UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Karina Magdalena Filipczak

Testing the Security Awareness using Open-Source Tools: Spear Phishing

Master's Thesis (30 ECTS)

Supervisors:
Sten Mäses
Raimundas Matulevičius

Tartu 2018

Testing the Security Awareness using Open-Source Tools - Spear Phishing

Abstract:

The psychological aspect of a human and the flaws of modern day technology are the lead culprits to the success and longevity of phishing. This case study is set to test the waters and identify weak spots of digital security in one of the biggest fintechs of Estonia. Using AWS and open-source tools like Nginx and MySQL, a virtual environment was created within the company. To send out phishing emails, a phishing framework called GoPhish was used, and different scenarios were built to suit the psychological weaknesses of all the targeted departments. As the first attempt of the phishing within the company, it has been made aware of its security weaknesses and how to target potential attacks with more due-diligence approach in the future. The outcome of the study clearly demonstrated the gap between human and technological cooperation in fighting against spear phishing, which leaves the room for future improvement. Almost 70% of the emails ended up tagged as "spam" without reaching the victims, which posed a greater limitation to potentially higher results of the study. Nonetheless, the emails that went through hooked 20% of the staff. In comparison to Verizon Data Breach Investigations Report from 2016, mentioned throughout the course of the paper, the numbers of the affected staff were similar to the results of this case study. The main factors that could have jeopardized the validity of the findings are maturation of this very test, gmail filtering and experimenter bias. The future work for the company, based on the findings, is going to entail the enhancement of security awareness programmes as well as betterment of internal and universally-used external digital tools.

Keywords:

Spear phishing, security awareness, social engineering, gophish, emails, fintech, loss of sensitive data

CERCS: P170, Computer science, numerical analysis, systems, control

Turvateadlikkuse testimine avatud lähtekoodi vahenditega – suunatud andmepüük

Lühikokkuvõte:

Inimese psühholoogilised aspektid ning moodsa tehnoloogia vead on põhilised süüdlased, mille tõttu andmepüük on kuni tänapäevani edukalt toiminud. See uurimustöö on seatud üles pinna sondeerimiseks ning nõrkade lülide avastamiseks digitaalsetes turvasüsteemides ühes eesti suurimas FinTech firmas. Kasutades AWS-i ja avatud lähtekoodiga vahendeid nagu Nginx ja MySQL, seati antud firmas üles virtuaalne keskkond. Andmepüügi meilide väljasaatmiseks kasutati andmepüügi raamisitikku nimega GoPhish, millel ehitati üles erinevad stsenaariumid, eesmärgiga sobituda sihtmärgiks võetud osakondade psühholoogiliste nõrkustega. Olles esimene

firmasiseselt korraldatud andmepüük, tegi see firma teadlikuks turvanõrkustest ning sellest, kuidas võimalike tulevaste rünnakute suhtes hoolsuskontrolli suurendada. Uurimustöö tulemus näitas selgelt lünka inimese ning tehnoloogia koostöös suunatud andmepüügi vastu võitlemises, mis jätab arenguruumi tulevikus täiustamiseks. Pea 70% meilidest märgiti rämpspostina ning need ei jõudnud ohvriteni, mis piiras võimalikku suuremat tulemust uurimustöös. Sellele vaatamata oli andmepüük edukas 20% juhtudest, kus töötajad meili kätte said. Võrdluseks võib tuua Verizon Data Breach Investigations raporti aastast 2016, millele on antud uurimustöös korduvalt viidatud, kus mõjutatud töötajate arv oli sarnane uurimustöös leitule. Põhilised ohustajad antud uurimustöö kehtivusele on käsitletava testi valmimine, gmaili filtrid ning katse läbiviija erapooletus. Tulevane töö firma jaoks, mis põhineb uurimstöös leiitule, hõlmab turvateadlikkuse programmide suurendamist ning samuti firmasiseste ning -väliste digitaalsete tööriistade parendamist.

Võtmesõnad:

Suunatud andmepüük, turvateadlikkus, sotsiaalne manipuleerimine, gophish, meilid, fintech, tundlike andemete kaotus

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

Non-exclusive licence to reproduce thesis

I, _____Karina Magdalena Filipczak_____,
(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

reproduce, for the purpose of preservation, including for the purpose of preservation in the DSpace digital archives until expiry of the term of validity of the copyright

"Testing the Security Awareness using Open-Source Tools - Spear Phishing",
(title of thesis)

supervised by ___Sten Mäses, Raimundas Matulevičius___,
(supervisor's name)

2. Making the thesis available to the public is not allowed.

3. I am aware of the fact that the author retains the right referred to in point 1.

4. This is to certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, 10.01.2018