Lunavarajuhtumi ennetamine

10 aastat tagasi - 13.04.2016 Autor: Anto Veldre

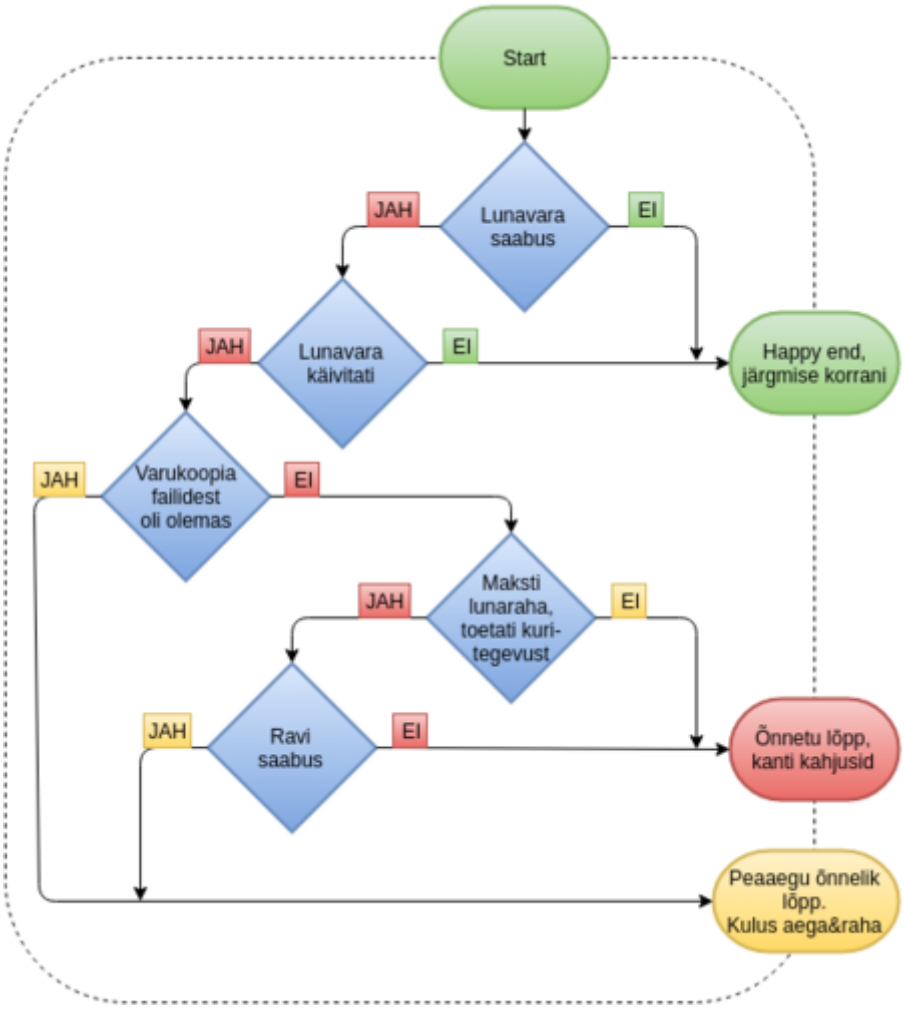
Aastal 2015 leidis Eestis aset vähemalt 150 lunavaraga seotud väljapressimisjuhtumit (kuid arvatavasti rohkemgi). Lunavarajuhtumite hulk ei kipu vähenema ka sel aastal. Kasutaja hooletu käitumise tõttu käivitub arvutis pahavara, mis muudab tuhanded failid mõttetuks bitijadaks. Olukorras, kus ravi puudub, tuleb pigem mõelda ennetusele.

PILT: (CC) Christiaan Colen / Flickr

Lunavara on erilist tüüpi kuri(tark)vara, mis krüpteerib ohvri failid ja nõuab siis taastamise eest lunaraha. Seni on võideldud põhiliselt tagajärgedega. Lunarahaviiruse külaskäigul on kindel hulk stsenaariume – kas varukoopia, kust oma failid taastada, eksisteerib või mitte?! Ning kui tekib küsimus kurjategijaile maksmisest, siis mõnikord saadakse omad failid tagasi, kuid vahel mitte.

Lunarahanõue tekitab keerulisi eetilisi dilemmasid – kurjategijatele makstes nimelt toetaksime kuritegevust täiesti otseselt. Ka pole garantiid, et ravim üldse saabub – on juhtunud ka sedasi, et pätid võtavad raha vastu, aga faile ikkagi lahti ei lukusta.

Alljärgnev kirjatükk käsitleb proaktiivseid lahendusi – ehk siis neid, millega peaks tegelema enne kui lunavara külla tuleb. Soovitused on kirja pandud CERT-EE ulatusliku kogemuse põhjal.



Põhilised vastumeetmed

Olgu tegu koduarvuti või firma arvutisüsteemiga, ennetava sekkumise kohti on põhiliselt neli:

1. Panna filter vahele, et lunavara ei jõuakski arvutisse. Üldisemalt tähendab see asjalikku viirusetõrjet ning netis sirvimise keskkonna pisukest häälestamist.
2. Takistada lunavaral käivitumist.
   Esimeseks filtriks on inimene, kes ei peaks uudishimust või tegevuslustist kõigel klikitaval klikkima. Inimeste teadlikkust saab oluliselt tõsta.
   Teiseks filtriks on operatsioonisüsteemide keerulisem timmimine nii, et tundmatu või vales kataloogis asetsev fail lihtsalt ei käivituks (Windows Group Policy, DEP; (SE)Linux).
3. Teha varukoopiaid süsteemselt ja sageli (ning ühtlasi viisil, mida lunavara ei suudaks rünnata).
4. Panna päitsed kahju ulatusele – ennetavalt luua piirangud (näiteks kasutajaõiguste piirangud), et pahalane ei ulatuks asutuse failiserverit kokku krüptima ega varem tehtud varukoopiat solkima.

Korporatiivse võrgu iseärasused

Asutuse või firma arvutisüsteemi puhul on väga palju kasu keskhaldusest. Kui pahavara ühes tööjaamas ära tuntakse, siis saab vastumeetmed hetkeliselt käivitada ka kõigis teistes tööjaamades. Kodu puhul säärased kallid automaatseadmed puuduvad ning pigem tuleb loota planeerimise ja ettevalmistuse kvaliteedile.

Asutuse/firma teine eelis on ülemaailmsesse reputatsioonisüsteemi ühendatud kallid riistapuud – tulemüürid, sisufiltrid jms, mis kasutajale märkamatult iga võrguühendust „nuusutavad“. Koos keskhaldusega moodustub reaalajalähedaselt tegutsev kaitse. Eraisik neid kaste osta ei jaksa, küll aga saab eraisik pingule timmida oma netisirviku häälestused.

Asutuse/firma kolmas eelis on palgaline itimees, kes orienteerub Windowsi Registry’s ja kasutajaõiguste finessides ning suudab arvutitele igasuguseid drakoonilisi piiranguid peale sundida.

Asutuse/firma iseloomulikuks probleemiks on töötajate arv. Ükski töötaja pole ilmeksimatu, saja töötaja puhul tõuseb tunduvalt tõenäosus, et mõni neist ikkagi kliki pahavaral. Piisab vaid ühest kasutajast ja mõnest ülearusest õigusest failiserveris, kui juba ongi tuhanded failid kasutamatuks muudetud. Halvimal juhul võib seetõttu peatuda kontori põhitegevus.

Varundamine

Varundamisel tuleb juhinduda 3-2-1 reeglist. Infost (failidest) peab olema vähemalt kolm eksemplari, vähemalt kahel erinevas tehnoloogias kandjal (magnet vs optiline) ning vähemalt üks eksemplaridest võiks asuda kusagil mujal (off-site), näiteks vanaema kapis või pangaseifis. Digitaalse info puhul on kohatu rääkida originaalist ja koopiatest, sest bitikombinatsiooni kõik esinemisjuhud on võrdväärsed. Originaal on koopiatest eristamatu.

Enne varundamist on oluline tuvastada unikaalne ja oluline info, mida pole võimalik mujalt hankida ega taastada. Näiteks pole eriti mõtet varundada Internetist kohale tiritud muusikat ja filme, seda kraami saab alati uuesti kohale tirida või vooteenusena vaadata. Oluline on varundada unikaalsed failid – perekonnapildid, originaalarved, kirjanduslik looming, asutuse töö käigus tekkinud dokumendid, patsiendi haiguslood – kõik see, mida nullist taastada polegi võimalik või mis nõuaks mahukat käsitööd.

Varukoopiate tegemist mõnikord kardetakse, kuivõrd planeerimisele kulub palju vaimuenergiat ja aega ning pole kindlalt teada, kas tagavarakoopiat üldse läheb kunagi vaja. Otsustamisel on abiks üks mõtteharjutus – küsige endalt, kui palju oleksite nõus maksma oma andmete tagasisaamise eest. Reeglina need, kel on kordki õnnestunud andmekaost pääseda ja oma failid varukoopialt tagasi saada, varundavad edaspidi palju agaramalt.

Mitte kõik varundusmeediad pole samaväärsed. Mistahes varukoopia on ikkagi parem kui selle puudumine, seejuures failiserver on parem kui üksik kõvaketas, pilv (Amazon, Google Drive) on parem kui USB pulk. USB pulkade ning isekõrvetatud DVD’de lugemisega tekib sageli probleeme, kuid alustamiseks kõlbavad needki.

NB! Soovitusi

C: kettal teise kataloogi tehtud lisakoopia pole varundamine, vaid pelk julgestuskoopia (omaenda vigade vastu)!

Riigiasutustes ja teravas konkurentsis töötavate firmade puhul pilv varundamiseks ei sobi – sest tundlikku infot ei sobi võõra onu juures hoida. Ka ei sobi pilv ülearu isiklike fotode jaoks, mis eiravad pilve asukohariigi konservatiivseid arusaamu kombekusest. Pilveketast (nagu DropBox) ei tohiks hoida kogu aeg arvuti küljes – või muidu suudab lunavara ära krüpteerida ka selle. Seevastu USB pulk võib äikeselise ilma või siidi ja villaste riiete vahelise hõõrdumise tulemusel tekkinud elektrilaengust hetkeliselt rikneda.

Eraldi küsimus on varundamise sagedus. Kodus tuleb normaalseks pidada üht korda nädalas, korraliku IT osakonnaga firmas või asutuses vähemalt kaks korda päevas, aga võimalusel suisa jooksvalt. Et andmemahud ülemäära ei paisuks, toimetatakse varundamist inkrementaalselt, ehk siis, iga korraga lisandub varukoopiale vaid see osa failidest, mis vahepeal loodi või mida vahepeal muudeti.

Tuleb arvestada, et kui failimaht ületab 1-2 terabaiti, siis hakkavad oma mõju avaldama füüsikaseadused. Statistiliselt esineb kettal lugemisvigu nii sageli (10*E-14), et mõni fail ikka saab rikutud. Statistiliste vigade vältimiseks ei peaks varundamiseks kasutama liiga suuremahulisi (8TB) üksik-kettaid ning asutuse/firma IT peaks kindlasti pruukima veaparandusega kettasüsteeme (RAID-6, RAIDZ-3).

Varunduslahendus peab arvesse võtma sama faili eri versioone – teisisõnu, ei tohi algset faili lunavara poolt ärakrüpteeritud monstrumiga üle kirjutada, sarnasele

nimele vaatamata.

Asjalik soovitus – identifitseeri oma kroonijuveelid oma andmete hulgas juba täna, osta suhteliselt odav väline kõvaketas ning soorita oma elu esimene tagavarakoopia!

Manused

Ehkki lunavara levitatakse ka muul moel kui e-kirjaga, on ohtlikul manusel klikkimine täna siiski esmane levituskanal.

Kõige keerulisemas olukorras on need töötajad, kelle ülesanne ongi avalikkuselt või partneritelt e-mailide vastuvõtmine. Kuid ka neil on võimalik järgida lihtsaid saastatuvastusreegleid. Siinkohal näide minu postkasti saabunud nn downloader'itest, millel klikkimine viib vältimatult TeslaCrypt'i või Locky'ga nakatumiseni:

Subject	From	Date	Size
Dossier n° 6336	**CABINET BETTAN**	**Thu 14:03**	**126 KB**
Dossier n° 6782	CABINET BETTAN	Thu 13:28	126 KB
Fwd: Your account has been remove	Support	2016-04-01 22:41	4 KB
Documents	Rene Herrera	2016-04-01 17:59	4 KB
Documents	Mike Boyer	2016-04-01 17:27	4 KB
images	Juan Manuel PEREDA	2016-04-01 15:13	6 KB
photo with u	Natalia LAMBERT	2016-04-01 13:54	6 KB
image	Axel MERCEDES	2016-04-01 13:38	6 KB
Photos	**Nadia Maria Ochoa**	**2016-03-31 16:48**	**6 KB**
hi prnt	**andrew**	**2016-03-31 14:06**	**6 KB**
Emailing: FILE73153029.xls	MXSCAN	2016-03-30 15:02	7 KB
Emailing: PDF950417011.PDF	EPSON	2016-03-30 14:10	7 KB
Bill N-B4CBC1	Ebony Banks	2016-03-29 22:12	6 KB
Bill N-CA7560	Shirley Collier	2016-03-29 20:55	6 KB
CCE29032016_00023	cleary@xyz.ee	2016-03-29 19:41	5 KB
Delivery Confirmation Receipt - Tracking #57DC...	Whitney western	2016-03-29 17:46	10 KB
Delivery Confirmation Receipt - Tracking #7335A...	Marco balderstone	2016-03-29 17:36	10 KB
Your Personal Information Has Been Updated	Estelle sandham	2016-03-29 13:23	10 KB
Reset your password	22mobi	2016-03-29 12:45	4 KB
Credit Card Has Been Declined *9438	Gladys brundell	2016-03-29 11:58	10 KB
Reduce Your Electrical-expense up to 80-per.	Electric_Bill	2016-03-29 01:38	25 KB
FW:	Jayne shearer	2016-03-28 17:01	10 KB
FW:	Roxanne cregan	2016-03-28 16:19	9 KB
FW:	Hope olds	2016-03-28 13:33	10 KB
FW:	Patricia meachem	2016-03-28 12:56	10 KB
FW:	Shanna landale	2016-03-28 12:10	9 KB
Sixt Invoice: 8772286969 from 24.03.2016	**Bianca - ICM Research**	**2016-03-24 17:29**	**70 KB**
Sixt Invoice: 4813941908 from 24.03.2016	**Marcie - Panmure Gordon & Co.**	**2016-03-24 17:27**	**70 KB**
Sixt Invoice: 1904386576 from 24.03.2016	**Rich - GCM RESOURCES PLC**	**2016-03-24 16:22**	**70 KB**
Contract ID 83893 has been terminated	Selena rhines	2016-03-23 19:22	6 KB
Invoice PNINV26107 from EARTHPORT PLC	Geraldine Blackburn	2016-03-23 16:04	64 KB

Pole vist keeruline märgata teatud seaduspärasusi – ühetaolised, uudishimu tekitavad ettekäänded, mitte-eesti nimed, selgelt äratuntavad kampaaniad, mille käigus saabub suur kogus ohtlikku materjali päevas. Kirjad tulevad firmadelt, millega me pole kunagi asju ajanud olnud, viidatakse kontodele ja ressurssidele, mida me pole kasutanud.

Küberkurjategijad firmanipp on saata pahaloomulisi meile, mis ei ole saajaga kuidagi seotud ning loota, et huvi või hirm või muu tugev emotsioon saab inimesest võitu. Näited: arve ettevõttelt, kust ei ole inimene kunagi midagi tellinud või hoopis kurikiri õiguskaitseorganilt – ohver, kartes seadusega pahuksisse jäämist, ei suuda vastu panna ja avabki lunavara sisaldava meili. Pole vahet, kas klikitakse manusel või pahatahtlikul lingil – lunavara suudab arvutisse ronida mõlemat pidi.

Järelemõtlemisreeglid enne kui klikkida on esitatud ühes varasemas blogiloos.

Vahel kasutab kurjategija meiliteesklust (spoofing). Sel juhul langeb saatja nimi kokku mõne sõbra või tuttava omaga, kuid meiliaadress ise (kurionu@kusagil.com) on loodud keskkonnas, kus tuttaval või sõbral aadressi polegi. Sestap tuleb postiaadressi väli alati üle inspekteerida, kuigi postiprogrammist olenevalt võib see nõuda päris mitut lisaklikki.

Kahtluse korral aitab väga lihtne nipp – helistada tuttavale või küsida temalt Skype’s, kas tema on säärase kirja saatnud. Kuid ettevaatust, ka sõbra Skype võib juba olla üle võetud eesti keelt mittekõnelevate kurjamite poolt…

Võrguadministraatorile: blokeerimine ja filtreerimine

Filtreerimine puutub nii veebisurfamisse kui e-maili saamisse. Eraisiku kodused võimalused on pisut piiratumad, kuid firma ja asutuse IT-administraatoril on vaba voli teatud failitüübid ära keerata. Säärane eristamine toimub faililaiendi põhjal. Alustada tuleks käivitamisohtlike failide nagu “.exe”, “.js”, “.com”, “.msi”, “.vbs”, “.jar” blokeerimisest.

Ärisuhtluses on “.pdf”, “.zip” ning “.rar” failide blokeerimine problemaatilisem, kuivõrd neid vorminguid kasutatakse äritegevuses sageli. Kõige vastuolulisemateks on “.docx” ja “.xlsx” laiendid – need failid on makrode tõttu ohtlikud, kuid äritegevuses vältimatult vajalikud. Firmal ning asutusel tuleb siin leida kompromiss, mis inimesi kaitseks, kuid veel ei segaks põhitegevust. Eriti tuleks karta Wordi ja Exceli faile, mis on saabunud tundmatust allikast ning mis nõuavad makrode aktiveerimist – säärased tuleks itimehe juurde kontroll viia.

Asutuses ja firmas tuleks kindlasti kasutada mõnda seadet, mis kontrollib kogu netisurfamist ning pistab kisama niipea kui veebilehelt leitakse mõni nakatunud reklaam. Sellise seadme häälestamine väljub käesoleva kirjatüki raamidest, kuid tuleks teha valik lubatud ja keelatud veebilehtede vahel. Üks häälestamisviise (whitelisting) on see, et kõik, mis pole otseselt lubatud, on keelatud. Keerulisema äri puhul tuleb kasutada blacklist tüüpi filtrit, ehk siis keelustada kõik veebisaidid,

mil pole tööprotsessiga pistmist (porno, sport, mängurlus). Vastava reputatsiooniteenuse saab sisse osta koos filtrikastiga.

Kodus tuleks kindlasti kasutada mõnd AdBlock taolist tarkvara, mis likvideerib kõik veebilehega otseselt mitteseotud lisamaterjali (reklaami, pakkumised). Kahjuks lõpetab iis töö ka mõni asjalik, kuid vale tehnoloogiat (java, javascript) kasutav veebileht – säärastele tuleb käsitsi teha erandid.

Filtreerimise tulemus – kurjategijatel ei õnnestu viia inimest ohtlikul lingil klikkima – filtrikast astub vahele ja blokeerib kahtlase veebisaidi vaatamise. Ühtlasi saadetakse e-kiri itimehele või turvatöötajale.

Konkreetse(ma)d soovitused

Enamikes arvutites sobib brauserina kasutamiseks Chrome, mis kaitseb kasutajat päris mitmel moel:

1. Sandboxing – teenus, mille eesmärgiks on tagada, et pahavaral poleks arvutis installiõigust ning eraldada Chrome’i eri aknad üksteisest (et üks aken teisest infot ei varastaks)
2. Uuendused – Chrome hoiab ennast pidevalt uuendatuna ning paigaldab turvapaigad automaatselt.
3. Safe Browsing – Kasutajat hoiatatakse kui ta satub teadaolevale pahalehele.

Adobe Flash on osutunud sedavõrd ebaturvaliseks, et targem on see oma arvutis keelata.

Sirviku pluginad – tuleks ka need üle vaadata, lubada vaid seda, mis on vältimatu (ID-kaardi tarkvara) või vastupidi, vajalik kahtlase materjali filtreerimiseks – nagu näiteks uBlock Origin .

Veel üks tore plugin on **ScriptSafe** – see ei luba veebilehtedel javascripti käivitada. Võrguadministraatorid saavad pluginaid majandada läbi Windowsi grupipoliitika (group policy).

Antiviirus – tuleb arvesse võtta, et mitte ükski neist ei suuda 100%-list kaitset pakkuda. Vähemalt 95%-list kaitset pakuvad neist siiski enamik, mistõttu viirustõrje peab kindlasti olema paigaldatud ja kindlasti ka uuendatud (ajakohane olgu nii tarkvara ise kui viirusi äratundvad definitsioonid). Tuleb paraku tõdeda, et tasuta viirustõrjed sageli ei suuda omi definitsioone piisava kiirusega uuendada, et pidevalt muutuva lunavara eest efektiivselt kaitsta.

Uuendused – tänapäeva maailma reaalsuseks on, et igas vähegi populaarses tarkvaras leitakse turvaauke kui mitte iga nädal, siis kord kuus kindlasti. Enam polegi muud varianti, kui lubada automaat-uuendused igas arvutis ja nutiseadmes.

Kasutajaõigused – ilmaasjata ei peaks keegi endale arvutis administraatori õigusi tahtma. Õigused peaksid olema täpselt nii pingule kruvitud, et kasutajad oleksid üksteisest eraldatud – kui ühel neist juhtubki äpardus, siis ei laiene see kogu kollektiivile. Eriti tuleks ligipääse piirata võrguketastel – sest sinna on kogunenud kõige kriitilisemad ressursid.

ANTO VELDRE
Riigi Infosüsteemi Ameti analüütik

Artikkel on pärit RIA blogist

- Lahendused
- Uudised

- Turvalisus