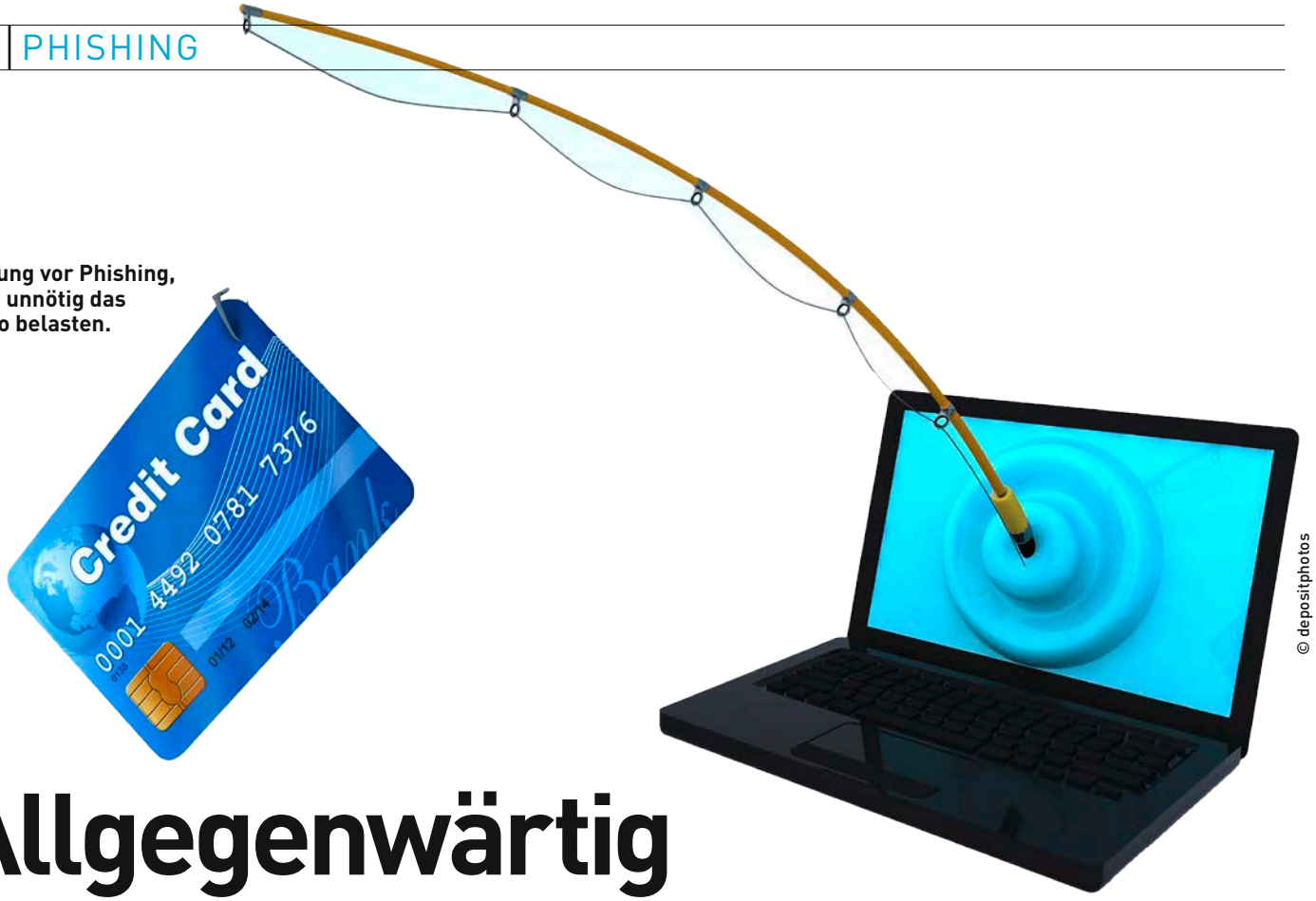

Achtung vor Phishing, nicht unnötig das Konto belasten.

Allgegenwärtig und äusserst gefährlich

In jüngster Zeit konnte viel über Phishing-Angriffe gelesen werden. Mit mehr oder weniger trivialen E-Mails versuchen die Angreifer an persönliche Informationen, vor allem aber an Zugangsdaten und Passwörter zu gelangen.

Von Andreas Wisler

Phising, ein Kunstwort aus Password Harvesting Fishing, bezeichnet den Versuch, an Benutzernamen, Codes, Passwörter oder andere vertrauliche Informationen zu kommen. Die Angriffsmöglichkeiten haben dabei verschiedene Gesichter. Oft werden, um Vertrauen zu erwecken, bekannte Firmen als Absender verwendet: Beispielsweise Credit Suisse. Der Empfänger wird darauf hingewiesen, dass man den Online-Banking-Account infolge eines Hackergangriffs gesperrt habe. Zum Reaktivieren müsse nur auf den untenstehenden Link geklickt werden. Oder ein weiteres Beispiel: DHL habe ein Paket zustellen wollen. Da jedoch niemand zu Hause gewesen sei, müsse nun ein Formular ausgefüllt werden, wann der DHL-Bote vorbeikommen könne. Bei beiden Angriffen ist grösste Vorsicht geboten. Immer wieder wird versucht, beim Aufruf der verlinkten Seite eine Malware (Virus, trojanisches Pferd oder dergleichen) zu installieren. Und dies auch, wenn das Formular gar nicht ausgefüllt wird. Daher gilt, diese E-Mails umgehend in den Papierkorb (Trash) zu verschieben.

Hauptsache, es wird auf den Link geklickt

Viele Menschen sehen sich nicht im Fokus eines Angriffs. «An meinen Daten hat eh niemand Interesse» oder «mit meinen Daten kann eh niemand etwas anfangen», sind häufig gehörte Aussagen. Dies mag stimmen, denn personenbezogene Angriffe sind (noch) eher die Ausnahme. Aber irgendwo in einem Gästebuch einen Eintrag mit der eigenen E-Mail-Adresse getätigt, an einem Wettbewerb mitgemacht oder auf der eigenen Homepage die E-Mail in uncodierter Form angebracht, und schon ist die E-Mail-Adresse auch für einen Angreifer sichtbar. Es existiert auch ein Adress-Handel. Für wenige Dollar können im Internet tausende (gültige!) E-Mail-Adressen gekauft werden. Wenn von 1000 angeschriebenen Personen nur schon wenige auf den Angriff hereinfallen, kann sich dies für einen Angreifer bereits lohnen.

In der immer stärker vernetzten Welt hinterlässt man oft unbewusst seine digitalen Spuren. In den Nachrichten des Vereins wird von einem Wettkampf oder einem Anlass erzählt und die Personen mit Namen veröffentlicht. Werden diese anschliessend mit Facebook, Xing, Twitter oder dergleichen kombiniert, kommen viele Informationen über einen Menschen zusammen. Yasni.ch ist eine spezialisierte Personensuchmaschine: aber Vorsicht beim Besuch der Seite! Diese sollte nur mit einem aktuellen gepatchten Betriebssystem und aktuellem Antivirenprogramm besucht werden. Auf der Seite können Informationen über eine Person auf einfache Art gesucht werden. Nur den

Namen eingeben und einen Moment warten. Die Suchmaschine durchsucht verschiedene andere Seiten und stellt alle Antworten übersichtlich dar. Die Informationen können anschliessend für einen personenbezogenen Angriff verwendet werden.

Mitarbeitende sensibilisieren

Der aktuelle 21. MELANI-Halbjahresbericht (Melde- und Analysestelle Informationssicherung, www.melani.admin.ch) zeigt, dass Phishing nach wie vor ein grosses Thema ist. Praktisch täglich stellen die MELANI-Leute mehr oder weniger grossflächige Phishing-Kampagnen fest. Dabei sind es oft triviale Angriffe wie gefälschte Steuerformulare oder E-Mails von angeblichen Banken. Aber auch aktuelle Themen wie die Flüchtlingsproblematik versuchen den E-Mail-Empfänger in die Irre zu führen. Vermehrt werden jedoch professionelle E-Mails von Angreifern in Umlauf gebracht. Die Anrede ist nicht mehr Pauschal oder enthält nur die E-Mail-Adresse, sondern der Leser wird korrekt mit Vor- und Nachnamen angesprochen. Dies soll das Vertrauen in die E-Mail verstärken. Auch der Autor hat schon einige solcher E-Mails erhalten. Bei einigen musste auch er mehrmals hinschauen, um den Phishing-Angriff zu erkennen.

Im geschäftlichen Umfeld könnte die E-Mail beispielsweise vom Chef kommen, mit der Bitte, eine spezielle Seite zu besuchen; im privaten Umfeld von einer ehemaligen Schulkollegin, die man schon lange nicht mehr gesehen hat. Werden in der E-Mail Dinge erwähnt, die eigentlich niemand anderes kennen kann als vertraute Personen, ist das Misstrauen viel geringer. Der Schritt, auf den Link zu klicken, ist dann nicht mehr weit entfernt.

Um die Mitarbeitenden für solche Gefahren zu sensibilisieren, kann ein gezielter Phishing-Angriff durchgeführt werden. Ein Szenario könnte zum Beispiel wie folgt ablaufen:

1. E-Mail im Namen des Geschäftsführers mit der Bitte, an einer Umfrage zur Erhöhung der Informationssicherheit mitzumachen.
2. Beim Klick erscheint eine Webseite, die genau im Design der Firmenseite erstellt wurde. Darin befinden sich einige Fragen zum Umgang mit dem Passwort (Länge, Änderungsrhythmus, wo aufgeschrieben, wann wem mitgeteilt usw.). Am Ende der Umfrage befindet sich ein Feld zur Kontrolle der Passwortstärke. Ein Balken von Rot nach Grün zeigt, wie sicher das Passwort wirklich ist. Fett steht der Hinweis «wird nicht gespeichert».
3. Beim Absenden werden alle Angaben an den Server geschickt, inklusive dem eingegebenen Passwort.

Die Auswertungen von über einem Dutzend durchgeführten Angriffen zeigt ein ernüchterndes Bild. Obschon immer wieder von Phishing gelesen werden kann, klicken über zwei Drittel der angeschriebenen Personen auf den Link. Etwa die Hälfte füllt auch das Formular aus. Hätte es sich um einen echten Angriff gehandelt, wäre das Firmenkennwort in die falschen Hände geraten. Doch schon der Klick auf den Link könnte, wie bereits erwähnt, reichen, den Firmen-Rechner mit einer Malware zu verseuchen. Die Auswertung der Zugriffe zeigt, dass die benutzten Geräte (installierter Browser und enthaltene Plug-ins) oft nicht auf einem aktuellen Patchstand sind und so leicht missbraucht werden können.

Wie kann man sich vor Phishing-E-Mails schützen?

Um sich vor Phishing-Angriffen zu schützen, wird folgende Vorgehensweise empfohlen:

- Persönliche Informationen sollten nie preisgegeben werden.
- Kein seriöser Dienstleister wird seine Kunden jemals per E-Mail-Nachricht oder Telefon zur Angabe von Passwörtern oder Kreditkartendaten auffordern.
- Geben Sie die Internetadressen nach Möglichkeit manuell ein oder überprüfen Sie diese vor einem Klick darauf.
- Gerne werden auch Schreibfehler oder Buchstabendreher für solche Angriffe verwendet. Auch könnte die Erweiterung falsch sein (.com anstelle .ch).
- Misstrauen Sie E-Mails, die Sie unaufgefordert bekommen. Besonders vertrauenswürdige Firmen werden gerne als gefälschte Absender-Adressen missbraucht. Dabei werden auch Schweizer Firmen für gezielte Phishing-Angriffe auf Schweizer E-Mail-Adressen verwendet. Bekannte Firmen für solche Angriffe in den vergangenen Monaten waren Swisscom, das Bundesamt für Energie oder Läderach Schokolade, um nur drei zu nennen.
- Seien Sie vorsichtig, wenn Sie E-Mails bekommen, die eine Aktion von Ihnen verlangen und ansonsten mit Konsequenzen (Geldverlust, Strafanzeige, Konto- oder Kartensperrung, verpasste Chance, Unglück) drohen.
- Verschiedene Firmen bieten ein Formular oder eine E-Mailadresse an, mit welchen ein Phishing-Angriff gemeldet werden kann.

Häufig per Telefon

Zugenommen haben auch Phishing-Angriffe per Telefon. Dabei wird versucht, den Angerufenen auf eine Webseite zu locken oder persönliche Informationen preiszugeben. Gerade angebliche Anrufe vom Microsoft-Support (oft in Englisch) verunsichern den Windows-Nutzer. Die Betrüger rufen wahllos Haushalte an und verlangen, dass auf dem Computer des Angerufenen dringend eine Sicherheitssoftware installiert werden müsse, da der Support einen Fehler beziehungsweise einen Schädling festgestellt hat. In einem zweiten Schritt werden dann Zugangsdaten oder die Kreditkartennummer abgefragt.

Mit all diesen Angriffen wird versucht, an die Hilfsbereitschaft oder an die Ängstlichkeit der angeschriebenen Personen zu appellieren. Da immer wieder Personen auf diese Art von Angriffen hereinfallen, hören diese auch nicht auf, sondern nehmen nur zu. Es ist wichtig, bei seltsamen E-Mails Vorsicht walten zu lassen. Lieber einmal zu viel eine E-Mail löschen, als auf einen Angriff hereinfallen. Mit gesunder Skepsis können viele Angriffe erkannt und erfolgreich verhindert werden.

Übrigens – wer ein Phishing-E-Mail erhalten hat, sollte dies der Plattform www.antiphishing.ch melden. ■

ANDREAS WISLER
Dipl. Ing. FH, CISSP, CISA, Lead Auditor ISO 27001 und 22301, IT-Sicherheitsbeauftragter BSI, CEO der Firma goSecurity GmbH