Praxisidee: Was ist hacken?

Infomaterial für Lehrpersonen

Modul B: Versteckte Daten

Abwandlung einer Übung von CS Unplugged, lizenziert unter CC BY-SA:
https://www.ada.wien/arbeitsblatt-geheimnisse-teilen/

In dieser Übung soll die **durchschnittliche Zahl der Social-Media-Profile** der Schüler:innen ermittelt werden. Das funktioniert genauso mit anderen Werten wie Alter, Körpergröße, Zahl der erhaltenen Geburtstagsgrüße etc.

Die Klasse teilt sich nun in eine Beobachtungsgruppe und eine Übungsgruppe ein. Etwa fünf Schüler:innen sollten sich an der Übung beteiligen. Es dürfen nicht weniger als drei sein, und ab etwa 8 Personen dauert das Experiment zu lang.

Die restlichen Schüler:innen in der Beobachtungsgruppe beobachten die Übungsgruppe bei der Ausführung. Die Lehrperson moderiert die Übung und gibt der Übungsgruppe Schritt für Schritt die Anweisungen durch.

Ablauf der Übung:

- In diesem Beispiel sind fünf Schüler:innen an der Übung beteiligt.
- Die erste Person wählt eine dreistellige Geheimzahl, zum Beispiel die Zahl 236, und schreibt sie auf einen Zettel, den sie für sich behält.
- Dann addiert sie zu der Geheimzahl die Anzahl ihrer Social-Media-Profile, nehmen wir an, es sind 7. Sie schreibt das Ergebnis - 243 - auf einen zweiten Zettel und reicht diesen verdeckt an die nächste Person weiter.
- Dieser Vorgang wird fortgesetzt, wobei jede Person die Anzahl ihrer Social-Media-Profile zu der empfangenen Zahl addiert, auf einen neuen Zettel schreibt und diesen weitergibt.
- Wenn alle an der Reihe waren, wird der letzte Zettel an die erste Person zurückgegeben. Darauf steht nun die Zahl 275.
- Die erste Person zieht die ursprüngliche Geheimzahl vom Ergebnis des letzten Zettels ab und erhält dadurch die Summe der Anzahl der Social-Media-Profile aller Beteiligten: 32.
- Diese Zahl wird durch die Zahl der Beteiligten dividiert und ergibt die durchschnittliche Zahl der Social-Media-Profile der Schüler:innen, nämlich 6,4.

Das Ergebnis ist der Durchschnittswert der Social-Media-Profile. Es ist nicht möglich, die Anzahl der Social-Media-Profile einer einzelnen Person zu ermitteln, es sei denn, zwei Personen arbeiten zusammen, vergleichen ihre Werte und „hacken“ damit das System. Das bedeutet, dass dies ein sicherer Vorgang im Sinne des Datenschutzes ist. Es können keine personenbezogenen Daten erfasst bzw. ausgelesen werden.

Modul C: Social engineering

Da Computersysteme meist sehr gut gesichert sind, wählen Kriminelle sehr oft zunächst die Menschen als Ziele aus, die mit diesen Systemen arbeiten. Mit verschiedenen psychologischen Tricks werden Menschen dazu gebracht, Zugangsdaten oder andere geheime Informationen zu verraten oder Schadprogramme zu installieren. Einige davon sind:

- Autorität: Hacker:innen geben sich als Vorgesetzte, Polizist:innen oder Beamt:innen des Finanzamts aus.
- Hilfsbereitschaft: Hacker:innen verleiten die Zielperson dazu zu kooperieren und liefern etwa eine genaue Anleitung, wie Daten auf einer Webseite einzugeben sind.
- Sympathie und Attraktivität: Hacker:innen gaukeln den Zielpersonen Freundschaft oder Liebe vor. Dazu präsentieren sie sich auf sozialen Netzwerken mit attraktiven Fotos. Es findet meist kein persönlicher Kontakt statt.
- Angst: Hacker:innen drohen mit schlimmen Konsequenzen, wenn nicht kooperiert wird.
- Gier: Hacker:innen machen der Zielperson ein vermeintlich tolles Angebot, das aber nur begrenzte Zeit gilt.

Häufige Methoden von „Social engineers“ sind:

- Phishing (ein Kunstwort, das „password fishing“ bedeutet): Gefälschte E-Mails an eine große Zahl von Empfänger:innen. Meist geben sie vor, von einer Bank oder großen Firma zu stammen und verlangen die Änderung eines Passworts. Phishing-Versuche können an der falschen Absender-Adresse und oft an Rechtschreibfehlern erkannt werden.
- Spear-Phishing: Gefälschte E-Mails, die gezielt an einzelne Zielpersonen gerichtet sind. Die Angreifer:innen informieren sich genau über die Personen, die Texte sind meist sorgfältig formuliert und enthalten persönliche Informationen. Spear-Phishing ist wesentlich schwerer zu erkennen als gewöhnliches Phishing.
- Vishing (Voice-Phishing): Anrufe von vermeintlichen Vorgesetzten, Firmen oder Familienmitgliedern sollen eine Person dazu bringen, persönliche Daten zu verraten, jemandem eine Tür zu öffnen oder Geld zu überweisen.
- Baiting (Ködern): Mit einem digitalen oder physischen Köder sollen Menschen verleitet werden, Daten preiszugeben oder Schadsoftware zu installieren. Ein solcher Köder kann entweder eine E-Mail zu einem angeblich gewonnenen Gewinnspiel sein oder auch ein „vergessener“ USB-Stick, der nach dem Anschließen einen Trojaner installiert.
- Pretexting: Ein falscher Vorwand (Pretext) wird genutzt, um der Zielperson Informationen zu entlocken oder sie zur Kooperation zu bewegen. Die Angreifer:innen recherchieren im Vorfeld sehr genau über die Zielperson (Profiling). Oft geben sich die Angreifer:innen als Vorgesetzte aus oder als Vertreter:innen von Firmen, mit denen die Zielperson in einer Geschäftsbeziehung steht - Telefonanbieter, Bank etc.

Modul C: Geschichte „Angriff auf Mark Gullible“

Einige mögliche Antworten auf die Fragen - es kann durchaus noch mehr kreative Zugangsmöglichkeiten geben:

Welche Angriffspunkte hat Mark Gullible?

- Er tut, was ihm gesagt wird, und ist wahrscheinlich autoritätshörig.
- Zu ihm kommen oft Personen von außerhalb der Firma.
- Er kennt seine Vorgesetzten nicht persönlich.
- In der U-Bahn können Menschen die Inhalte seiner Social-Media-Accounts einsehen.
- Er ist geschieden und auf der Suche nach einer Partnerin.
- Seine Tochter ist weit entfernt, und er hat nur lose Kontakt zu ihr.
- Er spielt Gewinnspiele.
- Er hat Schulden.
- Er sammelt originelle USB-Sticks.

Wie könnte man Schadsoftware in seinen Computer einschleusen?

- auf einer gefälschten Gewinnspiel-Seite
- im Foto einer vermeintlichen Interessentin von einer Partnersuchseite
- in einem Foto, das angeblich von seiner Tochter kommt
- auf einem in seinem Büro deponierten USB-Stick

Wie könnte man Mark dazu bringen, Geld zu überweisen?

- sich als Freund seiner Tochter ausgeben, die angeblich einen Unfall gehabt hat und Geld braucht.
- behaupten, er hätte viel Geld gewonnen, müsste aber zuerst einen Bearbeitungsbetrag überweisen, bevor er den Gewinn erhalten kann.
- sich als verliebte, aber weit entfernt lebende Frau ausgeben, die Geld braucht, um zu ihm zu reisen.

Wie könnte man Mark dazu bringen, persönliche Kontodaten oder Passwörter zu übermitteln?

- sich als sein Vorgesetzter ausgeben und ihn anrufen, dass man seine Zugangsdaten braucht.
- ihn mit der Behauptung erpressen, man hätte seine Tochter entführt.