RIIGI INFOSÜSTEEMI AMET

Trendid ja tähelepanekud küberruumis

Kvartaalne ülevaade, IV kvartal 2018

Varem kompromiteeritud meilivestlustesse vahelesegamine

OLUKORD:

Oleme näinud petukirjade lainet, kus kurjategijad püüavad ettevõtetelt raha välja petta kasutades ära kompromiteeritud meilikontode ja meilivestluste sisu. Näiteks suvel kompromiteeriti ühe Eesti ettevõtte meilikontod. Esialgu teatati meile suure hulga õngitsuskirjade väljasaatmisest, kuid tegelikult salvestati samal ajal meilikontode kirjavahetused, mida üritati paar kuud hiljem ära kasutada uueks rünnakuks ettevõtte partnerite vastu: ühe pikema meilivestluse jätkukirjana paluti välismaa partneril hakata tulevikus arveid maksma uuele pangakontole.

Sarnaseid kirju oleme näinud ka niipidi, kus Eesti ettevõte on meilivestluses teise riigi (nt Aasias asuva) koostööpartneriga. Pikema meilivestluse ühes etapis palub partner muuta pangakonto andmeid. Hiljem selgub, et partneri meilikontod on kompromiteeritud ja kurjategija püüab mõlema poolega eraldi vestelda ning raha välja petta. See tähendab aga, et ühe lühikese perioodi jooksul ei tea kumbki osapool, et meilivestlused on kaaperdatud.

ANALÜÜS:

Sellised rünnakud on palju keerukamad võrreldes tavapäraste petuskeemidega (kus näiteks ettevõtte juhina esinev kurjategija kirjutab finantsjuhile ühekordse küsimuse „kas me saame saata 30t täna?“) ja nõuavad kurjategijalt rohkem ressursse. Eesmärgiks paistab olevat leida ohver, kellelt suuremaid summasid saaks välja petta. Selle eesmärgi nimel on kurjategija valmis pikemat aega meilivestlusi jälgima ja otsima õiget hetke, kus end meilivestlusesse vahele segada.

Tegemist on raskesti äratuntava petuskeemiga, sest näiliselt tulevad kirjad ikkagi koostööpartnerilt endalt. Oleme näinud, kuidas petturid loovad kirjade võltsimiseks uusi (aga ettevõtte nimega seotud) meiliaadresse, mis võivad pettuse reeta. Eeldades, et kurjategijatel on õngitsuskirjade abil kätte saadud mingi hulk ettevõtete kasutajakontosid, peaksid kõik ettevõtjad olema ettevaatlikud ja kontrollima üle olukorrad, kus partner soovib arvete tasumist mõnele senisest erinevale pangakontole.

Vähem eraisikuid, rohkem ettevõtteid ehk Office 365 rünnakud

OLUKORD:

Eesti ettevõtted, kes kasutavad Microsoft Office 365 rakendusi, on teavitanud meid andmepüügist ja -vargustest. Ettevõtetele mõeldud Office 365 meilirakenduse kaudu on kurjategijad leidnud ka võimaluse meilivestlusi pikemalt jälgida ja endale kopeerida, et neid hilisemates petukirjades ära kasutada nagu eelpool kirjeldasime.

Sarnaseid juhtumeid on märganud ka Soome sideteenuste amet FICORA, kes teatas suvel mitmest Office 365 teenust kasutavast Soome ettevõttest, kes on langenud kalastamise ja seejärel niinimetatud tegevjuhi petuskeemi ohvriks. Office 365 kompromiteerimise trendile on tähelepanu pööranud ka mitmed küberturbefirmad oma ohuhinnangutes.

ANALÜÜS:

Arvestades keskmiste ja väiksemate ettevõtete hinnatundlikust ning Microsofti ülemaailmselt tugevat mainet, on Office 365 kasutamine ka Eestis üsna levinud. Kuna teenus võimaldab ettevõtte-üleseid aadressiraamatuid, on see tõenäoliselt ka edaspidi kurjategijatele atraktiivseks ründevektoriks. FICORA hoiatas, et kurjategijatel on Soomes õnnestunud mööda hiilida ka Office 365 mitmefaktorilisest autentimisest. (Sellest hoolimata tagab mitmefaktoriline autentimine kordades parema turvalisuse võrreldes lihtsalt paroolidega.)

Microsoft on samas investeerinud palju oma pilvetoodete turvalisuse parendamiseks, pöörates näiteks eraldi tähelepanu õngitsuskirjade takistamisele.

Olukord näitab, et ründajad sihivad järjest enam ettevõtete raha eest otsustajaid. Eraisikud (ja nende kontod) on samas esimeseks kohaks, kustkaudu kurjategijad meilikontodele ligi võivad pääseda.

64%

CERT-EE tänavu registreeritud intsidentidest* on seotud pahavaraga.

Mis teha, kui sinu ettevõtte meilikontodele ligi pääseti?

Arvestades meilikontode ärakasutamise trende soovitab RIA ettevõtetel ja asutustel väga tõsiselt pöörata tähelepanu kõikidele juhtumitele, kus töötajate meilikontodele on juurde pääsetud.

TEAVITA OMA KOOSTÖÖPARTNEREID

Kurjategijad võivad oodata mitu kuud, enne kui nad hakkavad uuesti sinu asutuse nime ära kasutades sinu partneritelt raha välja petma. Kui sinu asutuse töötaja meilikonto kompromiteeritakse, anna oma koostööpartneritele sellest märku, et oled langenud kuriteo ohvriks, mis võib partnereid hiljem mõjutama hakata – näiteks hoiata neid, et kui teie poolt hakkab keegi rääkima pangakonto detailide muutmisest. Selline põhimõtteline muutus tuleks kindlasti mitme kanali kaudu üle kinnitada. Nii näitad sa ka oma partneritele, et pöörad turvalisusele tähelepanu.

HOOLITSE OMA NIME EEST

Isegi kui SPF poliitika, DKIM tempel ja DMARC protokoll tunduvad liiga tehniliste kontseptsioonidena, on need ekspertide jaoks lihtsad ja odavad viisid, kuidas vähendada võimalust, et kurikaelad just sinu nime kasutades püüavad õngitsuskirju või pahavara laiali saata. Tee kurjategijatel elu oluliselt keerulisemaks.

OTSI VÕIMALUSI RAKENDADA MITMEFAKTORILIST AUTENTIMIST

Mõtle läbi, kuidas oleks sinu ettevõttes võimalik kasutada mitmefaktorilist autentimist, nii et võõrast arvutist meilidele ligi pääsemine oleks võimalikult keeruline. Suurte pakkujate kõrval on ka mitmed Eesti teenusepakkujad teinud kaheastmelise autentimise võimalikuks.

Sihitumad ja rohkem tööd nõudvad lunavararünnakud

OLUKORD:

Käesoleval aastal ja just viimaste kuude jooksul oleme näinud Eesti edukate lunavararünnakute puhul trendi, kus kurjategijad kasutavad kaugtöölaua (Remote Desktop Protocol ehk RDP) jaoks lahti jäetud võrguühendusi selleks, et pääseda sisse ettevõtete ja asutuste sisevõrkudesse. Selliseid kogu internetile avatuks jäetud kaugtöölaua teenuseid on võimalik leida automatiseeritult. Pärast teenuse leidmist püütakse jõuründega ära arvata kasutajatunnuseid ja paroole ning mõnikord see ka õnnestub, kuna kasutatakse lihtsalt nõrku paroole. Seejärel paigaldatakse (enamasti käsitsi) sisevõrku lunavara ja käivitatakse.

ANALÜÜS:

Hoolimata lunavararünnakute ulatuslikust mõjust ettevõtetele ja asutustele paistab jätkuvalt, et ettevaatusabinõud võetakse kasutusele alles pärast edukat lunavaraintsidenti. Kuigi RDP potentsiaal ründevektorina oli küberturvalisuse kogukonnale teada juba 2016. aasta teisest poolest, paistab, et ka kaks aastat hiljem tuleb süstemaatiliselt teavitustööd teha. USA föderaalne juurdlusbüroo pidas 2018. aasta septembri lõpus vajalikuks sel teemal eraldi teavituse teha, et kodanikud ja ettevõtted vaataks üle, millist ligipääsu väljastpoolt nende süsteemidesse vaja läheb ja kui tõenäoline oleks selle haavatavuse ärakasutamine.

Mõistame, et pelgalt teavitamine ei pruugi IT-võrkude eest vastutavate inimeste käitumist kohe mõjutada, kuid kavatseme edaspidigi koolitustel ja kogukonna koosviibimistel sellele ründevektorile tähelepanu pöörata. Eeldame, et lähiajal näeme jätkuvalt sellist meetodit kasutades edukaid lunavararünnakuid keskmistele- ja väikestele ettevõtetele ja asutustele, kellel pole ehk niivõrd palju ressursse end teadlikult kaitsta. See omakorda kinnitab trendi, kus kurjategijad on sihikule võtnud tavakasutajate asemel pigem organisatsioonid, kellelt on võimalik rohkem raha nõuda.

**** CERT-EE käsitleb intsidentidena neid juhtumeid küberruumis, millel oli mõju infosüsteemide konfidentsiaalsusele, terviklikkusele või käideldavusele. Lisaks riigivõrgule teavitavad CERT-EE-d vabatahtlikult veel mitmed ettevõtted, asutused ja eraisikud.***

13%

enam intsidente* registreeris CERT-EE 2018. aasta esimese 9 kuu jooksul võrreldes 2017. aasta sama perioodiga.

Teadaolevate nõrkuste ärakasutamine „unustatud" seadmete kaudu

OLUKORD:

2018. aastal on avalikustatud mitu turvaviga eraisikute ja väike-ettevõtete kasutuses olevates ruuterites. Need haavatavused võimaldavad kurjategijatel näiteks võrguliiklust jälgida või krüptoraha kaevandada. Ka meie saatsime juulis välja pressiteate Mikrotiki poolt toodetud ruuterite turvanõrkuse kohta ja palusime seadmete tarkvara uuendada. Sellest hoolimata jõuab CERT-EE-ni pidevalt teavitusi selle kohta, et uuendamata tarkvaraga ruuterid on jätkuvalt võrkudesse ühendatud nii avalikus sektoris kui ka eraettevõtete poolt.

ANALÜÜS:

Kuigi näiteks eelpoolmainitud ruuterite tarkvara saab uuendada, loodavad kurjategijad üsna tihti, et äsja avaldatud turvanõrkust ei pane kasutajaid tähele, ei näe uuendamiseks vajadust või ei mäleta, et nende võrku oleks mõni taoline seade ühendatud.

Avalikke teavitusi seadmete nõrkustest jälgivad nii küberturbe eksperdid, aga ka kurjategijad. Nii pea, kui värske haavatavuse detailid avaldatakse, püütakse selle nõrkuse peale ehitada uus eksploit. Kuna kiirus on oluline, suudavad kurjategijad kiiresti kasutada uuendamata seadmeid oma pahavara levitamiseks (kusjuures spämmimises võib süüdi jääda haavatava seadme omanik, kes võib seetõttu sattuda mõnesse musta nimekirja) või mõnel muul viisil seadme ära kasutamiseks.

Mida enam kasvab internetti ühendatud seadmete hulk – näiteks asjade interneti ehk IoT üha laiemal levikul – seda enam võime eeldada, et taoliste unustatud seadmete turvanõrkusi püütakse edaspidigi ära kasutada. Kui seadmed end ise automaatselt ei uuenda ning need ei ole enam ekspertkasutajate vaid tavakasutajate käsutuses, võib oodata, et veelgi väiksem osakaal kompromiteeritud seadmetest saavad kas kohe pärast nõrkuse avaldamist või mõistliku aja jooksul uuendatud.

LÄHEB PAREMAKS: ↗

Perearstid saavad rohkem tähelepanu

Võrreldes suuremate tervishoiuteenuste pakkujatega on meile muret teinud väiksemate perearstikeskuste küberturvalisuse võimekus. Samas oleme neile hakanud süstemaatiliselt tähelepanu pöörama ning vaikselt paistab edusamme. Oleme valmis saanud perearstide poolt kasutatavate infosüsteemide küberturvalisuse analüüsi, mille alusel saame Tervise ja Heaolu infosüsteemide keskusele teha ettepanekuid süsteemide arendamiseks.

Lisaks saavad perearstid nüüd sarnaselt avaliku sektori töötajatele teha küberhügieeni digitesti, mis oskuste kaardistamise kõrval aitab neil ka küberhügieeni kohta õppida. Lisaks kutsusid perearstikeskused Tallinnast ja Harjumaalt, Viljandimaalt ja Tartumaalt oktoobrikuus toimunud kübertalgutel endale eksperte külla koolitusi tegema.

EI EDENE: ⚠

Eesti ettevõtete ja asutuste e-kirju saab jätkuvalt võltsida

Paljud küberintsidendid saavad jätkuvalt alguse e-kirjadest, mille saatja aadressi ja kirjastiili on võimalik lihtsasti võltsida, jättes niimoodi mulje, et kiri tuli tuttavalt. Selle riski vähendamine on võimalik, kasutades tasuta lahendusi (näiteks SPF, DKIM, DMARC - küsi lisaks nõu cert@cert.ee), mis aitavad kontrollida, kas kiri tuli õigest kohast ja õigelt saatjalt.

Kuigi mõnel juhul võib nende konfiguratsioon tunduda keeruline, soovitame siiski ettevõtetel ja asutustel tungivalt sellised tehnoloogiad kasutusele võtta, et vähendada pahavara jagavaid ja kasutajaandmeid õngitsevaid kirju. See ei ole sajaprotsendiline kaitse, aga teeb ründajatel elu palju keerulisemaks.

Kui sa oled saanud kirja, kus sul palutakse vahetada pangakonto andmeid või saata tundmatusse kohta raha, tasub kiri veel mitu korda üle vaadata ja võimalusel mõnd muud kanalit kasutades see soov üle kinnitada.

Käesoleva kokkuvõtte koostas RIA küberturvalisuse teenistus eesmärgiga selgitada küberohtude trende võimalikult laiale auditooriumile, sealhulgas lugejatele väljaspool Eestit. Olukorda küberruumis analüüsib RIA küberturvalisuse teenistus detailsemalt igakuistes kokkuvõtetes. Tehnilisemaid soovitusi jagab CERT-EE koolitustel ja RIA koduleheküljе kaudu.