VORSICHT: HAKEN

Werfen Kriminelle im Internet ihre Angel aus, ködern sie potenzielle Opfer häufig mit Phishing-Mails – täuschend echt aussehende E-Mails. Ihr Ziel: Nutzerdaten.

2019 wurden in Deutschland 114 MIO. neue Schadprogramm-varianten registriert*.

„Was schwimmt denn da?“, fragt sich der Fisch und hängt im nächsten Moment am Haken. Er hat einen Köder geschluckt. Was sich beim Angeln im Wasser seit Jahrhunderten bewährt, hat sich längst in den virtuellen Raum verlagert. Statt Fische versuchen dort jedoch Kriminelle, sich Passwörter zu angeln. Diese Betrugsmasche wird auch „phishing“ genannt. Der Begriff setzt sich aus den englischen Wörtern „password“ und „fishing“ zusammen. Die Diebe ködern potenzielle Opfer mit betrügerischen Mails, sogenannte Phishing-Mails. Dabei ahmen sie vertrauenswürdige Adressen nach. Logo, Schrift und Farben wirken meist täuschend echt.

Nicht irritieren lassen

Der Inhalt der Nachricht suggeriert Handlungsbedarf: eine wichtige Neuigkeit oder Überprüfung, auf die umgehend reagiert werden müsse. Dafür ist die Eingabe der persönlichen Daten über einen Link erforderlich. Doch dieser lockt den Empfänger auf eine perfekt imitierte Website. Geben Ahnungslose dort ihre Nutzerdaten preis, hängen Benutzernamen, Passwörter, PIN oder Bankdaten an der Angel der Betrüger. Einmal in ihrem Besitz, können sie damit u. a. in einem Onlineshop einkaufen oder Überweisungen auf dem Bankkonto veranlassen.

TIPPS

- Achten Sie auf Absenderadresse, Betreff und Text: Phishing-Mails weisen oft Rechtschreibfehler auf oder weichen von der Originalschreibweise ab.
- Werden Sie stutzig, wenn Sie nicht persönlich mit Ihrem Namen angesprochen werden.
- Klicken Sie niemals auf Links oder Anhänge, wenn Sie an der Echtheit einer E-Mail zweifeln.
- Geben Sie niemals persönliche Daten, Passwort, PIN oder TAN per Mail preis.

Weitere Infos, wie Sie sich vor Phishing-Mails schützen, gibt es unter: www.bsi-fuer-buerger.de

Wer genau hinschaut, schluckt den Köder der Datenfischer erst gar nicht. Gleich vorneweg: Keine Bank und kein seriöser Anbieter fordert seine Kunden per Mail auf, vertrauliche Zugangsdaten preiszugeben. Am einfachsten zu durchschauen sind Phishing-Mails, die in schlechtem Deutsch geschrieben sind. Ein weiteres Indiz: auf Englisch oder Französisch verfasste E-Mails. Wer nicht gerade Kunde einer Bank mit Sitz im Ausland ist, kann sicher sein, dass ihn seine Bank – wenn überhaupt – nur auf Deutsch anschreibt.

Da stimmt was nicht

Auch wenn die direkte Anrede fehlt, sollten Sie stutzig werden: Seriöse Anbieter sprechen Sie nicht mit „Sehr geehrte Damen und Herren“ an. Vorsicht auch, falls Sie aufgefordert werden, ganz dringend oder innerhalb einer bestimmten Frist Ihre Kontoinformationen zu bestätigen. Besonders wichtig: Klicken Sie niemals auf Links oder Anhänge einer dubiosen Mail. Geben Sie erst recht keine Daten auf einer Internetseite mit unverschlüsselter Verbindung ein. Achten Sie dafür auf die Abkürzung „https://“ sowie auf das kleine Vorhängeschloss-Symbol in der Adresszeile Ihres Browsers. Nichts davon zu sehen? Dann Finger weg!

*Quelle: Lagebericht zur IT-Sicherheit 2019 vom Bundesamt für Sicherheit in der Informationstechnik (BSI)