Datenfischer wollen nur Ihr Bestes: Ihre persönlichen Daten

Nahezu täglich finden sich in unseren E-Mail-Postfächern offiziell aussehende Nachrichten und Mitteilungen. Doch manchmal trügt der Schein: Hinter den Mails stecken dann Kriminelle, die persönliche Angaben wie Passwörter und Login-Daten stehlen.

Die aus den Begriffen „Password“ und „Fishing“ abgeleitete Angriffs-Methode gehört neben der Malware zu den größten Gefahren im Internet. Datenfischer versenden hierbei täuschend echt aussehende E-Mails. Die gefälschten Absender sind häufig Banken, Webshops oder Paketlieferdienste. Vor allem über eingebundene Links in den E-Mails versuchen die Betrüger an Passwörter und andere persönliche Zugangsdaten zu gelangen. Gegen den Datenklau hilft vor allem eines: Aufmerksam sein.

Fiese Masche mit großem Erfolg

Jeder von uns hinterlässt Spuren im Internet, wie zum Beispiel Aufenthaltsort, Aktivitäten in sozialen Netzwerken oder Konsumverhalten. Das Geschäft mit diesen Verbraucher-Daten boomt – Unternehmen zahlen für möglichst vollständige Datensätze hohe Preise an Datenhändler. Aber auch Kriminelle sind auf der Jagd nach sensiblen Informationen: Passwörter, Kreditkartendaten oder Zugangscodes für das Onlinebanking sind dabei besonders begehrt.

„Ihr Konto wurde vorübergehend gesperrt“ oder „Sie müssen Ihre Zugangsdaten aktualisieren“ – so oder ähnlich lauten die Betreffzeilen der gefälschten E-Mails. Das klingt dringend und weckt die Aufmerksamkeit der Empfänger. Mehr als zehn Prozent aller Internetnutzer, die im Fokus einer solchen Attacke stehen, reagieren auf einen Phishing-Angriff. Jede zehnte E-Mail führt so zum Erfolg und macht Phishing zum lukrativen Prinzip für Cyberkriminelle.

Datenmissbrauch mit System

Klickt der User auf einen schädlichen Link in der Phishing-E-Mail ist der Schaden nicht mehr abzuwenden. Diese Links sind gut getarnt: Während der Linktext die harmlose Originaladresse anzeigt, führt das Linkziel mithilfe sogenannter Scripttechniken beim Anklicken auf eine gefälschte Webseite. Diese ist dann meist eine täuschend echt aussehende Kopie der Original-Webseite, zum Beispiel die Startseite der eigenen Bank. Auf den manipulierten Seiten werden Nutzer gebeten, ihre Zugangsdaten, Geheimzahl (PIN) oder Einmalpasswort (TAN) einzugeben. Wer dem nachkommt, leitet die begehrten Daten direkt an die Betrüger weiter. Zum Teil enthalten die Phishing-E-Mails auch gefährliche Anhänge. Diese installieren dann unwissentlich Schadsoftware auf dem Computer, die ebenfalls Daten abfängt und an Dritte weiterleitet.

Mit den gestohlenen Informationen übernimmt der Urheber der Phishing-Attacke die Identität seines Opfers und führt in dessen Namen unrechtmäßig Handlungen aus. Innerhalb von wenigen Minuten ersetzt er

die ursprünglichen Zugangsdaten für ein Bankkonto durch neue. Auf diese Weise gelangt der eigentliche Besitzer nicht mehr an seinen Account und kann die betrügerischen Vorgänge nicht unterbinden. Die Kriminellen räumen derweil das Konto leer. Nicht selten versteigern sie auch gestohlene Waren unter fremden Namen bei Online-Auktionen und begehen damit kriminelle Rufschädigung.

Durch den Missbrauch der persönlichen Daten entstehen jährlich beträchtliche Schäden - allein 2016 rund 8 Millionen Euro durch Phishing im Bereich Online-Banking (www.statista.de). Laut BKA-Angaben werden nur rund die Hälfte aller Fälle gemeldet, der tatsächliche Schaden liegt also weitaus höher.

Warnzeichen erkennen

Auch wenn Phishing-E-Mails immer besser getarnt sind, gibt es doch eindeutige Merkmale:

- **Betreffzeilen und Texte in fehlerhaftem Deutsch.** Der Grund: Sie werden von Computerprogrammen aus anderen Sprachen automatisch übersetzt. Ein weiterer Hinweis sind Zeichensatzfehler, wie etwa kyrillische Buchstaben oder fehlende Umlaute.
- **Vorsicht bei unpersönlicher Anrede wie „Sehr geehrte/r Kundin/Kunde“.** Banken und andere Geschäftspartner sprechen ihre Kunden grundsätzlich mit ihrem Namen an.
- **Zeitkritische Angaben im Betreff:** Drohende Kontosperrung, sofort erforderliche Zustimmung zur Datenschutzgrundverordnung oder ein dringender Datenabgleich wegen einer Gewinnbenachrichtigung – Panikmache in E-Mails sollte immer kritisch hinterfragt werden.
- **Die E-Mail fordert dazu auf, einem Link zu folgen und auf einer Internetseite persönliche Daten einzugeben.** Geldinstitute fragen diese Daten niemals per E-Mail ab - dies zählt zu den wesentlichen Sicherheitsregeln.

Ist man trotz aller Vorsicht auf einer gefälschten Webseite gelandet, erkennt man diese an folgenden Merkmalen:

- **Schreibfehler in der URL-Zeile:** Der Name der Webseite ist zwar auf den ersten Blick ähnlich zum Original, weist bei näherer Prüfung aber Fehler auf – häufig Rechtschreibfehler oder auch zusätzliche Zahlen-Buchstaben-Kombinationen.
- **Auf der Login-Seite werden TAN-Codes abgefragt.** In diesem Fall sollte man keine Daten eingeben und die Seite sofort schließen. Will man dennoch eine Login-Seite öffnen, sollten dies direkt über die Adresszeile des Browsers erfolgen – nie über einen Klick auf einen Link innerhalb der E-Mail.
- **Falsche Header-Angaben:** Mit der sogenannten Header-Auswertung lässt sich der Seiten-Betreiber über seine fälschungssichere IP-Adresse schnell und eindeutig prüfen. Eine Anleitung gibt es bei der Verbraucherzentrale: Link zur Verbraucherzentrale
- **Das Sicherheitszertifikat fehlt,** erkennbar an dem Schloss-Symbol in der Statusleiste. Die Zeile beginnt mit http:// statt mit dem verschlüsselten https://. Aber Achtung: HTTPS oder das Schloss-Symbol sind keine Garantie für die Echtheit einer Webseite. Inzwischen werden auch für Phishing-Webseiten häufig gesicherte Verbindungen oder korrekte Zertifikate eingesetzt, um potenzielle Opfer zu täuschen.

Der beste Schutz bleibt Misstrauen

Der beste Schutz gegen Phishing-Angriffe ist ein gesundes Misstrauen gegenüber allen E-Mail-Eingängen plus aufmerksames Lesen der Absender- und Betreff-Informationen sowie der Inhalte. Auf Nachrichten unbekannter Herkunft sollte man besser nicht reagieren und diese sofort löschen. Dateianhänge verdächtiger E-Mails sollten ebenfalls niemals heruntergeladen oder geöffnet werden. Daneben gibt es verschiedene technische Schutzmaßnamen, um sich vor Phishing zu schützen:

- **Antivirenprogramme auf dem neuesten Stand halten:** Viele Viren- und E-Mail-Programme erkennen gefährliche E-Mails aufgrund bestimmter Merkmale und warnen den Empfänger.
- **Die HTML-Darstellung im Mailprogramm ausschalten:** In Phishing-E-Mails verwendete Scripte sind dann nicht mehr verschleiert.
- **Aktuellste Version des Web-Browsers nutzen:** Viele Browser-Anbieter reagieren schnell auf Phishing-Methoden und färben die Adresszeile automatisch grün ein.

Bei Phishing handelt es sich um versuchten Betrug, also eine Straftat. Opfer sollten entsprechende Vorfälle zeitnah der Polizei melden und Anzeige erstatten. Wichtigste Anlaufstelle neben der Polizei ist die Verbraucherzentrale. Auf ihrer Webseite „Phishing-Radar“ veröffentlicht sie regelmäßig Meldungen zu Phishing-Angriffen.

BITel

Gesellschaft für
Telekommunikation mbH

Technik und Service – verlässlich vor Ort

Berliner Straße 260 I 33330 Gütersloh
info@bitel.de I www.bitel.de