Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

Universität der Bundeswehr München
Institut für Softwaretechnologie

Untersuchung der Relevanz von Remindern für Phishingkampagnen unter Berücksichtigung der Absender-E-Mail-Adresse

Form der Arbeit / Form of this work:	Bachelorarbeit
Themenschwerpunkte / Main focus:	Phishing
Voraussetzungen / Prerequisites:	Grundkenntnisse IT-Sicherheit Grundkenntnisse Identitätsmanagement
Lehrstuhl für / Professorship for:	Prof. Dr. Wolfgang Hommel
Betreuung / Supervisor:	Dr. Daniela Pöhn

Hintergrund und Motivation / Background Information and Motivation

Phishing ist ein über alle Bereiche und Organisationen[1] weit verbreitetes Mittel zur Informationsgewinnung von vertraulichen Daten wie Passwörtern, um weiterführende Angriffe zielgerichtet auf einzelne Personen(kreise), vgl. Spear-Phishing oder Whaling, oder gegen die breiter Masse vorzubereiten. Hierbei wird versucht das Opfer beispielsweise mittels eines in der Mail eingebetteten Links auf eine zumeist vertrauenswürdig anmutende, aber entsprechend präparierte Webseite zu locken, um dort vertrauliche Daten abzugreifen[2].

Damit die Erfolgsaussichten möglichst hoch sind, muss der Inhalt einer Phishing-Mail täuschend echt erscheinen. Angreifer werden hierbei immer raffinierter und es ist selbst für besonnene und sicherheitsbewusste Menschen nicht immer auf den ersten Blick möglich, derlei Mails zu erkennen[3].

[1] `https://de.statista.com/statistik/daten/studie/150871/umfrage/am-haeufigsten-von-phishing-betroffene-organisationen/`, aufgerufen am April 6, 2022

[2] `https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html` und `https://www.avg.com/en/signal/what-is-phishing`, aufgerufen am April 6, 2022

[3] Vergleiche Clone-Phishing. Geiger, E., Studie zu den Erfolgsfaktoren von Phishing anhand eines Beispiels am Münchner Wissenschaftsnetz, Ludwig-Maximilians-Universität München, Dezember, 2014. `https://www.statista.com/statistics/881180/response-simulated-phishing-campaigns/`, `https://link.springer.com/chapter/10.1007/978-3-319-70278-0_39` und `https://www.sciencedirect.com/science/article/pii/S1071581918303628`, aufgerufen am April 6, 2022

Ziel dieser Arbeit ist die Untersuchung der Zuträglichkeit von "Remindern" für eine erfolgreiche Phishingkampagne. Dazu sollen verschiedene Möglichkeiten von Remindern identifiziert[4] hinsichtlich der Nutzbarkeit für Phishing analysiert und bewertet werden. Außerdem soll ein Konzept zur Erstellung von Studien zur Untersuchung der Wirksamkeit von Remindern u.ä. auf Phishingkampagnen entwickelt werden. Hierbei soll die Auswirkung der Verwendung von gleichen und unterschiedlichen E-Mail-Adressen berücksichtigt werden. Darauf aufbauend soll eine Studie konzeptioniert und durchgeführt werden, um eine Indikation für die sinnvolle Nutzung von Remindern unter Berücksichtigung der E-Mail-Adresse im Kontext von Phishing zu erhalten. Im Hinblick auf die Unterstützung einer erfolgreichen Phishingkampagne sollen zudem Domain Trustscores[5] analysiert und berücksichtigt werden[6]. Die Arbeit basiert auf einer bereits abgeschlossenen Bachelorarbeit.

Ziel der Arbeit / Goal of this Thesis

- Wie sind aktuelle Phishingkampagnen aufgebaut, vor allem im Bezug auf die Realisierung des Ziels?
- Welche technischen Methoden, Werkzeuge bzw. Frameworks sind im Rahmen von Phishingkampagnen zu deren Vorbereitung und Umsetzung nutzbar bzw. um nötige Aspekte im Rahmen der Aufgabenstellung erweiterbar?
- Konzeptionierung und Durchführung einer aufbauenden Studie zur Überprüfung der Wirksamkeit von Remindern unter Berücksichtigung der E-Mail-Adresse.
  - Beachtung rechtlicher und ethischer Grundsätze.
  - Kontextbezogenes Sammeln und Analysieren von Adressen usw. potentieller Probanden.
  - Vergleichende Bewertung verschiedener kontextbezogener Reminder.
  - Einbeziehung von Trustscores, damit Phishingmails potentielle Spamfilter bzw. Schutzmechanismen bypassen können.
  - Einbeziehung der Absender-E-Mail-Adresse.

[4] Bspw. im Kontext von Newslettern, Marketingaktionen oder Terminen.
[5] Hier: Welche Charakteristiken weisen typische Phishing Domains auf, wodurch diese potentiell erkannt und geblockt werden?
[6] Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails, ISBN: 9781118958476. `https://www.helpnetsecurity.com/2019/10/09/phishing-increase-2019/`, aufgerufen am April 6, 2022

Kontakt / Contact

Bei Problemen oder Fragen, nehmen Sie bitte Kontakt auf mit / If you have any problems or questions, please contact:

Adresse / Address: Cascada-Gebäude, Raum 2718
Tel. / Phone: +49 (0)89 6004 7356
E-Mail / Email: daniela.poehn@unibw.de