Persönliche Sicherheit

1.3.1 Den Begriff Social Engineering verstehen und die Ziele kennen

Social Engineering bezeichnet Techniken, mit denen Angreifer versuchen, Menschen zu manipulieren, um vertrauliche Informationen zu erhalten oder unberechtigten Zugriff auf Systeme zu erlangen. Dabei zielen sie häufig auf emotionale Reaktionen ab, um ihre Opfer zur Preisgabe von Informationen zu bewegen.

Ziele von Social Engineering:

- **Unberechtigter Zugriff auf Computer und mobile Geräte:** Angreifer versuchen, durch Täuschung Zugang zu Geräten zu erhalten, um Daten zu stehlen oder Systeme zu manipulieren.

Beispiel: Ein Angreifer gibt sich als IT-Support-Mitarbeiter aus und fordert den Benutzer auf, sein Passwort zur „Überprüfung“ anzugeben.

- **Unerlaubtes Sammeln von Informationen:** Oftmals versuchen Angreifer, sensible Informationen wie persönliche Daten, Kontoinformationen oder Zugangsdaten zu sammeln.

Beispiel: Jemand fragt in einer E-Mail nach Informationen, die angeblich zur Verbesserung des Kundenservices benötigt werden.

- **Betrug:** Social Engineering kann auch dazu verwendet werden, finanzielle Vorteile zu erlangen, indem die Opfer in betrügerische Transaktionen verwickelt werden.

Beispiel: Ein Angreifer überredet das Opfer, Geld an ein gefälschtes Konto zu überweisen, indem er vorgibt, ein vertrauenswürdiger Bekannter zu sein.

1.3.2 Methoden des Social Engineering kennen

Angreifer verwenden verschiedene Methoden des Social Engineering, um an Informationen zu gelangen:

- **Telefonanrufe (Voice Phishing oder Vishing):** Vishing ist eine Form des Phishings, bei der Angreifer telefonisch Kontakt aufnehmen, um vertrauliche Informationen zu erhalten. Der Anrufer gibt sich oft als Mitarbeiter einer Bank, einer Behörde oder eines anderen vertrauenswürdigen Unternehmens aus.

Beispiel: Ein Anrufer gibt vor, von der Bank zu sein, und fordert den Kunden auf, seine Kontoinformationen zur Überprüfung zu bestätigen. Oft wird Druck aufgebaut, um das Opfer zur schnellen Preisgabe von Informationen zu bewegen.

- **Phishing:** Hierbei handelt es sich um den Versuch, über gefälschte E-Mails oder Websites an persönliche Daten zu gelangen. Oft sind diese E-Mails so gestaltet, dass sie echt erscheinen.

Beispiel: Eine E-Mail, die vorgibt, von einem Online-Shop zu stammen, fordert den Nutzer auf, seine Login-Daten auf einer gefälschten Website einzugeben.

- **Shoulder Surfing:** Diese Methode besteht darin, über die Schulter einer Person zu schauen, um vertrauliche Informationen zu erlangen, z. B. Passwörter oder PINs.

Beispiel: Jemand beobachtet einen Kollegen beim Eingeben seines Passworts an einem Computer.

1.3.3 Den Begriff Identitätsdiebstahl verstehen und die Folgen kennen

Identitätsdiebstahl bezeichnet die illegale Verwendung der persönlichen Daten einer anderen Person, um sich als diese Person auszugeben. Dies kann schwerwiegende Folgen für die Opfer haben.

Folgen von Identitätsmissbrauch:

- **Persönliche Folgen:** Betroffene können unter psychischen Belastungen leiden, da sie das Gefühl haben, dass ihre Privatsphäre verletzt wurde. Vertrauen in Online-Transaktionen und Dienstleistungen kann erheblich beeinträchtigt werden.
- **Finanzielle Folgen:** Identitätsdiebstahl kann zu erheblichen finanziellen Verlusten führen, beispielsweise durch betrügerische Kreditkartenkäufe oder die Eröffnung von Bankkonten im Namen des Opfers.

Beispiel: Ein Täter verwendet die gestohlenen Daten, um Kreditkarten zu beantragen und Käufe zu tätigen, die das Opfer dann zurückzahlen muss.

- **Geschäftliche Folgen:** Unternehmen, die von Identitätsdiebstahl betroffen sind, können rechtliche Konsequenzen und einen Verlust des Kundenvertrauens erleben. Das Unternehmen könnte auch für entstandene Schäden haftbar gemacht werden.
- **Rechtliche Folgen:** Das Opfer könnte fälschlicherweise mit Straftaten in Verbindung gebracht werden, die von den Tätern im Namen des Opfers begangen wurden.

Beispiel: Ein Täter benutzt die Identität einer anderen Person, um illegal Waren zu kaufen, was zu rechtlichen Problemen für das Opfer führen kann.

1.3.4 Methoden des Identitätsdiebstahls kennen

Es gibt verschiedene Methoden, wie Identitätsdiebstahl durchgeführt wird:

- **Information Diving:** Bei dieser Methode durchsuchen Täter Mülltonnen oder Abfälle, um vertrauliche Informationen zu finden, wie Kontoauszüge oder persönliche Dokumente.

Beispiel: Ein Täter findet alte Kontoauszüge mit persönlichen Informationen in der Mülltonne und verwendet diese, um sich als das Opfer auszugeben.

- **Skimming:** Hierbei handelt es sich um das Abgreifen von Informationen von Kreditkarten durch spezielle Geräte (Skimmer), die an Geldautomaten oder Verkaufsstellen angebracht werden.

Beispiel: Ein Skimmer wird an einem Geldautomaten installiert, um die Daten von Kreditkarten zu erfassen, wenn ahnungslose Benutzer ihre Karten einführen.

- **Pretexting:** Der Täter gibt sich als jemand aus, der einen legitimen Grund hat, Informationen zu erfragen. Er schafft eine falsche Identität oder Situation, um die gewünschten Daten zu erhalten.

Beispiel: Ein Angreifer gibt vor, ein Mitarbeiter einer Telefongesellschaft zu sein, und fragt nach persönlichen Informationen, um einen Service bereitzustellen.