Muster: Reflexion zu den Ergebnissen der Vorstellung

Schutz vor Identitätsdiebstahl am Beispiel Pishing-Mail

---

1. **Aufgabe** Beschreibt, was das Ziel dieser E-Mail sein könnte. Benenne Besonderheiten der Mail, die bei genauem Hinschauen skeptisch machen könnten. Beschreibt auch, was das Beispiel mit digitalen Identitäten zu tun hat.

Folgende Aspekte sind besonders wichtig:

- ein Ziel ist das Anklicken eines Hyperlinks, der z.B. die Werbeeinnahmen eines Betreibers erhöht, zur Eingabe persönlicher Daten über Formulare auf einer Webseite auffordert oder schadhaften Code enthalten kann

- ein weiteres Ziel ist bei Beispiel 2 die Herausgabe einer Telefonnummer oder Bestätigung einer Mailadresse, die vielleicht auf Verdacht angeschrieben wurde, um weitere E-Mails an diese versenden zu können

Besonderheiten der Mails sind folgende:

- es wird nicht persönlich angeschrieben („Sehr geehrter Herr Morisse“ z.B.), das heißt, vermutlich wurden sie automatisiert an sehr viele Adressen versendet

- die Mailadresse des Absenders ist unseriös (z.B. mit Bindestrich nach dem @ und als Namen „kontakt“ statt einen vollständigen Namen mit Vor- und Nachnamen.)

- es wird so getan, als ob es sich um eine Antwort handelt (Beispiel 3), um möglicherweise in einem Büro als Empfänger, das viele Mails am Tag zu bearbeiten hat, Flüchtigkeitsfehler zu fördern und Vertrauen zu wecken

- Rechtschreibfehler wie „applicationns“ (Bsp. 2) oder komische Sinnzusammenhänge „im Internet gefördert zu werden“ (Bsp. 1)

Die Beispiele haben mit digitaler Identität zu tun, da:

- ich nicht so einfach persönlich nachvollziehen kann, ob der Absender der ist, der er vorgibt zu sein und er mir in diesen Beispielen eine falsche Identität vorspielt

- durch die E-Mails vor allem auf die Herausgabe persönlicher Daten des Empfängers gezielt wird, also dessen digitale Identität versucht, möglichst umfangreich zu erfassen und zu verwerten.

2. **Aufgabe** Recherchiert und informiert euch, was eine Phishing-Mail ist und welche Möglichkeiten es für die Versender solcher Mails gibt, Mailadressen zum Anschreiben herauszufinden. Benennt Verhalten und Maßnahmen zum Schutz gegen solche Mails.

Muster: Reflexion zu den Ergebnissen der Vorstellung

> Erarbeitet Vorschläge, wie die Identität eines Absenders für den Empfänger überprüfbar bleibt.

Eine Phishing-Mail ist eine gefälschte Nachricht, um über Betrug an persönliche Daten eines anderen Users zu gelangen und damit Identitätsdiebstahl zu begehen. Die Gutgläubigkeit des Opfers wird dabei ausgenutzt, da dieser die gefälschte Nachricht auf den ersten Blick nicht erkennt.

Möglichkeiten, an Mailadressen zu kommen sind schlicht das automatisierte Durchsuchen von Webseiten nach Mailadressen oder das Erwerben von Datenbanken, z.B. von Datenhändlern, die legal beispielsweise in Form von sozialen Netzwerken oder illegal in Form von Datendiebstahl personifizierte Datensätze verkaufen.

Verhalten und Maßnahmen sollten sein:

- Datensparsamkeit: Persönliche Daten nur zweckgebunden weitergeben, wo möglich und angemessen Pseudonyme verwenden (Beispielsweise in sozialen Netzwerken)

- Wegwerf-Mailadressen für einmalige Bestellungen u.ä, verwenden oder eine Mailadresse extra nur für kommerzielle Online-Aktivitäten verwenden, die leicht neu angelegt werden kann, während eine private und persönliche Adresse nur gezielt weitergegeben wird

Vorschläge, wie die Identität überprüfbar bleibt:

- Angabe weiterer Informationen in einer E-Mail, z.B. Geschäftsadresse, Telefonnummer

- Zertifizierung via pgp-Signatur und Bestätigung der Identität durch Dritte

- persönliche Übergabe des Mailkontaktes oder Bereitstellung über eine seriöse Quelle wie eine offizielle Webseite mit Zertifikat

Weitergehende Fragen für die Reflexion können sein:

1. Welche Probleme entstehen durch Missbrauch, welche durch Fahrlässigkeit und was ist technisch gar nicht anders möglich oder ein technischer Mangel?

Erarbeitung einer begründeten Positionierung (z.B. Hinstellspiel / Position beziehen: Missbrauch / Fahrlässigkeit / technischer Mangel)

Beispiele: Missbrauch (Vorspiegelung einer falschen Identität) Fahrlässigkeit (Mailadresse eines Absenders nicht auf Glaubwürdigkeit überprüfen) technischer Mangel (E-Mail hat keine automatische Zertifizierung, diese muss extern eingeführt und eingefordert werden)

2. Welche Probleme lassen sich auf andere Anwendungen wie soziale Netzwerke, Messenger etc. übertragen?

- bei Messenger: Fremde Kontakte blocken oder zunächst über andere Kanäle erfahren, um welche Person / Organisation es sich handelt

Muster: Reflexion zu den Ergebnissen der Vorstellung

- kritische Grundhaltung aufbauen: Es ist einfach, eine Identität zu fälschen, solange nicht bestimmte, oben genannte Überprüfungen stattfinden

3. Wie kann meine Identität unautorisiert verwendet werden?

- sichere Passwörter sind wichtig, damit der Account nicht gekapert wird, auch für verschiedene Accounts verschiedene Passwörter nutzen

- Verschlüsselte Verbindungen nutzen, damit Passwörter nicht abgefangen werden können (bereits Standard bei Webseiten über https aber nicht bei Email!)

- zwei Phasen Identifizierung nutzen, z.B. beim Banking: Karte und PIN sind notwendig, damit Transaktionen verfügbar sind

- verschiedene Strategien beim Onlinebanking: Wie kann sichergestellt werden, dass nicht z.B. Gesichtserkennung über ein simples Foto, welches in die Kamera gehalten wird, „ausgetrickst“ wird?