Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Fachhochschule Dortmund
University of Applied Sciences and Arts

Aufgabe 3.1

Gucken Sie den Beitrag „Hirne Hacken“ von Linus Neumann zum 36. Chaos Communication Congress:

https://media.ccc.de/v/36c3-11175-hirne_hacken

Beantworten Sie folgende Fragen:

a) Was bemängelt Hr. Neumann an der aktuellen Lage der IT-Sicherheit?

b) Wie funktionieren die Scam, Fraud und Phishing Beispiele die Hr. Neumann vorstellt?

c) Welche Erklärungen für das menschliche Verhalten führt Hr. Neumann an?

d) Welche Lösungsansätze stellt Hr. Neumann vor?

Aufgabe 3.2

Angriffe mittels Social Engineering zielen meist auf spezielle menschliche Eigenschaften bzw. Reaktionen, so z. B. Angst oder Neugierde, ab und nutzen diese gezielt aus.

Erstellen Sie eine Kreuztabelle wie nachfolgend angedeutet, die den in der Vorlesung vorgestellten Angriffstechniken auf den Faktor Mensch jeweils eine oder mehrere menschliche Eigenschaften zuordnet, die für den Erfolg eines Angriffs entscheidend sind. Recherchieren und ergänzen Sie weitere Angriffstechniken, die aus Ihrer Sicht in den Kontext von Social Engineering passen und praktische Anwendung finden.

	Angst	**Neugierde**	**...**
Phishing	x	x	
Spam			
...			

Aufgabe 3.3

Im Rahmen einer fiktiven Anti-Phishing Kampagne soll die Security Awareness verbessert werden, indem absichtlich Phishing-E-Mails versandt werden. Erstellen Sie eine solche fiktive Phishing-E-Mail, mit der Benutzer des Studienportals der Fachhochschule Dortmund (https://portal.fh-dortmund.de/) verleitet werden könnten, eine private E-Mail-Adresse und das zugehörige Passwort preiszugeben.

a) Welche Möglichkeiten stehen zur Verfügung, um die Herkunft dieser Phishing-E-Mail möglichst realistisch wirken zu lassen? Welche Probleme ergeben sich hierbei unter Umständen?

b) Welche Mechanismen zur Abwehr von Phishing bzw. Spam könnten den Erfolg des fiktiven Angriffs gefährden?

c) Aus welchen Gründen sind die E-Mail-Adresse und das zugehörige Passwort ein lohnenswertes Angriffsziel? Wozu könnten diese Informationen im Falle eines erfolgreichen Angriffs weitergehend genutzt bzw. missbraucht werden?

Hinweis: Diese Phishing-E-Mail ist lediglich ein Beispiel im Rahmen der Übung und darf natürlich nicht als Phishing-E-Mail eingesetzt werden. **Unter keinen Umständen dürfen Sie diese Phishing-E-Mail versenden, auch nicht an sich selbst.**

Aufgabe 3.4

Ein wichtiger Teil von Angriffen mittels Social Engineering ist die Phase der Informationsgewinnung. Je mehr Informationen über ein mögliches Opfer vorliegen, desto gezielter kann ein Angriff erfolgen. Bei Spear Phishing ist z. B. die Plausibilität einer etwaigen Spear Phishing-E-Mail mitunter ausschlaggebend für den Erfolg.

a) Führen Sie ein Selbstexperiment durch und suchen Sie nach öffentlich verfügbaren Informationen zu Ihrer Person, die auch Dritte hätten finden können.
Nutzen Sie hierzu z. B. Suchanfragen bei Suchmaschinen, die explizit nach Ihrem Namen suchen: „Vorname Nachname“. Ergänzen Sie z. B. auch den Ort und weitere Informationen bei Ihren Suchanfragen. Beziehen Sie auch soziale Netzwerke bei Ihrer Suche ein und nutzen Sie etwaige gewonnene Informationen (z. B. Pseudonyme) für weitere Recherchen.

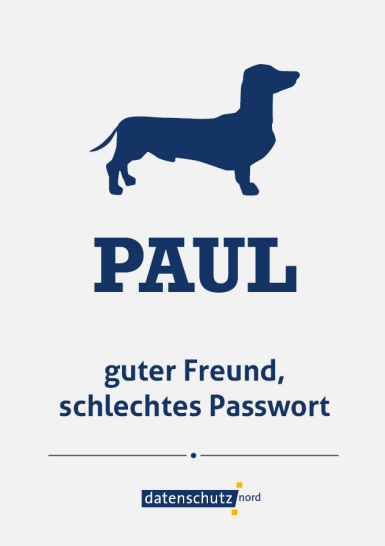
b) Bereiten Sie alle gefunden Informationen auf und erstellen Sie eine Übersicht, die Ihr Profil im Internet wiedergibt.

c) Welche dieser Informationen hätten ggf. für Angriffe mittels Social Engineering missbraucht werden können und wären Sie ggf. auf diese hereingefallen?

Aufgabe 3.5

Sie sind für eine fiktive Kampagne zur Steigerung der Security Awareness in einem Unternehmen verantwortlich. In regelmäßigen Abständen werden Materialien zu unterschiedlichen Themen der Security Awareness über das Intranet und über Plakate bereitgestellt. Aktuell geht es um das Thema Passwortsicherheit.

Erstellen Sie einen Entwurf für ein Plakat, das auf lustige Weise die Wichtigkeit von sicheren Passwörtern zum Ausdruck bringt und ggf. für Verständnis für diese Anforderung sorgen kann.



https://www.datenschutz-notizen.de/paul-guter-freund-schlechtes-passwort-3621339/#, aufgerufen am 18.04.2023