TARTU ÜLIKOOL
Arvutiteaduse instituut
Informaatika õppekava

Lauri Välja

Kalastuskirjade ohtlikkus tehnoloogiaettevõtte näitel

Bakalaureusetöö (9 EAP)

Juhendaja: Kristjan Krips

Tartu 2018

Kalastuskirjade ohtlikkus tehnoloogiaettevõtte näitel

Lühikokkuvõte:

Iga aasta põhjustavad kalastuskirjad ettevõtetele suuri kahjusummasid. Käesolevas töös tutvustatakse kalastusrünnetega seotud probleeme, antakse ülevaade tehnoloogiatest, mis võimaldavad ründeid vähendada ning uuritakse ühe konkreetse ettevõtte teadlikkust õngitsusrünnetest. Ettevõttes sooritatud katsega selgus, et erinevatest turvakoolitustest alati ei piisa ning töötajad võivad sattuda rünnaku ohvriks. Töö viimases peatükis tuuakse lugejale elulisi näiteid, kuidas vältida kalastuskirjadega kaasnevaid ründeid.

Võtmesõnad:

Kalastuskirjad, e-kiri, manipuleerimisründed, SPF, DKIM

CERCS: P175

Dangers of phishing based on an tech-company

Abstract:

Every year, companies spend big amounts of money because of phishing attacks. In the following work the author will give an introduction to problems about phishing, give an overview of the technologies used for phishing and an experiment on a tech-company. From the conducted experiment we learn, that despite different security trainings, people might still fall for phishing attacks. In the last chapter, there will be real-life examples and tips how to avoid phishing attacks.

Keywords:

Phishing, email, social engineering, SPF, DKIM

CERCS: P175

1. Sissejuhatus **4**

2. Ülevaade manipuleerimisrünnetest **6**

2.1 Kalastusründed 6

2.2 Miks on ründed muutumas järjest levinumaks? 8

3. E-kirja saatmine ning saamine **9**

3.1 E-kirjadega kaasnevad probleemid 10

3.2 E-kirjade turvalisus 11

Senders policy framework (SPF) 11

SPF Probleemid 12

DomainKeys Identified Mail (DKIM) 13

DKIM seadistamine 14

DKIM Probleemid 14

3.3 Nõrgimaks lüliks jääb inimene 15

4. Eksperiment **16**

4.1 Ettevõte 18

Koolitused töötajatele 19

Ettevõtte turvaprotokoll 19

4.2 Programm kalastuskirjade saatmiseks 19

4.3 Kalastuskirjade koostamine 20

4.4 Kalastusrünnaku läbiviimine 26

4.5 Ettevõtte töötajate teavitamine 26

4.6 Tulemused ja analüüs 27

4.7 Järeldus 30

5. Kuidas vältida rünnaku ohvriks sattumist? **31**

6. Kokkuvõte **37**

7. Viidatud kirjandus **38**

Litsents **44**

1. Sissejuhatus

Internetti kasutab üle nelja miljardi inimese, kellest 90% kasutavad igapäevaselt ka e-kirja teenust [1, 2]. Suur hulk interneti kasutajaid loob ühtlasi pinnast ka kuritegevusliku tegevuse tekkimisele. Potentsiaalsed ohud, millega interneti kasutajad silmitsi seisavad on näiteks krediitkaardi pettused, võltsuudised, infooperatsioonid, tundlike andmete vargused ning kahjurvaraga nakatamine.

Gemalto andmetel on alates 2013. aastast on peaaegu 10 miljardit lekitatud või varastatud andmekirjet ning nendest andmetest on kõigest 4% krüpteerimise tõttu loetamatud [3]. Identiteedivargus on kõige levinum andmelekke tüüp [3] ning suur osa identiteedivargustest viiakse läbi tänu manipuleerimisrünnetele. Manipuleerimisrünnak (*Social Engineering*) kujutab endast rünnakut, kus ründaja suhtleb sihtmärgiga ning kasutab ära tema heatahtlikkust, sõbralikkus, huvi või muid psühholoogilsi meetodeid mõjutamaks isikut pahaaimamatult välja andma informatsiooni. Manipuleerimisrünnakute üks alamkategooria on kalastuskirjad.

Kalastuskirjadeks või õngitsuskirjadeks (*phishing*), kutsutakse rünnakuid, mida teostatakse e-kirjade kaudu. Kalastuskirjade eesmärgiks võib olla ohvri arvuti nakatamine ohtliku programmiga, kontode üle võtmine ja muu tundliku info hankimine, mida saab omakasu eesmärgil kuritarvitada. Näiteks kui ründaja saab õngitsuskirja abil ligipääsu ohvri paroolidele, krediitkaardi numbritele, siis on tal võimalik muuta saadud info rahaliseks kasuks. Lisaks on võimalik ka varastatud info abil ohvrilt lunaraha välja pressida. Sellisel juhul tagastab ründaja varastatud info ohvrile kokkulepitud summa eest.

2017. aasta seisuga saadeti päevas ligikaudu 269 miljardit e-kirja [4], millest umbes 2 miljardit sisaldas kahjurvara [5]. Kuigi e-kirjade kaudu levitatud kahjurvara osakaal jääb alla ühe protsendi, siis sellegipoolest langeb suur osa inimestest kuritegelike kalastuskirjade lõksu. 2017 aastal puutus 9% ehk umber 350 miljonit unikaalset interneti kasutajat kokku kalastuskirjadega [6]. Cloudmark uuring, millele vastasid Suurbritannia ja USA ettevõtted, raporteeriti keskmiseks

kahjuks 1.6 miljonit dollarit [7]. FBI andmetel on ettevõtted kaotanud kolme aastaga miljardeid dollareid [8]. Seetõttu on oluline tõsta internetikasutajate teadlikkust kalastuskirjade ohtlikkusest.

Rünnakute ohvriks satuvad tihti ka inimesed, kes on juba teadlikud kalastuskirjadest ning oskavad neid tuvastada. Ründajad võivad koguda oma ohvri kohta infot koguda pikema aja vältel, et muuta kalastuskirja sisu võimalikult usutavaks ning meelitada ohvreid külastama e-kirjas olevat hüperlinki. Näiteks saadab ründaja e-kirja, kus saatjaks paistab justkui olevat ohvri pikaaegne teenusepakkuja. Vastavas e-kirjas võidakse mainida, et teenuse säilitamiseks, peab vajutama e-kirjas olevale hüperlingile ning järgima ettenähtud juhiseid. Kuna tõenäoliselt ei soovi ohver enda pikaaegsest teenustest ilma jääda siis psühholoogilistel põhjustel võib kaduda ohvril ohutunne ning vajutab e-kirjas olevale hüperlingile.

2016. aasta USA presidendivalimiste eel tegi Hillary Clintoni kampaaniajuhi, John Podesta assistent kogemata vea, märkides turvaliseks kalastuskirja, milles oli nõutud, et John Podesta muudaks enda e-posti konto parooli. Kuna assistent märkis e-kirja usaldusväärseks, siis pärast selle avamist said ründajad ligipääsu umbes 60 000 e-kirjale, mis olid Podesta privaatses Gmaili postkastis. Ründajad tegid antud e-kirjad avalikkusele nähtavaks. Antud intsident on hea näide kalastuskirjade ohtlikkusest ning võimaliku kahju ulatusest.

Käesoleva töö eesmärkideks on tutvustada kalastusrünnetega seotud probleeme, anda ülevaade tehnoloogiatest, mis võimaldavad ründeid vähendada ning uurida ühe konkreetse ettevõtte teadlikkust õngitsusrünnetest.
Selleks on antud uurimustöös läbi viidud eksperiment ühe ettevõtte töötajate peal ja välja toodud tulemused ning soovitused rünnete vältimiseks. Sama eksperimendi tulemusi kasutati ka Filipczak Karina magistritöös [9]. Eksperimendi koostamise käigus valmis infrastruktuur, mis võimaldab analoogset katset vajaduse korral korrata. Kuna eksperimendis osalenud ettevõte käsitleb palju tundlikku informatsiooni (klientide isikuandmed, pangaandmed jms.) siis püstitan hüpoteesi, et ettevõtte töötajad oskavad ära tunda ning vältida õngitsuskirju.

2. Ülevaade manipuleerimisrünnetest

Seal, kus liigub informatsioon, liiguvad ka pahatahtlikud inimesed, kes üritavad salajast informatsiooni kätte saada ning seda enda kasuks ära kasutada. Informatsiooni püütakse kätte saada kasutades ära infosüsteemide turvaauke, kuid enamjaolt ründajad ei püüa süsteemi turvaauke rünnata. Infotehnoloogia ehk IT turvalisus on just nii tugev, kui on tema nõrgim lüli. Seega on pahalastel kergem ära kasutada olemasolevat nõrgimat lüli, kelleks on tihtipeale arvutikasutaja. Arvutikasutajatel on otsene ligipääs rünnatavale seadmele ning see loob võimalusi kasutajate manipuleerimise või petmise teel nende seadmetesse ligi pääseda.

Inimesed ja nende mõtted, ideed, käitumine on pidevas muutumises. IT turvalisuse üks suurimaid valenõuandeid on see, et inimesed teeksid endale keerulisemaid paroole, ilma selle jaoks mõeldud paroolihaldustarkvara kasutamata. Kuid tegelikkuses mida keerulisemaks parool läheb, seda suurem tõenäosus on, et inimene on selle kuhugi üles kirjutanud või kasutab ühte keerulist parooli mitmel veebilehel [10]. Sama parooli kasutamine mitmel leheküljel on ohtlik, sest kui üks leht lekitab kasutaja parooli, siis on oht, et pääsetakse ligi kasutaja teistele veebikeskkondadele.

Manipuleerimisrünnak (Social Engineering) kujutab endast rünnakut, kus ründaja suhtleb isikuga ning kasutab ära tema heatahtlikkust, sõbralikkust või huvi mõjutamaks isikut pahaaimamatult välja andma informatsiooni ründajale. Manipuleerimisrünnakute üks populaarsemaid alamkategooriaid on kalastuskirjad, mille puhul kogub ründaja ohvri kohta piisavalt informatsiooni, et leida, mis oleks võimalikult efektiivne rünnak antud kasutaja pihta. Alla 10% rünnakutest on sooritatud ründetööriistu kasutades või riistvaralisi turvaauke ära kasutades. Kahjurvarad on suunatud tehniliste rünnakute sooritamiseks. Enamus rünnakuid, üle 90%, on seevastu kalastusrünnakud, kuna need on efektiivsemad [11].

2.1 Kalastusründed

Kalastuskirjad (*Phishing*), kujutavad endast teesklust, kus ründaja saadab tundliku info saamiseks e-kirja, mis võib olla näiliselt saadetud usaldusväärse allika poolt (pank,

teenusepakkuja). Kalastuskirjaks võib nimetada e-kirja, kus ründaja saadab laiali spämm e-kirju, mis sisaldavad endas juhiseid võiduraha kättesaamiseks, mis tegelikult on varguse skeem, kus veendakse meili saaja saatma raha ründajale. Neist tuntuimad stsenaariumid on niinimetatud "Nigeeria printsi" või loterii võitude kohta käivad e-kirjad. Samuti võib e-kiri sisaldada hüperlinki, kus kasutaja suunatakse ründaja poolt võltsitud veebilehele, mis imiteerib panga veebilehte. Näiteks inimene, kellele meeldib palju reisida, saab tõenäoliselt hulganisti e-kirju soodsatest reisipakkumistest. Seega, püüab ründaja koostada sellise e-kirja, mis kujutaks endast head reisipakkumist, et meelitada kasutaja antud kalastuskirja avama. Näiteks suurasutuse juht, omanik või keegi muu, kellel eeldatavasti on ligipääs sisevõrgule saab e-kirja ründajalt, kes teeskleb asutuse turvajuhti ning palub tal oma parooli muuta. Kui asutuse juht läheb ründaja e-kirja kaudu parooli muutma, siis potentsiaalselt saab ründaja selle teada, mille tagajärjel kasutatakse saadud informatsiooni ära pahatahtlikel eesmärkidel.

Kasutades ära avalikult leitavat informatsiooni sihtmärgi kohta suudab ründaja enda kohta kokku panna väga veenva profiili [12]. Tänapäeval on palju infokanaleid, kust saab koguda erinevat informatsiooni inimeste kohta, näiteks Google, Facebook, Youtube, LinkedIn või mõni muu keskkond. [13] Üsna tihti on inimeste nimed märgitud ettevõtte ürituste sotsiaalmeedia postitustel või on näha inimese piltidest, et ta on tihti mingi konkreetse ettevõtte kontoris. Samuti on sotsiaalmeedias sageli avalikult kättesaadav informatsioon inimese varasemast töökogemusest, haridusest, üritustel käimistest, piltidest jms. Näiteks on olemas veebilehed nagu PiPl.com, kust saab inimese nime järgi otsida tema kohta avalikult kättesaadavat informatsiooni [14]. Antud lehelt on inimesel võimalik leida enda kohta järgnevat informatsiooni: kasutajanimed, ülikooliharidus töökogemus jne. Mõndade inimeste kohta leiab rohkem, mõne kohta vähem informatsiooni. Iga infokild on ründajale kasulik, et panna kokku võimalikult hea profiili oma potentsiaalsest ohvrist.

Kõige efektiivsemad kalastamiskirjad on suunatud konkreetse inimese või asutuse vastu. Niisugust rünnet nimetatakse harpuunimiseks (*Spearphishing*). Ettevõtete puhul uuritakse välja töötajate nimed, positsioonid, töögraafikud, kõik mis on ründajale lihtsalt kättesaadav

sotsiaalmeedias või teistel avalikel veebilehtedel. Tavalisest spämm-kirjast erinevad nad sellepoolest, et neid saadetakse vähestele isikutele ettevõttes ning nendega nähakse rohkem vaeva, et e-kiri näeks välja tõepärane.

2.2 Miks on ründed muutumas järjest levinumaks?

Tänapäeval pööratakse riistvara ja tarkvaraarenduses järjest rohkem tähelepanu turvalisusele. Kuna süsteemide enda turvalisus tõuseb, siis muutub turvaaukude leidmine keerukamaks ning ründed aina kallimaks. See on üks põhjuseid, miks manipuleerimisrünnakute populaarsus järjest kasvab.

Ründajate sihtmärkideks on peamiselt ettevõtted ja nende töötajad. Üheks põhjuseks on see, et ettevõtte kalastuskirjade ohvriks langemise tulemusena on neilt võimalik rohkem raha välja pressida. Wombat Security tehtud uurigust on näha, et peaaegu 80% maailma asutustest on langenud kunagi kalastuskirja ohvriteks [15]. Tihtipeale ettevõtted ei pane piisavalt rõhku manipuleerimisrünnakute vastastele koolitustele ning seetõttu pole töötajad alati informeeritud neid ümbritsevatest ohtudest [16]. Eeldatakse, et inimesed teavad, et võõraid kirju ei tohi avada ning enne hüperlinkidele vajutamist peab kindel olema, et tegemist on ausa e-kirjaga. Vahel teevad ründajad väga hea kalastuskirja ning isegi teravam silm omab raskusi, et eristada kalastuskirja õigest.

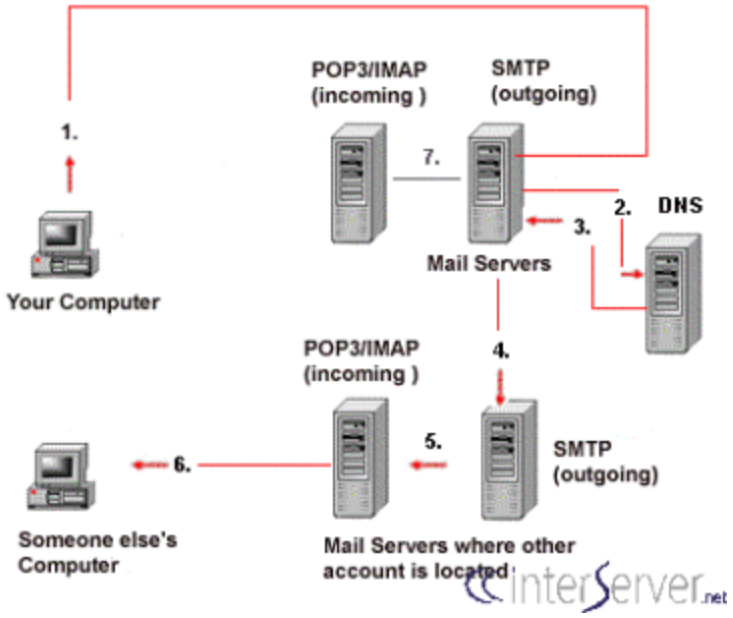
Kalastuskirjade populaarsus kasvab ka sellepärast, et ligikaudu 30% avatavatest kalastuskirjadest on edukad [17]. Kuni inimesed on liiga sinisilmsed võltskirjade suhtes, on ründajatel “motivatsiooni” selliseid rünnakuid rohkem läbi viia.

Näiteks 2017. aasta kolmandas kvartalis levisid mitmed kalastuskirjad orkaanide Irma ja Harvey ning Mehhiko maavärina kohta [18]. Kalastuskirjadega rünnati krüptoraha “buumi” ajal ka krüptoraha omavaid inimesi, kuna krüptorahade turuväärtus oli tõusnud 2017. aastaga 3000%, mis andis ründajatale võimaluse varastada kalastuskirjade ohvritelt suurtes kogustes raha [18, 19].

3. E-kirja saatmine ning saamine

E-kiri (elektronpost, e-post, meil) on elektroonselt kirjutatud sõnum, mida saadetakse ühise võrgu teel üle maailma. E-kirjad on tavalise teksti või html kujul, kuid samuti saab e-kirjadele lisada manusena faile [20]. Esimene e-kiri saadeti 1971 aastal Ray Tomlinsoni poolt iseendale. Tegemist oli test-kirjaga, millega Ray Tomlinson testis kahe arvuti vahelist suhtlust [21]. Tänapäeval saadetakse aastas umbes 269 miljardit e-kirja, millest alla 1% sisaldab kahjurvara [4, 5].

Kasutajale võib näida e-kirjade kasutamine väga lihtne, kuid tegelikkuses on e-kirjade saatmise tehnoloogiline pool veidi keerukam. Kõigepealt liigub e-kiri SMTP (Simple mail transfer protocol) ehk lihtsa meiliedastuse protokolliga meili-serverisse. SMTP käitub sarnaselt postkontorile, mille eesmärk on välja selgitada e-kirja lõpp sihtpunkt. SMTP saadab päringu DNS (Domain Name System) ehk domeeninimede süsteemi. DNS eesmärk on sobitada kasutaja sisestatud domeeninimed IP-aadressitega, kuna kõik seadmed, mis on internetivõrku ühendatud, omandavad IP-aadressi. Siis kontrollitakse, kas domeenil on olemas MX-kirjed, mis määravad ära domeeninimele vastavad meiliserverid. Kirje puudumisel e-kirja edasi ei saadeta ning kirje olemasolu korral tehakse märge e-kirja metaandmetesse. Nüüd on SMTP-l vajalik informatsioon olemas ning e-kiri saadetakse edasi saaja domeeni MTA (Mail Transfer Agent) ehk meiliagendile. MTA on tarkvara, mis võtab vastu sissetuleva e-kirja ja vajadusel suunab selle edasi järgmise meiliagendile, kuni e-kiri jõuab saaja meiliagendini. Arvuteid, mille eesmärk on selliseid süsteeme jooksutada, nimetatakse meiliserveriteks [22]. Seejärel otsitakse saaja domeenist üles saaja nimele vastav kasutaja, kelle saadetakse e-kiri. Lõpuks näeb saaja e-kirja enda meili-kasutaja sisendkaustas, kus tehakse see loetavaks IMAP või POP abil [23, 24].



Joonis 1: E-kirjade edastamise süsteem [25].

3.1 E-kirjadega kaasnevad probleemid

Päevas saadetakse umbes 269 miljardit e-kirja [4]. Andmeid koguva teenuse, Statista, andmetel on üle 50% saadetavatest e-kirjadest spämmkirjad ehk saajale soovimatud e-kirjad [26]. Need e-kirjad võivad ühtlasi sisaldada endas ka kalastusrünnakuid, vale-informatsiooni, reklaame vms. Suure spämm e-kirjade hulgaga kaasnevad ka erinevad probleemid. E-kirjade edestamise liiklus muutub aeglasemaks, kuna aina rohkem e-kirju on vaja e-posti serveritel üle-vaadata. Spämm e-kirjade pärast on ka kasutaja turvalisus ohus, aeg-ajalt ei suuda meiliagendid edukalt välja filtreerida spämmkirju ning kasutajateni võivad jõuda massidele suunatud kalastuskirjad. Õngitsuskirjade üheks trikiks on panna mõne tellimise lõpetamise (*unsubscribe*) nupu külge ohtlik hüperlink, mida vajutades satub kasutaja rünnaku ohvriks. Sageli kasutajad ei oska aimatagi hüperlingiga seosnevat pahatahtlikkust, kuna kalastuskirjad on üles ehitatud väga veenvalt ning usaldust tekitavalt. Seda illustreerib töö raames korraldatud eksperimendis osalenud isik, kes soovis spämmreklaami katkestada vajutades e-kirjas olevale nupule "*unsubscribe*".

3.2 E-kirjade turvalisus

SMTP loomisel ei olnud sellel krüpteerimise funktsionaalsust. See andis võimaluse kõrvalistel isikutel lugeda e-kirjade sisu. Pärast e-kirjade lugemise said ründajad muuta selle sisu või takistada e-kirja edasist liikumist. SMTP enda muutmise asemel kasutasid meiliserverid turvalisuse tõstmiseks lisamooduleid nagu SPF, DKIM, DMARC ja STARTTLS, mis autentisid kasutajaid ning välistasid e-kirjade võltsimist [27]. 2015. Aastal suutis Google Gmail valideerida 94% sissetulnud sõnumeid kasutades nii DKIM kui ka SPF-i, kuid 2015 aasta seisuga ainult 47% meiliserveritest kasutasid SPF-i, mille tagajärjel saaja meiliserver ei saanud alati aru, kas allkirjastamata e-kiri on pärit originaalse saatja poolt [27]. Siiski on probleeme ka vastavate tehnoloogiate rakendamisel, näiteks 29% vaadeldud SPF seadistustest oli kasutusel liiga üldine poliitika, mis kattis kümneid tuhandeid aadresse ning seetõttu ei olnud efektiivne [27].

Senders policy framework (SPF)

Turvalisuse tehnoloogiatest on Saatjapoliitika ehk Sender Policy Framework (SPF) kõige laialdasemalt levinud. Antud poliitikaga saab domeeni omanik kindlaks määrata, mis aadressitelt on lubatud antud domeenile kirju saata [28]. SPF kirjet kasutatakse meiliserverites, et vähendada rämpsposti. Mõned meiliserverid nõuavad sissetulnud e-kirjadel kehtivat SPF kirjet ning selle puudumisel võib e-kiri olla märgitud, kui rämpspost [29]. Antud meili autentimisviis aitab vältida spämm, võlts- või andmepüügi kirju, kuna saaja meiliserver kontrollib, kas saadetud e-kiri pärineb lubatud IP aadressilt ning kui see saatja IP ei sisaldu SPF kirjes, siis see e-kiri saaja postkasti ei tohiks jõuda.

SPF kirje seadistamiseks peab domeeni omanik lisama enda domeeni nimeserverisse (Doman Name System, ehk DNS) kirje. Kirjes on täpsustatud IP-aadressid, mis on lubatud saatma e-kirju sellelt domeenilt [28, 30, 31]. Näiteks Tartu Ülikooli (ut.ee) poolt saab kirju saata, kui kasutaja IPv4 aadress on 193.40.5.25.

Tartu Ülikooli SPF kirje [32]:

v=spf1 mx a:smtp1.it.da.ut.ee a:smtp2.it.da.ut.ee a:bounces.ut.ee a:mail.tarapitha.eu ip4:193.40.5.25 ip6:2001:bb8:2002:500::46 ip6:2001:bb8:2002:500::47 ip6:2001:bb8:2002:500::25 include:spf.protection.outlook.com ~all

Antud SPF kirje:

- tegemist on spf1 versiooniga, mis on kõige uuem ning stabiilsem
- E-kiri saadetakse edasi, kui see pärineb ühest järgnevast meiliserverist (smtp1.it.da.ut.ee, smtp2.it.da.ut.ee, bounces.ut.ee, mail.tarapitha.eu)
- E-kiri saadetakse edasi, kui see on saadetud lubatud IP vahemikus (ip4:193.40.5.25 ip6:2001:bb8:2002:500::46 ip6:2001:bb8:2002:500::47 ip6:2001:bb8:2002:500::25)
- include:spf.protection.outlook.com tähendab, et e-kirjad mis läbivad Microsoft Outlook SPF kirje kontrolli, on lubatud ka Tartu Ülikooli poolt. E-kirjad mis antud kirjele ei vasta, saaja postkasti ei saabu.

SPF Probleemid

Turvalisusega tegeleva ettevõte CipherTrust uuringust selgus, et spämm kirju, mis läbivad SPF kirje on ligikaudu 34% rohkem, kui mitte-spämm kirju. Antud probleemi põhjus seisneb selles, et spämm e-kirjade saatjad uuendavad SPF kirjeid tihedamini [33]. Tavalised e-kirjad ei läbi SPF kontrolli enamjaolt sellepärast, et domeeni omanik pole SPF kirjet üles seadnud. Kirje puudumisel mitmed meiliserverid ei saada kirju edasi [29].

Tihti on SPF kirje halvasti määratud, mille tagajärjel peab meiliserver otsustama, mida tehakse edasi e-kirjaga, mis ei läbinud SPF kontrolli. On olukordi, kus saaja teiseldusagent saadab e-kirja saajale olenemata kehvadest SPF sätetest. Antud olukord juhtub, kui SPF kirje kontrolli ebaõnnestumise tagajärjel meiliserver saadab e-kirja edasi [34].

SPF kirje ei kehti edasi saadetud e-kirjal. Selleks, et turvalisus säiliks soovitatakse kasutada *Sender Rewriting Scheme* (SRS) [35], kus e-kiri saadetakse uuesti eelmise saatja addressi poolt.

Meiliserverid sooritavad ainult 10 SPF kirje kontrolli päringut iga e-kirja kohta, et kaitsta servereid teenusetõkestusründe eest (*Denial of Service)*, mille puhul koormatakse serverit suure hulga päringutega. Seetõttu tekib olukordi, kus jääb mõni SPF kirje kontrollimata. Olukorra teeb halvemaks see, et pole viisi, kuidas teada saada, kas päringute limiit on täis. Võib juhtuda, et mõne SPF kirje reegel lubab e-kirja läbi, isegi, kui kirje terviklikult on katki. See võib juhtuda, kui mõnda kirjet ei kontrollitud, sest kümme päringut on täis ning mõni varasem päring on e-kirja usaldusväärseks autentinud [36]. Seega SPF kirjete seadeid ei tohiks liiga palju reegleid sisaldada.

SPF kontrollib domeeni, kuid ta ei kontrolli nime, mis on on enne domeeni, ehk lubatud.nimi@domeen.ee ning keelatud.nimi@domeen.ee on mõlemad lubatud. Antud e-kirja osa kontrollib DMARC.

SPF kirjes olev kirjaviga muudab selle kehtetuks, seega kirjet seadistades peab kindlasti kasutama SPF valiidsust kontrollivaid abivahendeid (näiteks SPF Validation Tool). Kui kirjet seadistades ei täideta mõnda nõutud välja, siis on kirje süntaks rikutud ning ei tööta.

Näide probleemsest SPF kirjest. [37]
Kirje 1: v=spf1 include:_spf.google.com ~all
Kirje 2: v=spf1include:sendgrid.net~all
Esimesel kirjel pole meilihalduri server (MX) lisatud. Teisel kirjel pole ühtegi tühikut, mis teeb antud SPF kirje kehtetuks.
Väljatoodud kahe SPF kirje õige ülesehitud näeks välja järgmine:
v=spf1 a mx include:_spf.google.com include:sendgrid.net ~all

DomainKeys Identified Mail (DKIM)

Domeenivõtmega identifitseeritud meil ehk *DomainKeys Identified Mail* (DKIM) on e-kirja autentimismeetod, mille abil saab saatja osa e-kirjast digi-allkirjastada [38]. Kasutatakse avaliku

võtme krüptograafiat nii, et privaatse võtmega allkirjastatakse kõik saatja meiliserverist välja saadetud e-kirjad [39]. Saaja meiliserveri saab vastava avaliku võtme kätte DNS abil.

Saatja meiliserver allkirjastab tervikliku või osalise e-kirja. Osad, mis on allkirjastatud, läbivad e-kirja kätte saamisel autentimiskontrolli ning kui selgub, et sisu on muudetud, siis kontrolli ei läbita ning e-kirja saajani ei saadeta [40].

DKIM seadistamine

Domeeni omanik peab genereerima domeeni võtme, mis lisatakse domeeni DNS kirjesse. E-kirja halduris peab domeeni omanik e-kirjade allkirjastamise sisse lülitama ning siis saab e-kirja saaja meiliserver antud võtme päisest kätte. Enamik keskkondi, mis müüvad domeene on antud protsessi automatiseeritud ning kasutaja ei pea ise midagi tegema. [40]

E-kirja saabudes saaja meiliserverisse, saab server aru, et see on allkirjastatud DKIM-ga. Peale mida võetakse DNSist avalik võti, millega dekrüpteerida e-kirja päis ning verifitseeida, et kiri tõesti pärines saatja domeeni poolt ning polnud saatmisprotsessi vältel muudetud, et saada ligipääs avalikule võtmele. [40]

Soovitused DKIM seadistamiseks

1. Kirje muutmisel või uue koostamisel peab DNS need ära kinnitama. Kinnitamine võtab aega uute kirjete puhul 10-15 minutit ning vanade muutmisel 2-24 tundi [41].
2. Kirjete kinnitamine võib ebaõnnestuda, kuna erinevatel DNS-del võivad olla erinevad vormistusreeglid. Näiteks mõni võib nõuda '\' enne ';' sümbolit DKIM kirje alguses ja lõpus [41].
3. DKIM kirje tegemisel on vaja enda DNS halduri käest uurida välja õiged vormistusreeglid [41].

DKIM Probleemid

Kõige tavalisem probleem DKIM-ga on edastatud e-kirja saajale mitte kohale jõudmine. Tavaliselt ei jõua e-kiri kohale, kui selle edasi saatnud meiliserver - edasi saatmise teenuse

pakkuja - lisab enda poolt e-kirjale info. Näiteks kui allkirjastatud on e-kirja keha ("*body*"), kuid edasi saates kolmandale isikule lisab meiliserver e-kirjale juurde "Edastatud MEIE poolt". Kuna edasi saadetud e-kirja sisu on muudetud, siis digiallkirja verifitseerimine ebaõnnestub ja e-kiri jääb edastamata.

E-kirja saaja võib sattuda "Replay attack" ohvriks. Tegemist on rünnakuga, kus DKIM-ga allkirjastatud e-kirjad on pahatahtlikud. DKIM võimaldab e-kirja saatjal valida e-kirja osad, mida räsitakse. Ründajad saavad allkirjastatud e-kirjale juurde lisada enda informatsiooni, näiteks muuta saates originaalse kirja enda nime alt edasi - sedasi ei mõjutata räsitud e-kirja osa. Seega lisades e-kirjale juurde uut teksti või kui lisada teine e-kirja saatja, jääb räsi muutumatuks, kuna digiallkirjastatud osa ei muudetud ning e-kiri saadetakse edasi. Näiteks alloleval pildil on kogu vana e-kiri jäetud samaks, kuid saatjaks on Random Spammer (ründaja), mitte Barack Obama (originaalne saatja). [41]

Date: Thu, 8 Aug 2013 21:44:28 -0700 (PDT)
From: Barack Obama <barack@whitehouse.gov>
From: Random Spammer <rndmspmr_098435@yahoo.com>
Reply-To: Random Spammer <rndmspmr_098435@yahoo.com>
Subject: Awarded a Pulizer for "DKIM is Harmful"
To: "Joseph Shmoe" <joe.shmoe@gmail.com>

Joonis 2: E-kirjal on kaks Saatja välja, millest üks on räsitud ja seega ka digi-allkirjastatud (Barack Obama) ja teine (Random Spammer - ründaja) ei ole [42].

3.3 Nõrgimaks lüliks jääb inimene

Turvalisuse kohta kehtib ütlus, et süsteem on just nii tugev, kui tema nõrgim lüli. Antud juhul jääb nõrgimaks lüliks arvutikasutaja. Erinevad meetodid, nagu SPF kirje, DKIM, spämmkirja filtrid, millega püütakse tõsta e-kirjade turvalisust ei hoia ära kõiki ohtusid, sealhulgas manipuleerimisründed. Seetõttu peavad olema arvutikasutajad tähelepanelikud ning oskama vastavalt käituda, et rünnaku ohvriks mitte sattuda. Järgnevas peatükis kirjeldatud katse abil püüan selgeks teha, kas inimesed on teadlikud kalastuskirjadest ning saada teada, kuidas nad käituvad, kui on sattunud rünnaku ohvriks.

4. Eksperiment

Inimesed ei saa tihti aru, millised näevad välja kalastuskirjad. Isegi kui töötajatele on tehtud koolitusi küberturvalisusest, ei saa mitmed enne aru, et on rünnaku ohvriks jäädud, kuni see mõjutab nende tööd. Töötajad, kes saavad päevas mitmeid e-kirju enda töö meilikasti, ei suuda alati kahtlustada kalastuskirju, eriti juhul kui nad ei ole oma töömeili mitte kuskile avalikult posititanud.

Katse abil selgitatakse välja, kas ettevõtte turvakoolitustest on kasu ning inimesed suudavad ennast kaitsta kalastuskirjade eest ning teavitada turvameeskonda. Eeldus on, et mitte keegi töötajatest ei vajuta kalastuskirjades võõrastele hüperlinkidele.

Eelduse läbikukkumise korral püütakse selgeks teha miks inimesed vajutavad hüperlinkidele, millele nad ei tohiks vajutada. Kas koolitus oli puudulik või töötajate tähelepanu lihtsalt hajus? Kas e-kirja sisu mõjutab töötajate otsust, kas vajutada hüperlinkidele e-kirjade või mitte?

Asutus, kus tehakse eksperiment: Ettevõtte soovil anonüümne
Katses osalevad töötajad, kes on jagatud erinevatesse gruppidesse vastavalt järgnevale jaotusele:

- Klienditugi
- Operatiivteenuste osakond
- Arendajad
- Tootejuhid ja juhatus
- Finants ja pangandus
- Personali osakond
- Turundus
- Järelvalve osakond

Töö e-posti aadressid on enamasti nimi.perenimi@asutus.com või siis nimi@asutus.com. Seega kui ründajal on teada töötaja asutus, siis on üsna lihtne sellest järeldada ohvri e-posti aadressi.

Eksperimendi ülesehitus:

- Ettevõtte ülevaade
- Kalastuskirjade koostamine
- Kalastusrünnaku läbiviimine
- Ettevõtte töötajate teavitamine
- Tulemuste analüüs
- Ettevõttele info edastamine
- Järeldused
- Soovitused töötajatele ning lugejale

Katse sooritamise hetkel oli asutuses ligikaudu 700 töötajat ning eesmärk oli katsetada erinevat tüüpi kirju. Selle jaoks jaotati töötajad erinevatesse gruppidesse ning meiligrupid loodi vastavalt sellele, millega töötajad tegelevad.

Tabel 1. Kalastuskirjade sihtgrupp, töötajate arv, tegevusala ning kalastuskirja tüüp

Sihtgrupp	**Töötajate arv**	**Tegevusala**	**Kalastuskirja tüüp**
Klienditugi	250	Aitavad kliente küsimuste ning probleemidega otseses suhtluses e-kirjade või telefonide teel	Tervituskiri, Hoiatus kalastuskirja kohta
Operatiivteenuste osakond	75	Tegelevad klientide rahade saatmisega pankade vahel	E-kiri panganduspartnerilt, LinkedIn
Järelvalve osakond	100	Teevad klientidele ning maksetele taustauuringuid ning vastutavad selle	Kiri kliendilt probleemiga

		eest, et raha on legaalselt saadud	
Finants ja pangandus	25	Tegelevad koostööpartneritega ning samuti asutusesisesed rahaasjad	Ryanair
Arendus	200	Inimesed, kes arendavad toodet ning omavad kõige paremat ülevaadet süsteemi sisemusest	LinkedIn
Tootejuhid ja juhatus	40	Arenduse juhid ning ettevõtte juhatus	LinkedIn, Ryanair
Turundus	20	Ettevõttega seotud turundus	Ryanair
Personaliosakond	40	Inimeste palkamine, aitamine. Omavad kõige rohkem infot ettevõttes töötavate inimeste kohta	LinkedIn, Ryanair

Ettevõttes pole seni korraldatud asutusesisest rünnakut, seega see on hea võimalus ettevõttel näha, kas turvakoolitustest on kasu ning millele peab rohkem tähelepanu pöörama. Pärast eksperimenti teavitatakse töötajaid antud testist ning antakse kõigile näpunäiteid ohtlike kirjade tuvastamiseks.

4.1 Ettevõte

Tegemist on IT-asutusega, millel on üle 2 miljoni kasutaja ning kuna käsitletakse väga paljude klientide isiklikke andmeid, siis on turvalisus väga tähtis. Tehnoloogiad, mida ettevõte kasutab peavad tagama konfidentsiaalsuse ja samuti töötajad, kes palgatakse peavad läbima turvakoolituse ning järgima asutusesiseseid turvanõudeid.

Koolitused töötajatele

Töötajad läbivad tööle asumise alguses umbes kahenädalase ettevõtet tutvustava koolituse, kus räägitakse süsteemidest, kasutatavatest tehnoloogiatest ning samuti turvalisusest. Töötajad, kellel on ligipääs kasutajate andmetele läbivad koolitusi, mille seas on ka kliendiandmete turvamise koolitus. Koolituse eesmärk on töötajatele selgeks teha kuidas kasutada enda töö sülearvutit, milliseid paroole kasutada, mida ei tohi klientidele rääkida ning kuidas vältida rünnaku ohvriks sattumist e-posti või telefoni teel.

Ettevõtte turvaprotokoll

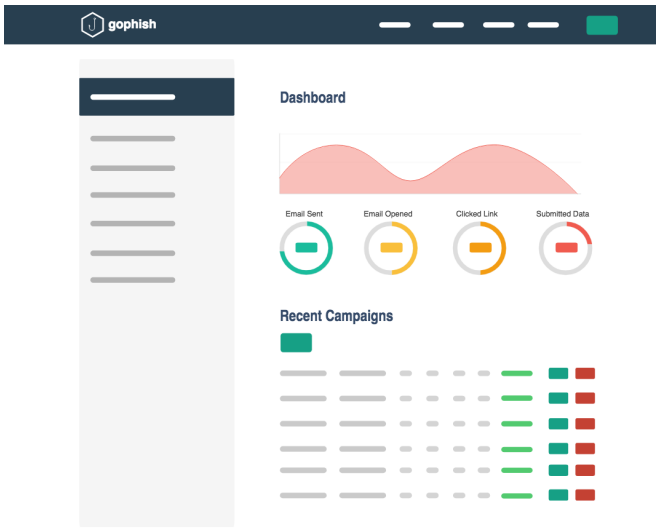
Igapäevase ettevõtte turvalisuse üle vastutab IT ja turvalisuse meeskond, kelle eesmärk on pidevalt jälgida süsteeme, et leida kahtlast tegevust arendatavas tootes, asutusesiseses keskkonnas ning ennetada turvariske. Kalastuskirjadega kokkupuutudes peab töötaja teavitama *Information Security Officer'i* (ISO) kes tegeleb ründe kahjutuks tegemisega ning terve ettevõtte teavitamisega antud ründest.

4.2 Programm kalastuskirjade saatmiseks

Rünnaku läbiviimiseks kasutati avatud lähtekoodiga programmi nimega GoPhish [43]. Valituks osutus GoPhish, kuna see oli avatud lähtekoodiga tööriist, mis täitis soovitud funktsionaalsusi ning oli mugava kasutajaliidesega. Leidus ka teisi teenusepakkujaid (KnowBe4, DuoInsight), kes viivad läbi sarnaseid katseid, kuid ei sobinud antud ettevõtte katse jaoks, kuna leheküljed soovisid lisainformatsiooni kasutajalt, et neid kasutama hakata.

Valitud programmi saab kasutada iga inimene - selleks tuleb paigaldada programm ning siis saab hakata ründeid läbi viima. Kasutaja peab valima sobiva kokkupakitud faili (.zip) vastavalt enda operatsiooni süsteemile (OSX, Linux, Windows). Antud fail on vaja lahti pakkida ning sätete failis (*config.json*) teha muudatused, et see töötaks lokaalsel masinal või virtuaalsel serveril. Tööarvutisse programmi paigaldamine ei sobinud, kuna programmile oli vaja ligipääsu mitmel inimesel ja see ei tundunud turvaline variant, kuna me polnud me kindlad, kas keegi võõras näeb asutusesiseselt kogutud andmeid. Keskkond oli vaja saada tööle nii, et see oleks ainult

asutusesiseselt kättesaadav ning informatsiooni, mida me sellega kogusime ei leviks avalikku võrku. Info kogumiseks kõikidest kontoritest loodi ligipääsu tööriistale läbi VPN-i, kuna see on kontorite vahel ühine. Programm seati üles AWS (Amazon Web Services) keskkonnas, sest see oli kõigest eraldatud ning turvaline. Andmete kogumiseks ühendati tööriist MySQL andmebaasiga, mida sai teha AWS-is. Lokaalse paigaldamisega võtab programmi tööle saamine paar tundi. Kuna süsteem oli vaja asutusesiseselt tööle saada, siis koos IT osakonna abiga (VPN ja AWS krediit), võttis see aega umbes 3 päeva. Pärast programmi tööle saamist oli ligipääs tööriistale ainult läbi VPN-i ja kaitstud parooliga.



Joonis 3: GoPhish avaleht pärast sisselogimist [43].

4.3 Kalastuskirjade koostamine

Koostati seitse erinevat kalastuskirja. Ettevõtte turvajuhi palvel loodi erineva "raskusastmega" e-kirjad. Mõni halb kalastuskiri, kus on lihtne tuvastada, et midagi on valesti. Samuti loodi e-kirju, mida ka teravam silm ei suuda kahtlustada.

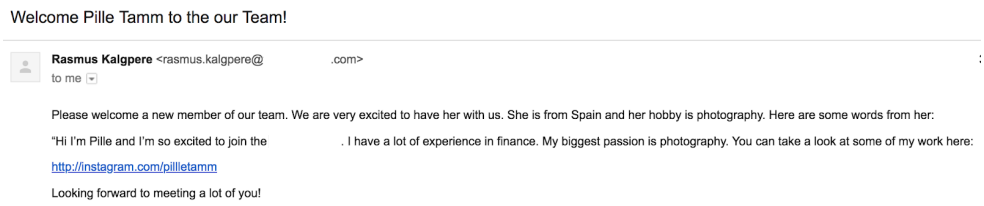
Kõik hüperlingid ja pealevajutatavad pildid e-kirjas suunasid kasutaja küsimustikku, kus küsiti lisainformatsiooni nagu näiteks miks e-kiri avati või miks klõpsati e-kirja sees olevale hüperlingile. Ründajad saavad samamoodi panna hüperlingi suunama ükskõik kuhu neile sobib.

Allpool on toodud näited e-kirjadest, mis loodi asutusesisese rünnaku jaoks (ettevõttega seotud nimetused on eemaldatud):

Tervituskiri

Tervituskirju saadetakse asutusesiseselt igapäevaselt, näiteks kui kõikidele töötajatele saadetakse uue töötaja kohta informatsiooni ning lastakse paar sõna endast rääkida. Kui sarnane e-kiri saadetakse välise ründaja poolt tähendaks seda, et ründajal on mingisugune arusaam ettevõtte sisekultuurist. Kasutati ettevõtte nimele sarnast e-posti aadressi, justkui tuleks e-kiri töökaaslaselt.

Uus töötaja, Pille Tamm, on fotograaf ning tema töid saab vaadata hüperlingilt, mis näib kui Instagrami hüperlink, kuid tegelikkuses suunab mujale.


Welcome Pille Tamm to the our Team!

Rasmus Kalgpere <rasmus.kalgpere@ .com>
to me

Please welcome a new member of our team. We are very excited to have her with us. She is from Spain and her hobby is photography. Here are some words from her:

"Hi I'm Pille and I'm so excited to join the . I have a lot of experience in finance. My biggest passion is photography. You can take a look at some of my work here:

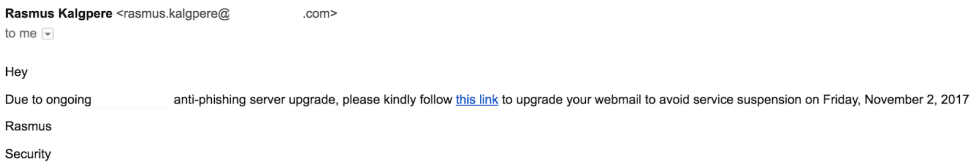
http://instagram.com/pillletamm

Looking forward to meeting a lot of you!

Joonis 4: Asutusesisene tervituskiri.

Hoiatus kalastuskirja kohta ning süsteemi uuendamise palve

Populaarne vorm, kus ründaja teeskleb asutusesisest turvatöötajat, paludes uuendada kasutajal midagi e-kirja sees oleva hüperlingi teel hiljemalt nädala jooksul. Tähtaeg lisab kasutajale tunde, et peab kiirustama. Sarnaselt eelmisele e-kirjale kasutati ettevõtte nimele sarnast e-posti aadressi.


Rasmus Kalgpere <rasmus.kalgpere@ .com>
to me

Hey

Due to ongoing anti-phishing server upgrade, please kindly follow this link to upgrade your webmail to avoid service suspension on Friday, November 2, 2017

Rasmus

Security

Joonis 5: Asutusesisene süsteemi uuendus.

E-kiri panganduspartnerilt

Ettevõtte panganduspartner saadab Operatiivteenuste osakonnale e-kirja, kus selgitab, et maksetega on probleeme. E-kiri sisaldab hüperlinki panga lehele, et töötaja saaks kontrollida milles probleem. Antud e-kirja jaoks kasutati tavalist Google Gmail kontot, mis võiks olla e-kirja saajale märk sellest, et midagi on valesti. Panganduspartner saadaks enda ettevõtte domeeniga e-posti aadressi poolt.

Error for last 1000 transfers

Peter Stone <peterstoner4@gmail.com>
to me

Hi there, we have encountered an error while reading your last batch file.

We added a screenshot under this link, could you please take a look!

https://www.hsbc.co.uk/1/2/payments/sS3oN8dm3Pz.pdf

Could you upload again the file for those transfers? It might have been a glitch in our system.

Sincerely,

Peter Stone

Finance operation assistant

Joonis 6: Panganduspartneril on probleeme maksetega.

Kiri kliendilt probleemiga

Klient kirjutab, et maksega on probleeme ning soovib abi postitades makse hüperlingi.

Where is my money?!

Peter Stone <peterstoner4@gmail.com>
to me

Hi

I wrote you an email before, but you have still not gotten back to me regarding it.

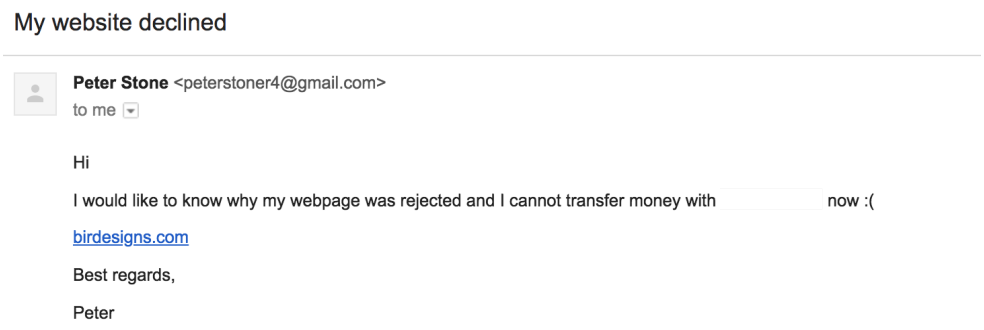
Please look into this as soon as possible. I want to know where my money is. Here is the payment https:// .com/payment/24049135

Sincerely,

Peter

Joonis 7: Klient kurdab, et raha on kaduma läinud.

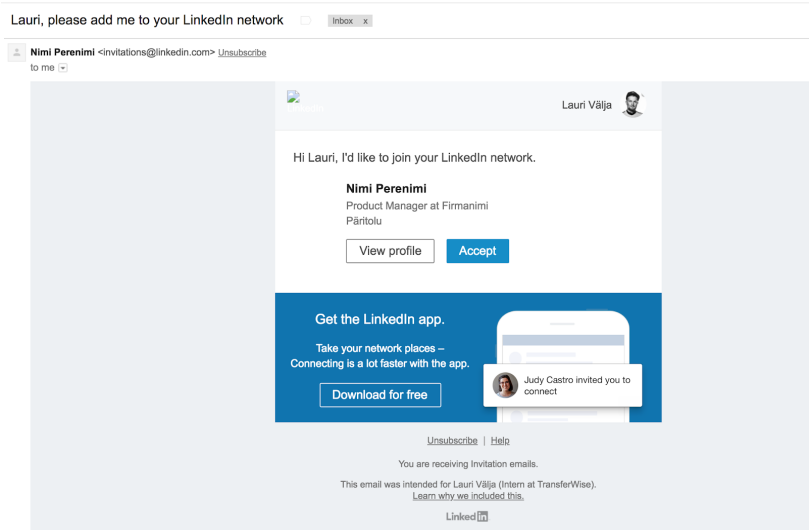
Klient kirjutab, et meie süsteem ei valideerinud nende veebilehte ning lisab juurde hüperlingi lootuses, et töötaja kontrolliks manuaalselt lisatud hüperlinki.



Joonis 8: Klient kurdab, et veebilehel oli probleem.

LinkedIn

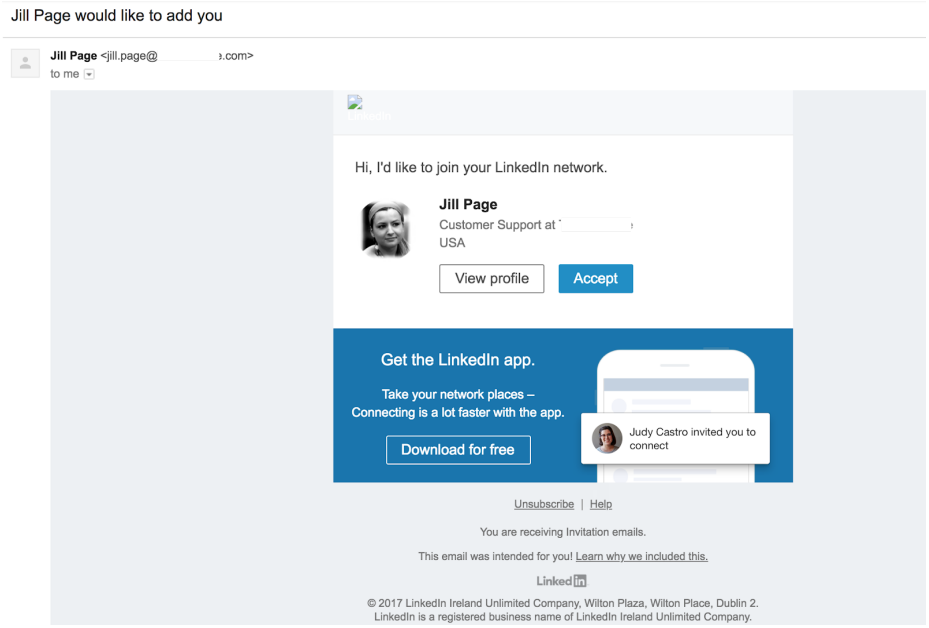
E-kirja loomisel kasutati autori sisendkausta tulnud e-kirja näidisena (esimene pilt). Kustutati personaliseeritud väljad ning muudeti isiklik e-kiri üldistatavamaks, mida saab kõikile inimestele saata. Tavaliselt on sellised e-kirjad personaliseeritud - minu nimi on pealkirjas ning samuti näitab minu kasutaja profiilipilti ja täisnime.



Joonis 9: LinkedIn originaalne e-kiri.

LinkedIn-i kalastuskirjas kustutati ära personaaliseeritud sõnumid ning asendati kontakti saatja väljad väljamõeldud isiku andmetega. Ametlik e-posti aadress, kust tulevad LinkedIn kontakti e-kirjad on: invitation@linkedin.com. Antud juhul kasutati ettevõtte nimele sarnast domeeni ning kasutades väljamõeldud isikut, Jill Page.

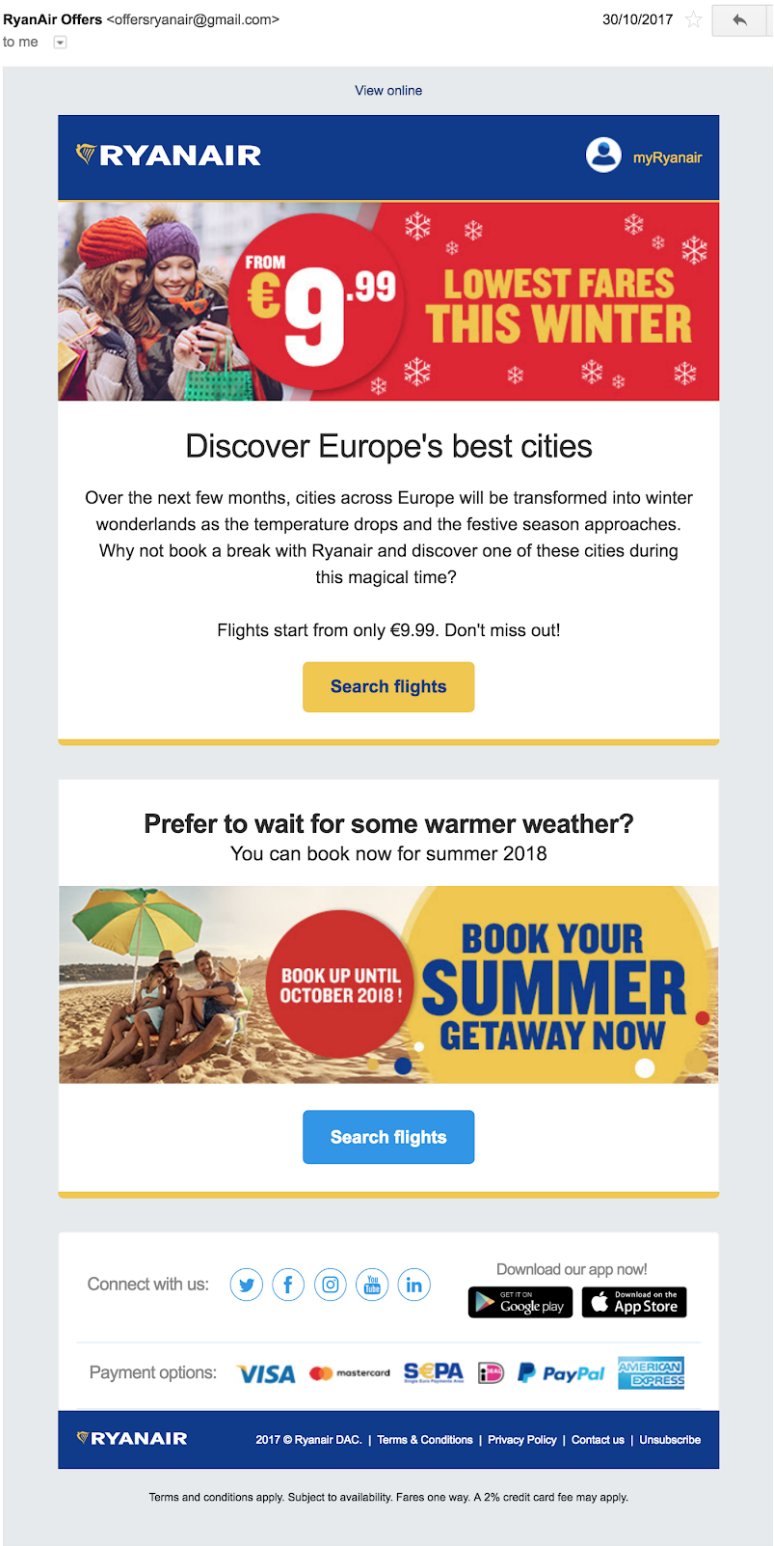
Autentse LinkedIn e-kirjaga võrreldes on katse käigus loodud kalastuskirjas muudetud saatja e-posti aadressi, eesnimi pealkirjas on eemaldatud ning personaliseeritud andmed kustutatud. Kõik klõpsatavad hüperlingid ja pildid on muudetud nii, et suunavad küsimustikku.



Joonis 10: LinkedIn kalastuskiri.

RyanAir e-kiri

Võeti autori e-posti sisendkaustast üks RyanAir reklaamipakkumine ning asendati kõik hüperlingid küsimustiku hüperlingiga. Antud kalastuskirja puhul peaksid ohvrid aru saama, et see e-kiri on saadetud tavaliselt Google Gmail kontolt. Samuti enamus töötajad ei telli uudiskirju ega sooduspakkumisi enda töö e-posti kontole.



Joonis 11: RyanAir kalastuskiri

4.4 Kalastusrünnaku läbiviimine

GoPhish nõudis e-kirjade saatmiseks saatja nime, saatja e-posti aadressi, saatja e-posti konto parooli, meiliserveri IP aadressi ning saajate e-posti aadresse.

Katses olevate e-postide jaoks, kasutati kahte teenust: GoDaddy, mis on veebilehtede edasimüüja, kaudu renditi ettevõtte nimele sarnane domeen ning domeenile loodi kaks e-posti kontot Microsoft Office poolt (jill.page@, rasmus.kalgpere@). Teised e-posti kontod lõin läbi Google Gmaili teenuse (peterstoner4@gmail.com, offersryanair@gmail.com).

Eesmärk oli saatja e-posti kontod muuta vaikimise lubatuks, et nendelt tulevaid kirju ei blokeeritaks. Ettevõtte IT haldur tegi seda ettevõtte e-posti sätetes, et e-kirjad ei oleks märgitud rämpspostina. Pärast seadistamist saadeti kõik e-kirjad samaaegselt välja. Hoolimata seadistusest läks ligikaudu 75% e-kirjadest rämpsposti kaustadesse ning katse polnud nii efektiivne kui alguses loodeti.

4.5 Ettevõtte töötajate teavitamine

Kolm päeva pärast e-kirjade laiali saatmist, anti asutusesiseses suhtluskanalis kõigile teada, et tegemist oli testiga. Leidus töötajaid, kes avasid ning vajutasid hüperlinkidele pärast teavitust. Intsident näitas, et info ei pruugi kõikideni jõuda ning ohvreid võib tekkida ka pärast ründe tuvastamist. Kaks nädalat pärast e-kirjade saatmist sai saadetud kõikidele töötajatele e-kiri, kus selgitati, et tegemist oli asutusesisese katsega ning anti lühike ülevaade, mida antud katsega välja selgitati.

Hey all!

DL;TR

- We had an **internal phishing attack/test** 2 weeks ago
- The link was clicked on 20% of opened emails, which was a super indicator for us to start making improvements on!
- During a real attack, it would've been shut down very quickly and probably prevent further clicks.

gophish

Longer version
As most of you **should** be aware by now, we had an **internal phishing attack/test** around 2 weeks ago. I took part in sending out those under the leadership of our ICO.
The main focus was to see how well prepared we are (as a company) when a real attack occurs. Here are more details about it.

Statistics:

- We sent around 1300 emails
- Around 75-80% went to spam (sadly)
- 168 emails were opened (that were not in spam)
- Almost 20% people clicked a link in that phishing email
- The quickest reaction was posted in Slack 7 minutes after the emails were sent out
- Around 75% of the clickers would be interested a security session regarding this
- We used different @gmail.com emails (ryanairoffers, peterstoner4 etc.)
- Also used custom domain @ (jill.page, rasmus.kalgpere)

Joonis 12: E-kiri töötajatele katse tulemustest.

4.6 Tulemused ja analüüs

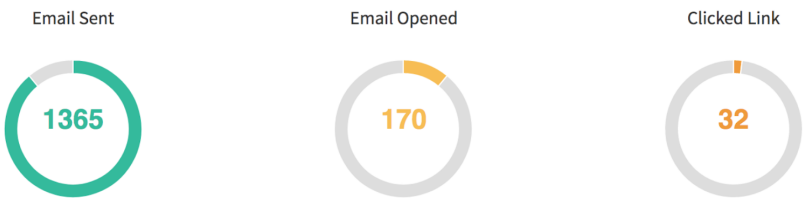
- Saadeti umbes 1300 e-kirja
- 75-80% e-kirjadest märgiti rämpspostiks
- 168 e-kirja avati
- Umbes 30 korda vajutati e-kirja sees olevale hüperlingile
- Esimene sõnum töötajalt saabus 7 minutit pärast e-kirjade väljasaatmist
- Kasutati nelja erinevat e-posti aadressi

Täpne põhjus, miks sedavõrd palju e-kirju märgiti Google Gmail-i poolt rämpspostina, on teadmata. Arvatavasti e-posti aadressite lubamine ettevõtte meiliserverites polnud piisav ning Google Gmail filtrid suutsid kiirelt tuvastada kahtlase tegevusega seotud e-posti aadressid. Samuti võisid töötajad saadud e-kirju Google Gmail keskkonnas raporteerida kalastuskirjana.

Pärast esimest töötaja poolt kirjutatud hoiatussõnumit hakkasid inimesed vähem e-kirju avama, teavitama IT ning turvameeskonda. Leidus ka töötajaid, kes ei lugenud sisemiselt suhtluskanalilt, et töötajaid rünnatakse kalastuskirjadega ning endiselt lugesid kalastuskirju. IT meeskond kinnitas, et tegelikkuses selline rünnak suudetakse loetud minutitega tuvastada ning

kinni panna, kustutades kõik rünnakuga saadetud e-kirjad. Antud katse jaoks oli tehtud kokkulepe, mille raames üritati kalastuskirju võimalikult kaua töötajate postkastides hoida.

Järgnev joonis on võetud GoPhish rakendusest, mis annab ülevaate saadetud e-kirjadest - mitu neist avati ning mitmel avatud e-kirjal vajutati hüperlingile.



Joonis 13: Eksperimendi käigus saadetud e-kirjade ülevaade.

Kuna sihtgrupid olid jagatud rühmadesse, siis oli rakenduses võimalik näha meeskondade järgi kui efektiivsed teatud e-kirjad olid. Joonisel 14 on välja toodud, mida võis kasutatud rakenduses näha.

Finance&Banking / Marketing / RYANAIR	October 31st 2017, 1:11:24 pm	46	36	6

Joonis 14. GoPhish statistika - sihtgrupp ning e-kirja tüüp, kuupäev, saadetud e-kirjad, avatud e-kirjad ning hüperlinkidele vajutamised.

Tagasiside töötajatelt, kes avasid e-kirjas oleva hüperlingi

Küsimustikule vastas ligikaudu 75% inimestest, kes avasid hüperlingi. Tagasiside küsimuste koostamisel pidasin nõu ettevõtte turvaeksperdiga, et saada head ülevaadet põhjustest miks inimesed hüperlingile vajutasid ning kuidas seda tulevikus ennetada.

Küsimused:

- Miks te vajutasite hüperlingile?
- Kas te kontrollisite ettevõtte sisemist suhtluskanalit või küsisite IT käest nõu enne e-kirja avamist?

- Kas te vahepeal tundsite, et antud e-kirja kohta oleks pidanud teavitama ISO või IT-d?
- Kas te oleksite huvitatud antud teemal toimuvast asutusesisesest koolitusest?

Miks vajutati hüperlingile?

24st vastajast 13 arvasid, et tegemist on usaldusväärse hüperlingiga ning 11 andsid järgnevaid põhjuseid:

- Nägin, et tegemist on e-kirjaga kliendilt ning kui ma selle avasin, sain aru, et tegemist on kalastuskirjaga, kuid ma eeldan, et see oli juba liiga hilja.
- Tegin hüperlingi lahti ja panin kohe kinni.
- Oli kiire ning ei olnud hoolikas.
- Kuna ma saan tööl olles üsna tihti kirju klientidelt enda e-posti aadressile või lausa Facebooki, siis ma ei osanud arvata, et tegemist on ohtliku e-kirjaga ning avasin selle.
- Mind huvitavad alati reisipakkumised, seega ma tahtsin täpsemat infot saada.
- Vajutasin nuppu "unsubscribe", kuna ma vihkan neid spam e-kirju.
- Tundus olevat seotud kliendi probleemiga, kuigi hetk hiljem sain ma aru, kui suure eksimuse ma tegin.

Kas te kontrollisite sisemist suhtluskanalit või küsisite IT käest nõu enne e-kirja avamist

24st vastajast 22 ei kontrollinud ega küsinud nõu enne e-kirja avamist.

Kas te vahepeal tundsite, et antud e-kirja kohta oleks pidanud teavitama ISO või IT-d?

14 vastasid "jah" ning 10 "ei".

Kas te oleksite huvitatud asutusesisesest koolitusest antud teemal?

18 töötajat oleksid huvitatud koolituses ning 6 ei ole.

Katse sooritamise ajal oli tegu tavalise tööpäevaga, seega e-kirjad, mis töötajad said võisid olla välise saatja poolt saadetud. Küsitluse vastuste põhjal tundub, et kas inimesed polnud piisavalt keskendunud või nad ei osanud näha nendes e-kirjades ohtu. Ettevõttes tehakse sarnaste rünnete

ärahoidmiseks treeninguid ning kõik töötajad peaksid tegelikkuses kursis olema, mida sellises olukorras teha. Antud käitumine töötajate poolt võib kunagi ettevõttele ohtlikult mõjuda, kuid selle katsega püüame tõsta töötajate teadlikkust antud teemal.

4.7 Järeldus

Antud asutusesisene turvalisuse test oli esimene, kus saadeti töötajatele e-kirju, et testida nende teadlikkust turvalisusest. Kuna ettevõttes tehakse iga-aastaseid turvalisuse koolitusi ning kontrollitakse teadmisi selle kohta, siis see eksperiment oli ideaalne võimalus panna töötajate teadmised proovile. Antud katse jaoks pandi püsti virtuaalne keskkond ning kasutades avatud lähtekoodiga rakendust saadeti kõikidele töötajatele kalastuskirju. Erinevat stiili e-kirjad meelitasid erinevaid inimesi ning kõikidel loodud e-kirjadel oli vähemalt keegi, kes avas selle e-kirja ning klõpsis e-kirjas olnud hüperlingile.

Eksperimendi tegemise ajal töötas asutuses umbes 700 töötajat, kelle seast avasid e-kirja umbes 160. Nende seast omakorda 20% vajutasid mõnele hüperlingile. Tegelikkuses piisab ründajal ainult ühest e-kirjast, mille hüperlink avatakse. Sooritatud katsega avati ligikaudu 30 hüperlinki, mis annab ettevõttele head infot, et turvalisust tõsta.

Kuna ettevõttel on ligikaudu 2 miljonit kasutajat, siis nende andmete kaitsmine on asutusele väga tähtis. Kui andmed peaksid lekkima, siis klientide usaldus ettevõtte vastu kahaneks ning ettevõtte väärtus kukuks, mis annaks konkurentidele eelise.

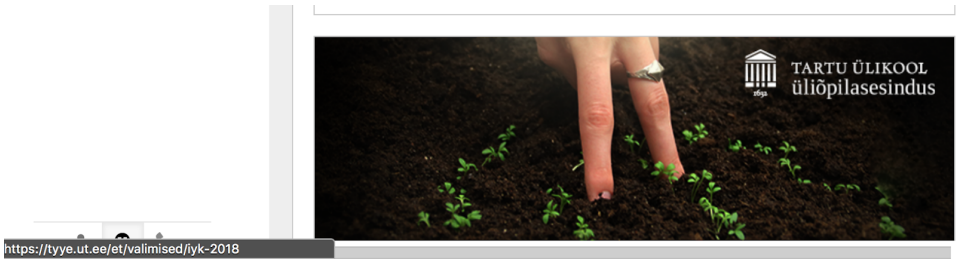
Olenemata sellest, et ettevõttes on turvalisus väga kõrgel kohal, siis leidub alati midagi, mida töötajatele õpetada turvalisuse kohta ning just säärased testid annavad asutuse turvaekspertidele häid näiteid selle kohta, mis on ettevõttes nõrgad kohad.

5. Kuidas vältida rünnaku ohvriks sattumist?

Antud peatükis toon välja erinevaid viise, kuidas saab kasutaja potentsiaalse rünnaku ära tunda ning vältida ohvriks sattumist. Üks turvalisemaid viise on avada kahtlaseid e-kirju isoleeritud virtuaalmasinas, kuna kahjurvara korral ei juhtu päris arvutiga midagi ning vajaduse korral on võimalik virtuaalmasina olek ära kustutada. Virtuaalmasin ei kaitse rünnakute eest, kus kasutaja sisestab ise midagi, seega järgnevate soovituste abil püüan tõsta kasutajate teadlikkust. Samuti ei ole kõigil töötajatel virtuaalmasina kasutamise võimalust.

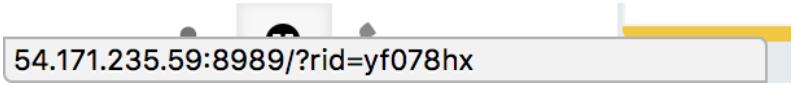
Vaata, aga ära vajuta linkidele [45]

Hõljudes hiirega linkide kohal, näitab veebilehitseja antud hüperlinki lehe allosas. Sedasi saab kindlaks teha, kas tegemist on usaldusväärse veebilehega ning kui tegemist on tundmatu hüperlingiga, siis parem on sellele mitte vajutada. Samuti võib hüperlink välja näha väga sarnane, näiteks LinkedIn.com ning Linkedln.com on hetkel kaks erinevat veebilehekülge, kuid peale vaadates näevad need sarnased välja - teisel hüperlingil on kasutatud suure ‘i’ tähe asemel väikest ‘l’ tähte. Seega peab olema väga tähelepanelik ning võimalusel kasutama virtuaalmasinat hüperlinkidele vajutamisel.



Joonis 15: Hõljudes hiirega pildil on näha hüperlinki, kuhu pilt suunab.

Eksperimendis kasutatud hüperlinkidel ning piltidel hõljudes oli näha, et pildi sisu ei sobitu aadressiga, millele see viitab.



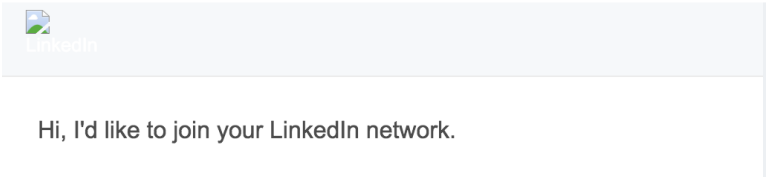
Joonis 16: Hõljudes hiirega hüperlinkidel/piltidel eksperimendis olnud e-kirjadel.

Kirjavead [45]

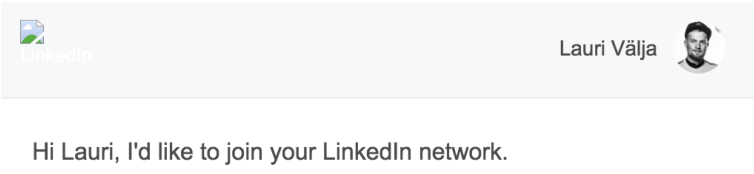
Ettevõtted on enemasti e-kirju saates väga hoolikad. Usaldatavad e-kirjad tavaliselt ei sisalda suuri kirjavigu või kehva grammatikat, seega tasub lugeda e-kirja hoolikalt ning vigade nägemisel suhtuda antud e-kirja skeptiliselt.

E-kirjas pöördumine kasutaja poole [45]

Korrektsetes e-kirjades pöördutakse enamjaolt saaja poole personaalselt kasutades ees- ning perekonnanime. E-kirjad, kus kasutatakse üldistatud pöördumist, näiteks "Tere austatud klient" võib tähendada, et tegemist on kalastuskirjaga, mis on saadetud paljudele inimestele.



Joonis 17: Eksperimedi käigus koostatud LinkedIn e-kirja kontakti kutse.



Joonis 18: Autentne LinkedIn kontakti kutse.

Ära jaga personaalseid andmeid e-kirja teel [45]

Pangad ning enamus teisi ettevõtteid ei küsi personaalset infot e-kirja teel. Enne personaalse info jagamist tuleks teha kindlaks, kas saatjaks on see, kellena ta esineb. Selleks saab helistada näiteks panka ning kontrollida, kas tegemist on nende poolt saadetud e-kirjaga.

Ära usu kõike, mida sa e-kirjas näed [45]

Kalastuskirja koostajad on enamjaolt heade oskustega. Tihti suudetakse teha väga veenev e-kiri ning on raske ära näha, kas tegemist on ohtliku e-kirjaga. E-kirjade puhul peab alati olema skeptiline ning kui see näeb välja vähemalgi määral kahtlane, siis ei tasu seda avada.

Saatja aadress ja e-kirja sisu võrdlus

E-kirja sees kasutatud hüperlingid peaksid sobima kokku saatja domeenidega. Kui reklaam@selver.ee saadab e-kirja erinevate piltide ning hüperlinkidega, siis nendel hiirega hõljumisel peaksid need olema selver.ee'ga seotud. Saades e-kirja selver.ee domeenilt, kuid hüperlingid on seotud näiteks mõne panga nimega, siis see on selge märk, et midagi on valesti.

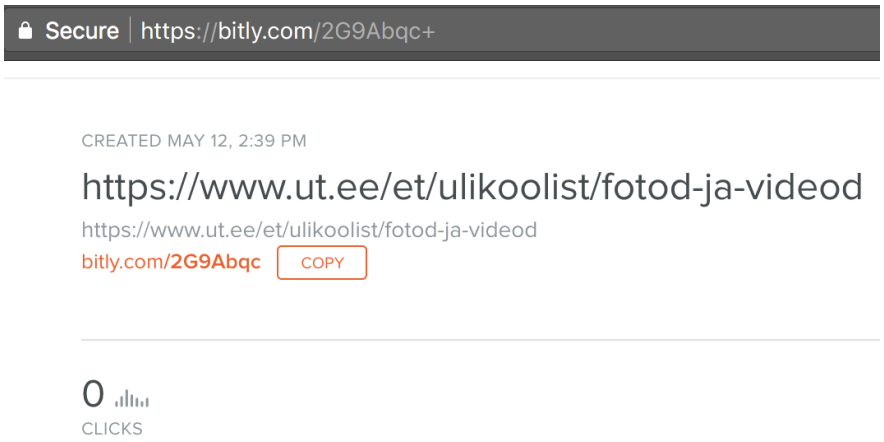
Lühendatud hüperlingid

Lühendatud hüperlingi teenus TinyURL loodi 2002. aastal Kevin Gilbertson poolt [46]. Teenuse eesmärk on võtta pikad domeenid nagu näiteks https://www.ut.ee/et/ulikoolist/fotod-ja-videod, muutes selle lühemaks https://tinyurl.com/y9bhfcpa ning lõpuks viitavad mõlemad samale allikale [47]. Lühendatud hüperlinkidega kaasneb ka turvalisuse risk - kasutaja tegelikult ei tea kuhu lühendatud hüperlink viitab ning sedasi saab ründaja varjata ohtlikku veebilehte [48].

2016. aasta John Podesta kalastuskirja juhtumis kasutasid ründajad Bitly poolt lühendatud hüperlinki, et varjata pahatahtlikku veebilehte, mis varjas järgmist hüperlinki [49]:
http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ==&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg==.
Kasutajale jääb küllap silma *myaccount.google.com*, kuid tegelikult oli domeeniks *com-securitysettingpage.tk*. Sellisest domeeni varjamisest on kirjutatud "Domeeni hierarhia kontroll" peatükis [49]. Kui poleks kasutatud Bitly teenust, siis oleks arvatavasti Google Gmail antud e-kirja automaatselt märkinud kalastuskirjaks.

Lühendatud hüperlinkide kontrollimiseks on erinevaid meetodeid. Erinevad teenusepakkujad omavad nende poolt loodud lühendatud hüperlinkide kohta statistikat. Näiteks Bitly ning Google

puhul on vaja lisada hüperlingi lõppu “+”, tiny.cc puhul lisada lõppu “=” ning tinyURL kontrollimiseks on vaja lisada “preview.” domeeni algusesse.



Joonis 19: Bitly lühendatud lingi sisu kontroll ning peale vajutamiste arv [50].

Joonis 20: TinyURL lühendatud hüperlingi sisu kontroll [51].

Teine viis saada lühendatud hüperlingi kohta informatsiooni on näiteks teenus CheckShortURL, mis teeb lühendatud hüperlingist tervikliku [52]. Samuti on teenuseid, mis kontrollivad hüperlinkide sisu ning annavad kasutajale teada, kas tegemist on usaldusväärse lehega, näiteks VirusTotal [53].

Lühendatud hüperlinkide puhul peab olema kasutaja teadlik, kas antud hüperlink pärineb usaldatavast allikast ning kui allikas on tundmatu, siis on kindlam seda mitte avada või kontrollida eelmainitud meetoditega.

QR-koodide kontrollimine

QR-kood on kahe-dimensiooniline triipkood, mida saab skännida kasutades nutitelefoni või veebikaamerat [54]. QR-kood sarnaneb lühendatud hüperlingile, kuna koodi vaadates ei saa kasutaja aru, mis veebilehega on tegemist. Enne QR-koodis oleva veebilehe avamist tuleb hinnata selle allikat, asukohta ning veebilehte. Ründajad võivad ohtlikke QR-koode kleepida tänavatel olevatele plakatitele, saata e-kirju, mis sisaldavad QR-koodi ning seega kasutaja peab olema tähelepanelik enne koodi avamist.

Joonis 21: QR-kood, mis suunab Tartu Ülikooli pealehele.

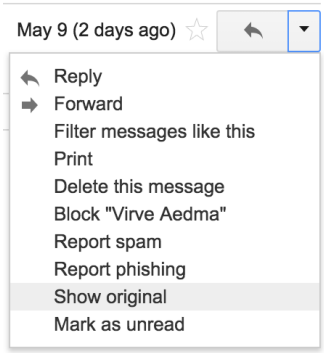
E-kirja metainfo

Kõik e-kirjad sisaldavad metainfot, mis sisaldab täpset informatsiooni konkreetse e-kirja kohta. Info sisaldab [55]:

- saatja e-post aadressi või nime
- saaja e-post aadressi
- Pealkirja
- Kuupäeva, millal e-kiri saadeti
- Meiliserver kust e-kiri pärines
- E-posti aadress, kuhu e-kiri vastuse korral tagasi saadetakse

Eelnevat infot ära kasutades saab kasutaja selgeks teha, kas tegemist on usaldusväärse e-kirjaga. Enamjaolt tuleks kontrollida e-posti aadressi, kuhu e-kiri vastuse korral saadetakse ning kui see ei klapi saatja e-posti aadressiga, siis on potentsiaalselt tegemist kolmanda isikuga.

Google Gmail e-kirjas saab vaadata metainfot, kui pärast e-kirja avamist vajutada menüü noolekese peal ning valida “Show original”



Joonis 22: Google Gmail e-kirja menüü.

Domeeni hierarhia kontroll

Ründajad loovad tihti panga hüperlingile sarnaseid hüperlinke kasutades ära domeeni hierarhiat. Näiteks www.swedbank.ee.142.com võib esmapilgul näida, kui Swedbank-i hüperlink, kuid tegelikkuses hüperlingiks on *142.com*, kus *swedbank.ee* on selle alamdomeen. Kasutaja peab jälgima tähelepanelikult kus on üladomeen (.com, .ee, .net, .org) ning mis eelneb sellele.Sedasi on võimalik selgeks teha, mis domeeniga on tegu. Domeeni hierarhiat tuleb lugeda paremalt vasakule, kusjuures paremal on hierarhia kõrgem. Kalastuskirjade puhul kasutatakse sarnast tehnikat, et näida usaldusväärse saatjana.

Joonis 23: E-kiri example.com domeenilt, mis pole tegelikult LinkedIn teenusega seotud [55].

Ei tohi kõike uskudas, mida e-kirjas nähakse [45]

Kalastuskirja koostajad on valdavalt heade oskustega. Tihti suudetakse teha väga veenev kalastuskiri, mille puhul on raske ära näha, kas tegemist on ohtliku e-kirjaga. Kasutaja peab tundmatute e-kirjade puhul alati olema skeptiline ning kui see näeb vähemalgi määral kahtlane välja, siis ei tasu seda avada.

6. Kokkuvõte

Käesoleva töö eesmärkideks oli tutvustada kalastusrünnetega seotud probleeme, anda ülevaade tehnoloogiatest, mis võimaldavad ründeid vähendada ning uurida ühe konkreetse ettevõtte teadlikkust õngitsusrünnetest.

Esimeseks eesmärgiks oli tutvustada kalastusrünnetega seotud probleeme. Töös kirjeldati, kui aktuaalseks probleemiks on manipuleerimisründed, mille üheks alamkategooriaks on kalastuskirjad. Antud rünnete populaarsus üha kasvab, seega uuritakse töö käigus täpsemalt, mis seda põhjustab ning kui lihtne on kalastusründe ohvriks sattuda.

Teiseks eesmärgiks oli anda ülevaade tehnoloogiatest, mille käigus kirjendati e-kirjade saatmise protsessi, e-kirjade turvalisust ning milliseid meetodeid kasutatakse e-kirjade turvalisuse tõstmiseks. Toodi välja erinevate turvameetodite (SPF, DKIM) seadistamise soovitusi, probleeme ning kuidas ründajad neid ära kasutavad.

Kolmandaks eesmärgiks oli uurida tehnoloogiaettevõtte teadlikkust õngitsusrünnetest. Selle jaoks viidi läbi eksperiment ettevõttes, kus töötajatele saadeti autori poolt koostatud kalastuskirju. Inimesed, kes avasid kalastuskirja ning klõpsasid selle sees olevale lingile vastasid koostatud küsimustikule, millega lükati ümber püstitatud hüpotees. Eksperimendi tulemusel selgitati välja, mida peab ettevõte tegema, et tõsta töötajate teadlikkust manipuleerimisrünnete kohta.

Töös antakse lugejale mitmeid soovitusi, millele peab tähelepanu pöörama, et kalastusrünnaku ohvriks mitte sattuda. Soovitustes tuuakse välja probleeme, mis on seotud lühendatud hüperlinkide, QR-koodide, domeeni nimetuste, e-kirja stiiliga jms. Samuti töö eksperimendi koostamise käigus valmis infrastruktuur, mis võimaldab analoogset katset vajaduse korral tulevikus korrata.

7. Viidatud kirjandus

[1] *World Internet Users and 2018 Population Stats*. (2018). https://www.internetworldstats.com/stats.htm (7.05.2018)

[2] *Email Statistics Report, 2018 – 2022*. (2018). https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf (7.05.2018)

[3] Breach Level Index. https://breachlevelindex.com/ (7.05.2018)

[4] *Number of sent and received e-mails per day worldwide from 2017 to 2022*. (2017). https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/ (25.04.2018)

[5] Jonathan Crowe. (2017). *Must-Know Phishing Statistics 2017*. https://blog.barkly.com/phishing-statistics-2017 (17.02.2018)

[6] D. Gudkova, M. Vergelis, T. Shcherbakova, N. Demidova. (2018) *Spam and phishing in 2017*. https://securelist.com/spam-and-phishing-in-2017/83833/ (25.04.2018)

[7] Tara Seals. (2016). *Spear Phishing Incident Average Cost is $1.6M*. https://www.infosecurity-magazine.com/news/spear-phishing-incident-average/ (25.04.2018)

[8] Federal Bureau of Investigation. (2017). *Business E-mail compromise, E-mail account compromise, the 5 billion dollar scam.* https://www.ic3.gov/media/2017/170504.aspx (7.05.2018)

[9] Karina Filipczak (2018). https://cmserv.cs.ut.ee/ati_thesis/datasheet.php?id=60626&year=2018 (10.05.2018)

[10] Jakob Nielsen. (2000). *Security & Human Factors*. https://www.nngroup.com/articles/security-and-human-factors/ (25.04.2018)

[11] Nate Lord. (2015). *Social Engineering Attacks: Common Techniques & How to Prevent an Attack.* https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack (17.02.2018)

[12] US-CERT Publications. (2009). *Avoiding Social Engineering and Phishing Attacks.* https://www.us-cert.gov/ncas/tips/ST04-014 (17.02.2018)

[13] Ray Pompo. (2017). *Phishing for information, part 2: How attackers collect data about your employees.* https://f5.com/labs/articles/threat-intelligence/identity-threats/phishing-for-information-part-2-how-attackers-collect-data-about-your-employees (7.05.2018)

[14] Pipl. (2006). https://pipl.com/ (7.05.2018)

[15] Wombat Security Technologies (2017). *State of Phish 2017.* https://info.wombatsecurity.com/hubfs/State%20of%20the%20Phish%202017/Wombat%20State%20of%20the%20Phish%202017.pdf (13.05.2018)

[16] Marika Samarati. (2017). *6 reasons why phishing is so popular and successful.* https://www.itgovernance.co.uk/blog/6-reasons-phishing-is-so-popular-and-so-successful/ (17.02.2018)

[17] Jonathan Crowe. (2016). *Phishing by the Numbers: Must-Know Phishing Statistics 2016.* https://blog.barkly.com/phishing-statistics-2016 (17.02.2018)

[18] D. Gudkova, M. Vergelis, T. Shcherbakova, N. Demidova. (2017). *Spam and phishing in Q3* 2017 https://securelist.com/spam-and-phishing-in-q3-2017/82901/ (17.02.2018)

[19] CoinMarketCap. *Total Market Capitalization* https://coinmarketcap.com/charts/ (13.05.2018)

[20] Margaret Rouse. (2005). *E-mail (electronic mail or email)*. https://searchexchange.techtarget.com/definition/e-mail-electronic-mail-or-email (10.12.2017)

[21] The Centre for Computing History. *First Network Email sent by Ray Tomlinson.* http://www.computinghistory.org.uk/det/6116/First-e-mail-sent-by-Ray-Tomlinson/ (7.05.2018)

[22] Margaret Rouse. (2006). *Mail server (mail transfer/transport agent, MTA, mail router, Internet mailer)* https://searchmicroservices.techtarget.com/definition/mail-server-mail-transfer-transport-agent-MTA-mail-router-Internet-mailer (17.02.2018)

[23] Yatri Trivedi. (2016). *How Does Email Work?* https://www.howtogeek.com/56002/htg-explains-how-does-email-work/ (10.12.2017)

[24] Microsoft Office 365. *What are IMAP and POP?* https://support.office.com/en-us/article/what-are-imap-and-pop-ca2c5799-49f9-4079-aefe-ddca85d5b1c9 (7.05.2018)

[25] interServer.net. *Exactly How Emails Works – Steps and Explanation*. https://www.interserver.net/tips/kb/exactly-emails-works-steps-explanation/ (10.12.2017)

[26] Statista. (2017). *Global spam volume as percentage of total e-mail traffic from January 2014 to September 2017, by month.* https://www.statista.com/statistics/420391/spam-email-traffic-share/ (7.05.2018)

[27] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey, J. A. Halderman. (2015). *Neither Snow Nor Rain Nor MITM… An Empirical Analysis of Email Delivery Security* http://conferences2.sigcomm.org/imc/2015/papers/p27.pdf (10.12.2017)

[28] Matt Moorehead. (2015). *How to Explain SPF in Plain English.* https://blog.returnpath.com/how-to-explain-spf-in-plain-english/ (10.12.2017)

[29] Google Support. *About SPF records*. https://support.google.com/a/answer/33786?hl=en (10.12.2017)

[30] DNS Made Easy. (2016). *TXT Record*. http://help.dnsmadeeasy.com/managed-dns/records/txt-record/ (10.12.2017)

[31] Brian Marshall, Stephanie Crawford. *How Domain Name Servers Work.* https://computer.howstuffworks.com/dns.htm (10.12.2017)

[32] MX Toolbox. https://mxtoolbox.com/SuperTool.aspx? (7.05.2018)

[33] John Leyden. (2004). *Spammers embrace email authentication*. http://www.theregister.co.uk/2004/09/03/email_authentication_spam/ (10.12.2017)

[34] Ian Chard. (2014). *Why is email being delivered normally despite an SPF "hardfail"?* https://serverfault.com/questions/580278/why-is-email-being-delivered-normally-despite-an-spf-hardfail (10.12.2017)

[35] Julian Mehnle. (2008). *SRS: Sender Rewriting Scheme*. http://www.openspf.org/SRS (10.12.2017)

[36] Valimail. (2016). *Two Common Problems with SPF You're Probably Overlooking*. https://www.valimail.com/blog/two-common-problems-with-spf-youre-probably-overlooking/#.559ydxps4 (10.12.2017)

[37] https://returnpath.com/blog/spf-common-problems-and-solutions/ (10.12.2017)

[38] John Thies. (2017). *What is DKIM? Everything You Need to Know About Digital Signatures*. https://www.emailonacid.com/blog/article/email-development/what_is_dkim_everything_you_need_to_know_about_digital_signatures (12.05.2018)

[39] dkim.org. *DomainKeys Identified Mail* (DKIM). http://www.dkim.org/ (10.12.2018)

[40] Google Support. *Authenticate email with DKIM*. https://support.google.com/a/answer/174124?hl=en (13.05.2018)

[41] Bpm online academy. (2018). *General recommendations on SPF and DKIM record setup*. https://academy.bpmonline.com/documents/marketing/7-12/general-recommendations-spf-and-dkim-record-setup (7.05.2018)

[42] Larry Seltzer. (2013). DKIM: *Useless or just disappointing*? https://www.zdnet.com/article/dkim-useless-or-just-disappointing/ (10.12.2017)

[43] GoPhish https://getgophish.com/ (10.12.2017)

[44] Slack. https://slack.com/

[45] Estelle Derouet. (2015). 10 *Tips on How to Identify a Phishing or Spoofing Email*. https://blog.returnpath.com/10-tips-on-how-to-identify-a-phishing-or-spoofing-email-v2/ (10.05.2018)

[46] Margaret Rouse. (2017). *URL shortening*. https://whatis.techtarget.com/definition/URL-shortening (10.05.2018)

[47] TinyURL https://tinyurl.com/ (10.05.2018)

[48] Panda Security. (2016). https://www.pandasecurity.com/mediacenter/security/shortened-urls/ (10.05.2018)

[49] Jeremy Ashkenas. (2017). *Was It a 400-Pound,14-Year-Old Hacker, or Russia? Here's Some of the Evidence.* https://www.nytimes.com/interactive/2017/01/06/us/russian-hack-evidence.html (12.05.2018)

[50] Bitly. https://bitly.com/ (12.05.2018)

[51] TinyURL. http://tinyurl.com/ (10.05.2018)

[52] CheckShortURL. http://checkshorturl.com/ (10.05.2018)

[53] VirusTotal. https://www.virustotal.com/#/home/upload (10.05.2018)

[54] QR Code Generator. *What is a QR Code?* https://www.the-qrcode-generator.com/whats-a-qr-code (10.05.2018)

[55] Unichange. (2018). *Phishing emails: How to check email headers.* https://unichange.me/articles/check_email_header (10.05.2018)

[56] Proofpoint. (2017). *Snowshoe Spamming Brings Scale to Savvy Subdomain Phishing Attacks.* https://www.proofpoint.com/us/threat-insight/post/snowshoe-spamming-brings-scale-savvy-subdomain-phishing-attacks (10.05.2018)

Litsents

Lihtlitsents lõputöö reprodutseerimiseks

Mina, Lauri Välja,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
Kalastuskirjade ohtlikkus tehnoloogiaettevõtte näitel,

mille juhendaja on **Kristjan Krips**,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu alates **01.06.2020** kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud reprodutseerimise õigus jääb alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **13.05.2018**