Computacenter

SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT – UMGANG MIT INFORMATIONEN

Social Engineering

SOCIAL ENGINEERING

EINFÜHRUNG

„Social Engineering“

Hier erfährst Du, was Social Engineering ist, mit welchen Methoden die Angreifer arbeiten und wie Du Dich davor schützen kannst.

Interne Informationen sind für Kriminelle oft eine wertvolle Ressource. Da die technischen Schutzmaßnahmen aber immer schwerer zu überwinden sind, suchen die Angreifer zunehmend andere Schwachstellen.

So lassen sich interne Informationen oft auch über soziale Interaktionen mit arglosen Mitarbeitern beschaffen, deren Höflichkeit und Hilfsbereitschaft ausgenutzt wird.

Diese Art von Angriff auf das Unternehmen wird „Social Engineering“ genannt.

Szenarien

Social Engineers sind Wirtschaftsspione. Ihre Beute sind Insiderinformationen.

Lasse Dich nicht beirren. Die Angreifer sind geübt darin, in unterschiedliche Rollen zu schlüpfen. Sie markieren etwa den großen Boss, einen wichtigen Kunden oder bitten um Hilfe..

Trotz Sicherheitsmaßnahmen gelingt es Social Engineers immer wieder, in Unternehmensgebäude einzudringen.

Wenn Du in einem Firmengebäude einen Unbekannten siehst, der keinen Ausweis bzw. Besucher-Ausweis trägt, sprich ihn oder sie darauf an, sofern Du dich sicher fühlst. Melde den möglichen Eindringling andernfalls umgehend einem Vorgesetzten oder dem Sicherheitspersonal am Standort.

Die Angreifer sind geübt darin, in unterschiedliche Rollen zu schlüpfen. Sie markieren etwa den großen Boss, einen wichtigen Kunden oder bitten um Hilfe.

Social Engineering ist keine Methode, die sich auf den persönlichen Umgang beschränkt. Häufig wird versucht, per E-Mail (auch als Phishing bekannt), per Telefon (Vishing) oder sogar per SMS (SMiShing) an die gewünschten Informationen zu gelangen.

Opfer eines telefonischen Social Engineering-Angriffs kann jeder werden, von der Reinigungskraft bis zum Vorstand.

In vielen Fällen handelt es sich bei den Informationen, die bei Social Engineering-Attacken ausgespäht werden sollen, um scheinbar banale Angaben, wie z. B. wer für was zuständig ist oder die Handynummer eines Kollegen. Aus diesem Grund ist es sinnvoll, sich eine Strategie zurechtzulegen, wie man sich vor solchen Angriffen schützt.

Wie kannst Du Dich davor schützen?

- Ich hinterfrage die Legitimation eines Anrufers und stelle z. B. Kontrollfragen.
- Bei einem Anruf von außen bitte ich um eine interne Telefonnummer (keine Mobilnummer) und biete an, zurückzurufen.
- Ich gebe über das Telefon keine sensiblen Informationen weiter, insbesondere keine Zugangsdaten.

All diese Maßnahmen sind sinnvoll, um sich vor einem Social Engineering-Angriff zu schützen.

Was aber ist zu tun, wenn die Angreifer die Informationen erhalten, nach denen sie gesucht haben? Nehmen wir an, dass Du Deine Anmeldedaten nach einem verzweifelt klingenden

Anruf aus der IT-Abteilung weitergegeben hast.

Eine Stunde später triffst Du jemanden aus der Abteilung und stellst fest, dass es gar kein Problem gab und Du hereingelegt wurdest.

Auch wenn es Dir peinlich ist: Bitte verschweige einen solchen Vorfall nicht. Je schneller das Leck gestopft ist, desto weniger Schaden wird angerichtet. Auch misslungene Angriffsversuche solltest Du melden, um Computacenter zu warnen.

Zusammenfassung

In dieser Lektion hast Du gelernt, dass …

- der Informationsdiebstahl über die Mitarbeiter als „Social Engineering“ bezeichnet wird.
- die Angreifer interne Angaben nutzen, um glaubwürdig zu erscheinen und die Opfer manipulieren zu können.
- Wachsamkeit und ein gesundes Misstrauen den besten Schutz gegen die Angriffe bieten.
- jeder Vorfall im Unternehmen gemeldet werden muss.
-

Datenschutzverletzungen und Informationssicherheitsvorfälle:

Wenn Du glaubst, dass Du auf einen Social Engineering-Angriff hereingefallen bist, melde bitte einen entsprechenden Informationssicherheitsvorfall über das NGSD. Melde auf den Vorfall auch dann, wenn der Angreifer die gewünschten Informationen nicht erhalten hat.