautentimist *(Multifactor Authentication ehk MFA)* võimaldavaid VPN lahendusi, kõik muud kaugtööteenused nagu RDP, WINRM, SSH jms ei tohi olla avalikult kätte saadavad.

2. Teostada inventuur kaugtööks kasutatavate teenuste kasutajakontode üle, sealhulgas partnerite ligipääsud, ning kasutajakontode õiguste üle. Veenduda, et sisemistele teenustele on ainult vajalikud ligipääsud.

3. Välistele partneritele (tööjaamadele / arvutitele / muudele seadmetele), kellel on ligipääsud kaugtöö lahendustele, peavad olema kehtestatud sellised turvanõuded, mis vastavad organisatsiooni enda turvapoliitikale.

4. Teostada oluliste võrkude ja teenuste isoleerimine, sh avalikud teenused, nt veebiserverid. Lubada ainult vajalikud sisenevad ning väljuvad ühendused IP-aadressi ja pordi põhiselt. Sama põhimõtet tuleb kasutada ka sisevõrkude suunalise liikluse puhul.

   NB! Kui sisenevate ühenduste puhul on antud meede üldjuhul hästi rakendatud, siis teenuse haavatavuse korral on eriti oluline, et ründajal ei oleks võimalik haavatavuse ära kasutamiseks luua väljuvaid ühendusi, mille kaudu alla laadida pahavara ja muid tööriistu ründe jätkamiseks.

5. Uuendada tarkvara viimasele ametlikule versioonile. See soovitus kehtib nii avalike teenuste kui ka lõppkasutajate tarkvara puhul ning puudutab ka neid tarkvarasid, mis on kasutusel süsteemides, mis ei ole otseselt internetist kätte saadavad. Veenduda, et tarkvara või teenus ei ole haavatav Log4Shell detsembris avaldatud turvanõrkuste kaudu.

6. Jälgida logisid mistahes anomaaliate suhtes, eriti kaugtöö lahenduste ning teenusserverite väljuvaid ühendusi.

7. Hoiatada kasutajaid parooliõngitsuste eest ja kohustada teavitama infoturvet, juhul kui kasutaja kahtlustab, et on õngitsuse ohvriks langenud.

8. Veenduda, et varunduslahendused on olemas ja toimivad.

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