INFOBLATT

Phishing E-Mails

Phishing ist eine Art von Betrug, bei dem versucht wird, mit Hilfe von Werkzeugen (z.B. falsche Webseiten) persönliche Informationen der Benutzer zu stehlen, z.B. Anmeldedaten für den Zugang zu geschützten Systemen (Dhamija et al., 2006).

Meist werden gefälschten Webseiten via E-Mail an potentielle Opfer geschickt unter der Prämisse von Webshops oder Banken zu sein (Ma et al., 2009).

Es gibt verschiedene Arten von Phishing, die wichtigsten für Unternehmen sind Spoofed URL und Spear-Phishing.

Spoofed URLs werden meist per E-Mail oder SMS versendet (Aleroud & Zhou, 2017; Berghel et al., 2007). Es gibt hier verschiedenen Arten:

- Falscher Domain Name: http://onlinebanking.realbank.com
- Verkürzte URLs die zu einer gefälschten Domain führen: http://bit.ly/cikl0z
- Verschleierte URL: http://realbankS.com
- Verschleierte und codierte URL: http%3A%2F%2Frealbank.com+

Spear Phishing beschreibt gezielte Angriffe auf Organisationen und Firmen (Aleroud & Zhou, 2017; Berghel et al., 2007). Sie enthalten meist Logos oder Signaturen von bestehenden Menschen innerhalb der Organisation. Und sind damit mit hohem Aufwand verbunden. Sie sind dadurch auch schwierig zu erkennen, kommen oft „aus den eigenen Reihen“ und sind oft in Kombination mit Spoofing.

Prävention

Es gibt verschiedenen Methoden der Prävention gegen Phishing:

- Client-server authentication
- Honeypots
  - Fallen für Phishing mails
- Verschiedene Geräte zur Prävention/zum herausfiltern
  - (Aleroud & Zhou, 2017)
- Anti-virus Software (Berghel et al., 2007)
- Firewall/ IDS Blocker (Berghel et al., 2007)
- Anti-Spyware (Berghel et al., 2007)
- Anti-spam Filter (Berghel et al., 2007)

Detektion

Es gibt verschiedene Möglichkeiten der automatischen Detektion von Phishing:

- Machine Learning
  - Klassifizierung
  - Clustering
  - Anomalien Detektion
- Text mining

Da diese aber für KMUs meist unzugänglich sind, müssen die Mitarbeitenden die Phishing Attacken erkennen können und es sollte in der Prävention nicht gespart werden. Mitarbeitende sollten Trainings Angebote wahrnehmen, aufgeklärt werden und es sollte Zeit eingeräumt werden für das Lesen von E-Mails, da häufig auf gefährliche Links geklickt wird wenn man unter Zeitdruck steht.

Erkennung

Es gibt sechs Merkmale in Phishing Attacken, die darauf hinweisen können, dass es sich um eine Phishing E-Mail/Nachricht handelt.

- **Dringender Handlungsbedarf**: "Wenn Sie Ihre Daten nicht umgehend aktualisieren, dann gehen sie unwiederbringlich verloren“ (BSI, 2022)

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Phishing E-Mails

- **Drohungen**: „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren …" (BSI, 2022)
- Sie sollen vertrauliche Daten wie die PIN für Ihren Online-Bankzugang oder eine Kreditkartennummer eingeben (BSI, 2022)
- Die E-Mail enthält Links oder Formulare (BSI, 2022; Fette et al., 2007)
    - Die URL des Hyperlinks stimmt nicht mit der echten URL der Organisation überein (Fette et al., 2007; Singh et al., 2019)
    - Es sind mehrere Links in der Email enthalten (Fette et al., 2007; Ma et al., 2009)
- Die E-Mail scheint von einer bekannten Person oder Organisation zu stammen, die **E-Mail-Adresse** ist aber eine andere (BSI, 2022)
- Der Text hat kein bestimmtes Layout und/oder HTML (Fette et al., 2007)

Praxistest

Wenn Sie wissen möchten, wie gut Sie schon im Erkennen von Phishing E-Mail sind, stellen Sie sich dem Phishing-Quiz:
https://play.bakgame.de/PhishingQuiz/

Dieses Quiz wurde von dem Mittelstand-Digital Projekt „Bakgame" entwickelt um Ihnen zu helfen Phishing E-Mails noch besser zu erkennen.

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der *Initiative IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Referenzen

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Berghel, H., Carpinter, J., & Jo, J.-Y. (2007). Phish Phactors: Offensive and Defensive Strategies. In M. V. Zelkowitz (Hrsg.), *Advances in Computers* (Bd. 70, S. 223–268). Elsevier. https://doi.org/10.1016/S0065-2458(06)70005-5

BSI. (2022). *Wie erkenne ich Phishing-E-Mails und -Webseiten?* Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten.html?nn=132200

Button, M., & Cross, C. (2017). *Cyber Frauds, Scams and their Victims*. Routledge. https://doi.org/10.4324/9781315679877

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581–590. https://doi.org/10.1145/1124772.1124861

Fette, I., Sadeh, N., & Tomasic, A. (2007). *Learning to detect phishing emails | Proceedings of the 16th international conference on World Wide Web*. 649–656. https://doi.org/10.1145/1242572.1242660

Ma, L., Ofoghi, B., Watters, P., & Brown, S. (2009). *Detecting Phishing Emails Using Hybrid Features*. 493–497. https://doi.org/10.1109/UIC-ATC.2009.103

Singh, K., Aggarwal, P., Rajivan, P., & Gonzalez, C. (2019). Training to Detect Phishing Emails: Effects of the Frequency of Experienced Phishing Emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 453–457. https://doi.org/10.1177/1071181319631355

Stevens, G., Boden, A., Alizadeh, F., Jakobi, T., Walther, M., & Krüger, J. (2022). Wie gehen Verbraucher*innen mit Onlinebetrug um? – Eine Literaturübersicht. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Handbuch Cyberkriminologie—Band 2: Cybervictimologie*. Springer.

UK Fraud Act. (2006). *Fraud Act 2006* [Text]. Statute Law Database. https://www.legislation.gov.uk/ukpga/2006/35/contents

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages