Karlsruher Institut für Technologie

Bereich II – Informatik, Wirtschaft und Gesellschaft

Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)

NoPhish

Security Awareness Konzept: Schutz vor Phishing-E-Mails und anderen betrügerischen Nachrichten

Internetbetrüger nutzen verschiedene Strategien, um Personen, Unternehmen oder Einrichtungen zu schaden. Eine beliebte und weit verbreitete Methode besteht darin, diesen Nachrichten mit gefährlichen Inhalten zu schicken. Dabei können die Nachrichten auf unterschiedliche Art und Weise gefährlich sein. Die Nachricht kann die Empfängerin oder den Empfänger auffordern, Überweisungen vorzunehmen oder (kostenpflichtige) Anrufe zu tätigen. Sie kann gefährliche Links und/oder gefährliche Anhänge enthalten. Betrügerische Nachrichten lassen sich in Form von E-Mails, aber auch in jeder anderen Form verschicken. Im Fall von gefährlichen Links in E-Mails sprechen Fachleute oft von Phishing-E-Mails.

Gefährliche Nachrichten erkennen – und sich davor schützen

Damit Nutzerinnen und Nutzer Angriffe in Gestalt von betrügerischen Nachrichten besser verstehen und lernen, wie sie sich schützen können, hat die Forschungsgruppe SECUSO (Security – Usability – Society) am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des KIT das NoPhish Konzept entwickelt und daraus verschiedene Maßnahmen abgeleitet und evaluiert.

Das Konzept umfasst vier Themenbereiche:

- Einführung in das Thema
- Erkennen von unplausiblen, betrügerischen Nachrichten
- Erkennen von Nachrichten mit gefährlichen Links (einschließlich Ermitteln der URL hinter dem Link, Aufbau der URL und Tricks der Angreifer)
- Erkennen von Nachrichten mit gefährlichen Anhängen (einschließlich Ermitteln des Formats der Datei, Liste von besonders gefährlichen Dateiformaten und Tricks der Angreifer)

Die Entwicklung des NoPhish Konzepts startete an der TU Darmstadt, unter anderem im vom Bundesministerium für Wirtschaft und Energie im Rahmen der Initiative IT-Sicherheit in der Wirtschaft geförderten Projekt „KMU Aware“ sowie im vom Bundesministerium für Bildung und Forschung geförderten CRISP Projekt. Das Konzept wiederum ist auf Forschungsarbeiten rund um die NoPhish Android App aufgebaut. Die verschiedenen Maßnahmen sowie das Konzept werden nach wie vor evaluiert und auf der Basis der Ergebnisse weiterentwickelt. Außerdem werden neue Maßnahmen erarbeitet. Derzeit läuft die Forschung rund um das NoPhish Konzept unter anderem im Helmholtz Topic „Engineering Secure Systems“.

Bislang neun Maßnahmen für unterschiedliche Bedürfnisse

Das NoPhish Konzept wurde bisher in neun verschiedenen Maßnahmen implementiert und evaluiert. Diese sind unterschiedlich detailliert. Konkret sind dies die folgenden Maßnahmen:

- Flyer mit einer allgemeinen Einführung ins Thema und den wichtigsten Regeln zum Erkennen von betrügerischen Nachrichten
- Schulungsunterlagen zum Thema betrügerische Nachrichten mit vielen Beispielen, weiterführenden Informationen und Übungsaufgaben zum Selbststudium oder als Ausgangspunkt für eine Verbreitung des Wissens, beispielsweise durch Vorträge im eigenen Unternehmen
- E-Learning zum Thema betrügerische Nachrichten mit vielen Beispielen und weiterführenden Informationen zum Selbststudium. Das E-Learning besteht aus verschiedenen Levels; um ins jeweils nächste Level zu gelangen, müssen Nutzerinnen und Nutzer ein kleines Quiz bestehen.
- Erklärvideos, entwickelt gemeinsam mit dem Videokünstler Alexander Lehmann, die in jeweils weniger als fünf Minuten eine allgemeine Einführung geben und die wichtigsten Regeln zur Erkennung von betrügerischen Nachrichten erklären
- Quiz zum Erkennen betrügerischer Nachrichten, mit dem Nutzerinnen und Nutzer sich selbst testen können
- Online-Spiel „Phishing Master", das etwas andere Serious Game zum Erkennen betrügerischer Nachrichten
- Infokarte mit den wichtigsten Regeln zum Erkennen von Phishing und anderen betrügerischen Nachrichten im Hosentaschen-Format
- Poster mit den wichtigsten Regeln zum Erkennen von Phishing und anderen betrügerischen Nachrichten zum Aufhängen im Büro oder an zentralen Orten
- Challenge Poster mit verschiedenen Formen von (betrügerischen) Nachrichten und der Frage: Ist diese Nachricht vertrauenswürdig? Mithilfe eines QR-Codes kann der Nutzer diese Frage beantworten und landet dann auf einer Seite mit der Auflösung und weiteren Tipps zum Erkennen von Phishing und anderen betrügerischen Nachrichten.

Ziele und Evaluation

Die Maßnahmen zielen darauf, Nutzerinnen und Nutzer für die Gefahren zu sensibilisieren und ihnen gleichzeitig zu vermitteln, wie sie sich konkret schützen können. Die beiden kompakten Maßnahmen Poster und Infokarte dienen eher der Auffrischung des Wissens. Das Quiz eignet sich zum Überprüfen des aktuellen Wissensstands. Anders als viele andere im Internet verfügbaren oder von Firmen angebotenen Security Awareness Maßnahmen sind die NoPhish Maßnahmen empirisch hinsichtlich der Zielerreichung evaluiert; die Ergebnisse sind in wissenschaftlichen Arbeiten veröffentlicht. Die Zielerreichung evaluieren die Forschenden, indem sie messen, wie viel Prozent der im Rahmen der Studie gesehenen Nachrichten korrekt als Phishing oder als legitime Nachricht klassifiziert werden.

Hinweise zu verschiedenen Nutzungsszenarien und -rechten finden sich unter https://secuso.aifb.kit.edu/downloads/Nutzungsszenarien.pdf

Unternehmen und Einrichtungen, die den Einsatz von simulierten Phishing Kampagnen erwägen, finden eine Analyse solcher unter https://publikationen.bibliothek.kit.edu/1000119662/74582106

Karlsruher Institut für Technologie (KIT)
Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)
Prof. Dr. Melanie Volkamer
Kaiserstr. 89
76133 Karlsruhe
E-Mail: melanie.volkamer@kit.edu
Telefon: +49 721 608-45045
www.aifb.kit.edu/web/Melanie_Volkamer

SECUSO
SECURITY · USABILITY · SOCIETY

Karlsruher Institut für Technologie (KIT) · Präsident Professor Dr.-Ing. Holger Hanselka · Kaiserstraße 12 · 76131 Karlsruhe · www.kit.edu