



TRENDID JA TÄHELEPANEKUD KÜBERRUUMIS

II KVARTAL 2023

- 1.** Ettevaatust – õngitsussõnumid!
- 2.** Kübertest sai valmis!
- 3.** Ründed teenusepakkuja kaudu on püsiv risk
- 4.** Eestis on ligi sada paikamata tarkvaraga veebipoodi

1. Ettevaatust – õngitsussõnumid!

Teises kvartalis levisid Omnivat imiteerivad õngitsussõnumid kulutulena. Kahju ennetamisel on abiks teadlikkus sellistest ohtudest ning eeskujulik küberhügieen.

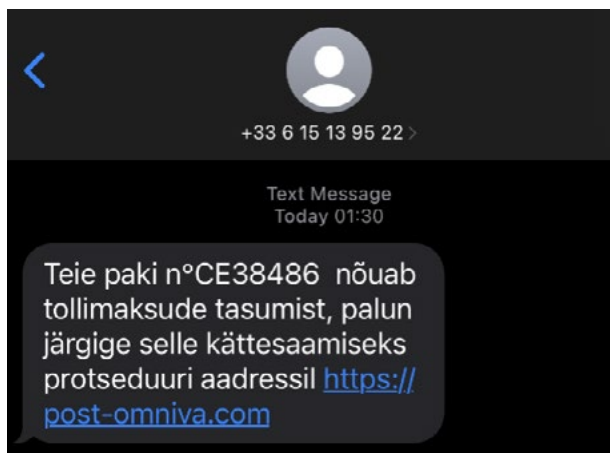
Olukord

Õngitsuste kaudu püütakse inimestelt välja petta nende paroolid, pangakaardiandmeid ja raha. Kui enamasti saadavad petturid masspostitustega õngitsevaid e-kirju, siis viimastel kuudel näeme eriti sagedasti SMS-i teel saadeta- vaid õngitsussõnumeid. Peasjalikult jäljendavad petturid Omnivat, aga ka teisi kullerteenuse pakkujaid.

Pahaaimamatule ohvrile Omniva nimel saadetud sõnum teavitab inimest, et tema pakk ootab kohaletoimetamist ning selle kättesaamiseks tuleb tasuda lisatasu või tollimaks. Sõnum sisaldab ka linki libalehele, mis on Omniva veebilehega äravahetamiseni sarnane. Suurimad kahjusummad, mida inimesed õngitsustele maikuus kaotasid, jäid paari tuhande euro kanti.



Näiteid libasõnumitest.



RIA hinnang

Omnivat imiteeriva õngitsussõnumi muudab ohtlikumaks asjaolu, et postiteenuse pakkuja kasutab ka ise SMS-i ühe viisina kliendiga kontakteerumiseks. Näiteks on Omniva SMS-i teel suunanud inimesi uuendama oma andmeid. Kui mõnikord aitab õngitsussõnumit ametlikust sõnumist eristada teadmine, et teenusepakkuja SMS-iga teavitusi ei saada, siis Omniva sõnumite puhul tuleb olla eriti tähelepanelik tegelike ja libasõnumite eristamisel.

Õngitsussõnumid inimestele tuttavate ettevõtete nimel jäävad kindlasti üheks viisiks, kuidas petturid hõlptulu püüavad. Tuletame meelde põhilised ohumärgid, mis viitavad, et tõenäoliselt on tegu õngitsusega:

1. Sõnumil on kehv õigekiri ja/või ebalooiline lausete ülesehitus.
2. Sõnum on saadetud kahtlaselt ja/või välismaa numbrilt.
3. Sõnum sisaldab kahtlast veebilinki, mis sisaldab tihti mingil kujul viidet imiteeritava organisatsioonile/ ettevõttele, kelle klientidelt üritatakse andmeid/raha välja petta.
4. Sõnumi tekst viitab probleemi kiireloomulisusele.
5. Tavapärastel teenusepakkuja sõnumi teel kliendi poole ei pöördu / sellise sisuga sõnumeid ei saada.

Juuni alguses avaldas RIA õngitsussõnumitest ka ohuhinnagu, mida saab lugeda [siin](#).

2. Kübertest sai valmis!

Aprilli algusest pakume RIA loodud Kübertesti, mille eesmärk on tõsta ja hoida kõigi töötajate küberturbeteadlikkust.

Test on suunatud eelkõige riigiasutustele (valitsusasutused, põhiseaduslikud institutsioonid ja kohalikud omavalitsused) ning elutähtsa ja olulise teenuse osutajatele, kuid ootame küberturvalisuse koolitust läbima ka teisi huvilisi.

Kübertest jaguneb kaheks. Esmalt palume kasutajal läbi töötada kursuse osa, mis katab 12 teemat. Neist paljude juurest leiab hoiatavaid näiteid päriselust, näiteks reaalseid õngitsuskirju ja pettuseid, mida on CERT-EE meeskonnale uurimiseks saadetud. Pärast kursuse läbimist tuleb sooritada test. Testis on 25 küsimust, mis valitakse juhuslikult küsimustepangast ja seega igaühel tuleb sooritada veidi erineva sisuga test. Iga kasutaja saab kohe teada oma punktisumma ning tagasisidet õigete ja valede vastuste kohta. Kursuse ja testi läbimine võtab aega umbes poolteist tundi ning see on kõigile tasuta.

Kübertestis kaetakse näiteks järgmised teemad: paroolid ja kontode turvalisus, lunavara ja õngitsuslehed, viirused ja pahavara, e-kirja teel levivad ohud, mälu pulgad ja muud andmekandjad, turvaline kaugtöö, nutiseadmete ja sotsiaalmeedia turvaline kasutamine ning veel palju muud.

Esimese kolme kuu jooksul on Kübertestiga liitunud juba 90 asutust ja organisatsiooni. Nende hulgas riigiasutused, kohalikud omavalitsused, koolid, haiglad, perearstikeskused ja ka mõned ettevõtted. Juuni lõpu seisuga on juba enam kui 8300 inimest jõudnud oma teadmisi täiendada ja testida.

Senise statistika põhjal võib öelda, et Kübertesti tegijatel on üsna head teadmised nutiseadmete kaitsmise vajadusest ja kaugtöö ohtudest – neil teemadel vastab suurem osa kasutajatest õigesti. Kõige rohkem raskusi valmistab aga õngitsuslehe äratundmine ja õige tegutsemine. Kahjuks seda trendi näeme ka CERT-EE registreeritud intsidentidest: igas kuus on ligi pooled teavitused just õngitsuslehtede kohta ja näeme, et paljud Eesti inimesed satuvad õngitsuste ohvriks.

Kui sinu asutusel või ettevõttel on huvi Kübertestiga liituda, kirjuta aadressil kybertest@kybertest.ee. Kübertesti kasutamise taotluse ja muu info leiad [RIA kodulehelt](#).

RIA_ITT / Küberturbe koolitus

TUND

Küberturbe koolitus

Tere,


Oled alustamas küberturvalisuse koolitust, mis koosneb 12 erinevast teemast.

Palun tutvuda kursuse sisuga enne testi tegemist.

Head õppimist!

Teema 10: Turvaline kaugtöö

Olenevalt asutusest võib kaugtöö tegemise kord varieeruda. Kaugtöö lubamine või piiramine on iga asutuse või ettevõtte enda reguleerida ning täpsema info saamiseks tuleks tutvuda enda organisatsiooni kaugtöö korraga.



Kõige levinum ja turvalisem variant on teha kaugtööd asutuse sülearvutiga **VPN ühenduse kaudu**. VPN tähendab virtuaalset privaatvõrku, mis tekitab sinu ja kasutatava teenuse vahele turvatud ühenduse, kus edasi-tagasi liikuvad andmed on kaitsitud kolmandate osapoolte eest.

Üldjuhul ei ole lubatud tööga seotud dokumentide salvestamine isiklikku seadmesse - see kehtib nii arvuti kui ka mobiiltelefoni või tahvelarvuti puhul. Samuti ei tohiks tööandja dokumente salvestada isiklikule mäluvälisele või välisele kõvakettale.

TUNNI MENÜÜ

- Sissejuhatus
- Teema 1: Infoturvet ja küberturvalisus
- Teema 2: Milleks meile küberturvet?
- Teema 3: Juhtumid küberruumis
- Teema 4: Paroolid ja kontode turvalisus
- Teema 5: Viirused, pahavara ja kuidas end kaitsta
- Teema 6: Lunavara ja õngitsuslehed
- Teema 7: E-kirja teel levivad ohud
- Teema 8: Turvaline andmeside ja WiFi ehk traadita võrk
- Teema 9: Mälu pulgad ja muud andmekandjad
- Teema 10: Turvaline kaugtöö
- Teema 11: Nutiseadmed
- Teema 12: Sotsiaalmeedia, sõnumivahetusprogrammid ja pilved

Kokkuvõtte

3. Ründed teenusepakkuja kaudu on püsiv risk

Teenusepakkujast tulenevaid riske täielikult välistada ei ole võimalik, ent saab astuda samme, mis neid vähendavad ja võimalikku mõju piiravad.

Olukord

Möödunud kvartalis nägime taas ühte juhtumit, kus kurjategijatel oli õnnestunud sisse häkkida ühte tarkvarateenust pakkuva ettevõtte võrku ning levida sealtkaudu edasi ka mitme teise kliendi infosüsteemi. Klientide hulgas oli erineva suuruse ja profiiliga ettevõtteid, mõnedki neist pigem hea üldise küberturvalisuse tasemega.

Lisaks ründest põhjustatud otsesele kahjule – näiteks andmekadu või infosüsteemi nakatumine pahavaraga – toovad sellised ründed kaasa rea probleeme, mis on seotud teenusepakkuja vastutuse ja kliendisuhetega kaasnevate lepinguliste kohustustega laiemalt. Isegi kui lõplik rahaline vastutus jääb teenusepakkuja kanda, võib sellele eelne da pikk ja kurnav menetlusprotsess, mis paratamatult segab ettevõtete tavalist äritegevust.



RIA hinnang

Ründed teenusepakkuja kaudu, mida nimetatakse ka tarneahelarünneteks, on viimastel aastatel saanud palju tähelepanu nii küberkogukonnas kui ka rahvusvahelises meedias laiemalt. Oleme ka oma kvartaliülevaadetes nendest varem kirjutanud (nt [2021 1. Ja 2. kvartali ülevaates](#)).

Sõltumata sellest, mis on kurjategijate algne eesmärk, võivad tarneahelaründed kiiresti laieneda ning halval juhul mõjutada tuhandeid kliente üle kogu maailma, nagu nägime NotPetya rünnaku puhul 2017 ja SolarWinds juhtumiga 2020. aastal. Ehkki sellise mastaabi ja hävitava mõjuga ründed on siiski haruldased, on teenusepakkujast tulenevate küberturvalisuse riskide teadvustamine ja vähendamine teema, millele ka Eestis tuleb jätkuvalt tähelepanu pöörata.

Teenusepakkujat valides soovitame tutvuda ettevõtte küberturvalisuse standarditega, toimivate kriisiplaanide olemasolu ja klientide teavitamise korruga ning vastavad punktid ka lepingus kajastada. Siis on lootust, et rünnaku korral on selle mõju sinu ettevõttele minimaalne ja kiiresti ohjatav.

4. Eestis on ligi sada paikamata tarkvaraga veebipoodi

Vaatamata CERT-EE korduvatele teavitustele on Eestis sadakond veebipoodi, mis kasutavad aegunud Magento tarkvara ning ei ole seetõttu küberturvalised.

Olukord

Lõppenud kvartalis saime teada juhtumist, kus ründajatel õnnestus sisse saada ühe veebipoe võrku ning varastada sealt kliendiandmebaas (pangaandmeid andmebaasis ei olnud). See ei ole üllatav, sest juba eelmisel aastal tuvastas CERT-EE rutiinse seire käigus üle kolmesaja veebipoe Eestis, mis kasutasid aegunud versiooni avatud lähtekoodiga Magento e-kaubanduse platvormist ning olid seetõttu haavatavad ühe konkreetse turvanõrkuse vastu.

Kõigile neile saadeti teavitused ning korduvteavitused, et nad tarkvara esimesel võimalusel uuendaksid. 2023 maiks olid ligikaudu kaks kolmandikku veebipoodide seda ka teinud, ülejäänutele saadeti järjekordne meeldetuletus, et asjad oleks vaja korda teha.

Juuni lõpus korratud kontrollseire näitas, et viimasele teavitusele olid reageerinud vaid üksikud ohus olevad veebipoodid. Seega eksisteerib täna endiselt peaaegu sada erinevaid tootegruppe müüvat vähem või rohkem tuntud Eesti veebipoodi, mille kaubandusplatvorm ei ole küberturvaline.

Juuni lõpus korratud kontrollseire näitas, et viimasele teavitusele olid reageerinud vaid üksikud ohus olevad veebipoodid.

RIA hinnang

Aegunud ja turvanõrkustega tarkvara kasutavad e-poodid on ründajatele mõistagi ahvatlevaks sihtmärgiks. Kui õnnestub e-poe platvormile sisse häkkida, proovitakse sageli varastada klientide andmeid, sealhulgas pangakaartide andmeid. Selleks paigaldatakse veebipoele vastav pahavara või lisatakse õngitsusleht, mille kaudu ohvrite andmed kokku korjata.

Kui e-poodi haldav ettevõtte on oma hooletusega põhjustanud isikuandmete lekke, võib see kaasa tuua kopsaka rahatrahvi riikliku järelevalveasutuse poolt – vastavalt Euroopa isikuandmete kaitse üldmäärusele kuni 20 miljonit eurot või kuni 4% ettevõtte eelmise majandusaasta ülemaailmsest kogukäibest. Sellises mastaabis trahve Eestis seni õnneks määratud ei ole, aga võimalus selleks on olemas ning trahvidest sõltumata ei tohiks ükski e-pood oma küberturvalisusega nii kergekäeliselt ümber käia.

Väga oluline on järgida RIA poolt tehtavaid hoiatusi ja soovitusi, eriti juhul, kui saate CERT-EE käest personaalse hoiatuse. Magento platvormi kasutajatele andsime konkreetsed soovitusel oma maikuus avalikustatud [ohuhinnangus](#).



Läheb hästi

Mitme valdkonna väikese ja keskmise suurusega ettevõtetele on võimalik taotleda küberturvalisuse taseme kaardistamise ja arendamise toetust. Toetuse omafinantseering on 50% ning maksimaalne võimalik toetus on 60 000 eurot. Taotlusi saab esitada jooksvalt, loe lähemalt [RIA kodulehelt](#) ja [EASi kodulehelt](#).



Saaks paremini

Aprillis saime teada ühest suuremast andmelekkest, kus paikamata jäänud turvanõrkuste tõttu lekkisid erakõrgkooli endiste ja praeguste tudengite nimed, e-posti aadressid, paroolid ja muu tundlik info. Selline andmebaas on potentsiaalne kullaauk kurjategijatele edasiste sissemurdmiste kavandamiseks. Siinkohal tuleb jälle tõdeda, kui oluline on turvapaikade regulaarne rakendamine.