Phishing-Angriffe auf Unternehmen: Gegen die Schwachstelle Mensch hilft keine Software

Stand: August 2019

Nahezu täglich finden sich in E-Mail-Postfächern deutscher Unternehmen offiziell aussehende Nachrichten und Mitteilungen. Doch manchmal trügt der Schein: Hinter den Mails stecken dann Kriminelle, die persönliche Angaben wie Passwörter und Log-in-Daten stehlen. Erfahren Sie in unserem dritten Teil zur Informationssicherheit alles über das Phishing-Prinzip und wie Sie sich als Unternehmen schützen.

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 Ihrer Mitarbeiter zu gelangen. Gegen den Datenklau hilft vor allem eines: Aufmerksam sein.

Fiese Masche mit großem Erfolg

„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 Mail führt so zum Erfolg und macht Phishing zum lukrativen Prinzip für Cyberkriminelle.

Auch Mitarbeiter von Unternehmen sind immer häufiger Opfer dieser Masche. Das perfide: Obwohl die Spam-Filter von Unternehmen auf Phishing-E-Mails ausgerichtet sind, rutschen insbesondere persönlich zugeschnittene E-Mails durch. Sogenannte Spear-Phishing-Attacken sind in den vergangenen Jahren um mehr als ein Drittel gestiegen. Die E-Mails von Betrügern sind bei dieser Methode direkt auf das potenzielle Opfer zugeschnitten. Dazu spähen die Cyber-Kriminellen Unternehmen und ihre Mitarbeiter gerne über soziale Netzwerke aus. Im Visier stehen dann zum Beispiel Mitarbeiter aus der Personal-Abteilung, die E-Mails als Reaktion auf eine vermeintliche Stellenanzeige ihres Unternehmens erwarten.

Datenmissbrauch mit System

Klickt der Mitarbeiter 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 beim Anklicken auf eine gefälschte Webseite. Diese ist dann meist eine echt aussehende Kopie der Original-Webseite, zum Beispiel die Startseite der vertrauten Haus-Bank. Auf den manipulierten Seiten werden Nutzer gebeten, ihre Zugangsdaten oder Passwörter 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. Bei Unternehmen ist dies besonders kritisch:

Wenn sich einmal ein Krimineller Zugang zu einem PC verschafft hat, kommt er an Geschäftsdaten heran, kann Börsenkurse manipulieren oder Produkt-Spionage betreiben. Installiert sich über angehängte Dateien dann noch Malware auf dem Firmenrechner, kann dieser Teil eines sogenannten Botnets für DDoS-Angriffe (Distributed-Denial-of-Service Attacke) werden. Hierbei werden Anfragen per Mail von einer Vielzahl von Rechnern gleichzeitig durchgeführt, um eine mutwillige Überlastung und im schlimmsten Fall sogar den Zusammenbruch eines Servers zu provozieren.

Phishing stellt eines der schwerwiegendsten Probleme deutscher Unternehmen dar, Tendenz steigend. Experten gehen davon aus, dass im Schnitt täglich drei infizierte Mails im Postfach eines Mitarbeiters landen. Das Problem: Rund 80 Prozent dieser Mitarbeiter können Phishing-E-Mails nicht von echten E-Mails unterscheiden.

Warnzeichen erkennen

Auch wenn Phishing 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.
- **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.

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.

In Unternehmen wehren zwar Firewalls die meisten Bedrohungen ab, doch am Ende bleibt der Mensch die größte Schwachstelle. Unwissenheit und ein laxer Umgang mit unbekannten E-Mails sind die häufigsten Ursachen dafür, dass Cyber-Kriminelle erfolgreich an kritische Firmendaten gelangen. Unternehmen tun deshalb gut daran, ihre Mitarbeiter regelmäßig zu schulen und deren Awareness (engl. Aufmerksamkeit) im Rahmen strategisch angelegter Cyber-Prävention zu trainieren.

Speziell durchgeführte interne Phishing-Test sind dabei sehr effektiv: In regelmäßigen Abständen versendet hierbei die IT-Abteilung präparierte Phishing-Nachrichten. Die realistisch aussehenden E-Mails lassen sich meist einfach in den Arbeitsalltag integrieren, der Erfolg misst sich an der Klickrate. Ein falscher Klick ruft Schulungsmaterialien zum richtigen Umgang mit Phishing-E-Mails auf, sodass die Mitarbeiter das korrekte Verhalten direkt am Objekt erlernen und nachhaltig im Gedächtnis speichern.

BITel

Gesellschaft für
Telekommunikation mbH

Technik und Service – verlässlich vor Ort

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

GRUPPE GRUPPE