12. Juli 2017

# Cyber-Kriminalität: Achtung Manipulation

## Schlagworte

Verbraucher
Datenschutz
Cyberattacken
Cyberkriminalität
Social Engineering

Vorsicht Falle! Die Masche ist relativ neu und sehr ausgeklügelt. Der Name: Social Engineering. Auf Deutsch: Sie werden manipuliert, damit Sie sich „freiwillig“ Schadsoftware auf PC, Tablet oder Smartphone laden oder Passwörter preisgeben. Beispiele: Sie mögen Katzen! Eine vermeintliche Freundin schickt Ihnen per E-Mail Fotos von Katzenbabys – nur einen Klick entfernt. Oder: Per SMS werden Sie eingeladen, an einem Gewinnspiel teilzunehmen. Hierfür müssten Sie nur die Anschrift in ein Internet-Formular eintragen („Bitte auf den Link klicken“).

Das Perfide: Diese Angriffsform konzentriert sich zunächst nicht auf die Technik, sondern nimmt das menschliche Verhalten ins Visier. Angegriffen wird über jede Form der Kommunikation – z.B. über Links in E-Mails oder SMS oder über das Telefon. Der Täter versucht mit seinem Opfer in eine Beziehung zu treten und so an sensible Daten zu gelangen. Der spätere Online-Angriff wird erst möglich gemacht, wenn es ihm gelingt, Sie dazu zu bringen, Passwörter oder Adressdaten preiszugeben, Sicherheitsfunktionen am Computer auszuschalten oder Schad-software zu installieren. Dabei nutzen die Cyberkriminellen Eigenschaften wie Neugier, Vertrauen, Angst oder Hilfsbereit-schaft aus.

Die Tricks zu erkennen ist nicht einfach, aber das Wissen um diese Angriffsarten kann das Risiko eines erfolgreichen Angriffs verringern. Die wichtigsten Tipps:

- **Mit gesundem Menschenverstand agieren**
  Ein gesundes Misstrauen kann gegenüber Beeinflussung helfen. Wenn Sie z.B. aufgefordert werden, eine bestimmte Aktion durchzuführen, hinterfragen Sie den Sachverhalt. Hinterfragen Sie die Identität der Person, die Sie kontaktiert.

- **Sensible Daten schützen**
  Gehen Sie verantwortungsbewusst mit Ihren persönlichen Daten um. Dazu gehören neben Passwörtern, Kartendaten, Geheimzahlen (PINs) und TANs auch Ihre Adresse, Ihre Telefonnummern oder Ihr Geburtsdatum. Ihre Bank wird Sie zudem nie zu einer Bestätigung Ihrer sensiblen Daten per E-Mail auffordern. Klicken Sie auch keine Links an, die Sie weiterleiten sollen, um solche Daten einzugeben.

- **Inhalt von E-Mails prüfen**
  Bevor Sie Anhänge öffnen oder auf Links in einer E-Mail klicken, überprüfen Sie den Inhalt und Absender der Nachricht. Kennen Sie den Absender und ist der Inhalt der E-Mail glaubwürdig bzw. plausibel? Im Zweifel löschen, ohne auf den Link zu klicken.

- **Auf sicheres Einloggen achten**
  Bei Phishing-Angriffen versuchen Betrüger, Sie auf kopierte Websites zu locken, um Ihre Daten abzufangen. Folgen Sie keinen Links, sondern geben Sie die Webadresse Ihrer Bank immer selbst in die Browserzeile ein. Bevor Sie sich beim Online-Banking einloggen, überprüfen Sie, ob es sich wirklich um die verschlüsselte Seite Ihrer Bank handelt („https…“) und im Browser ein Schloss-Symbol erscheint.

- **Aufmerksam in Sozialen Netzwerken**
  Akzeptieren Sie nicht leichtfertig Kontaktanfragen von Unbekannten. Prüfen Sie jede von Ihnen veröffentlichte Information darauf, ob diese gegen Sie oder Andere verwendet werden kann. Je mehr Sie von sich preisgeben, desto leichter fällt Kriminellen das Ausspähen.

- **Soft- und Hardware immer auf neuestem Stand halten**
  Ihre Sicherheitssoftware für PC, Smartphone und Tablet sollte immer auf dem neuesten Stand sein. Sie brauchen für alle Geräte einen aktuellen Virenscanner, eine Firewall. Halten Sie auch die Software immer aktuell, indem Sie Updates umgehend installieren.

Pressekontakt:

Julia Topar
Pressesprecherin
Telefon: +49 30 1663-1240
julia.topar@bdb.de