Ein Fall aus der Praxis des (Senioren-)Sicherheitsberaters; heute: Phishing per Brief (Folge 8 der Reihe „Aber sicher!")

Phishing ist ein Kunstwort aus Passwort und Fishing. Es bezeichnet ein Verfahren, das mit gefälschten E-Mails oder Webseiten unbemerkt persönliche Daten auf fremden Rechnern ausspioniert. PIN und weitere wichtige Zugangsdaten werden also „abgefischt". Betroffen hiervon sind bisher vorwiegend Home-Banking-Kunden. Diese erhalten fingierte E-Mails, angeblich von der eigenen Bank, die täuschend echt aufgemacht sind und zumeist einer „Sicherheitsaktualisierung" dienen. Im Anschreiben warnen die Betrüger kurioserweise vor der eigenen Masche: Um sich vor unerlaubtem Zugriff auf persönliche Daten zu schützen, sollen sich die Kunden über einen Link auf eine Internetseite einwählen und die persönlichen Daten aktualisieren. Der Link führt jedoch auf die Internetseite der Betrüger, die der entsprechenden Hausbank zum Verwechseln ähnlich sieht. Hier werden die Bankkunden dann aufgefordert, Kontonummer, PIN und TAN einzugeben, mit deren Hilfe die Abzocker dann das Konto abräumen können.

Ein Freund wies mich vor ein paar Tagen auf eine neue Version dieser Betrugsmasche hin: Phishing per Brief. Verschiedene Polizeidienststellen warnen bereits vor dieser neuen Form des Betrugs.

Wie funktioniert Phishing per Brief?

Kriminelle versuchen, Debit- und Kreditkarteninhaber (dazu gehört auch die girocard – ehemals ec-Karte) zur Preisgabe ihrer Kartendaten zu verleiten. Das Hinterhältige dabei ist, dass die Betrüger jetzt einen Weg benutzen, der gemeinhin als seriös und vertrauenswürdig gilt: ein Anschreiben, das mit der Post nach Hause kommt. Auch hier werden die Bankkunden mit täuschend echt wirkenden Briefen von Geldinstituten oder Kreditkartenunternehmen wie VISA, MasterCard usw. unter dem Vorwand einer Sicherheitsüberprüfung aufgefordert, ihre Kartendaten auf einer bestimmten Internetseite einzugeben. Um der Aufforderung Nachdruck zu verleihen, wird in dem Brief angedroht, dass bei unterlassener „Sicherheitsüberprüfung" die Karte nach 14 Tagen gesperrt wird.

Wer nun in Panik auf die bezeichnete Internetseite geht, wird feststellen, dass sie ebenso echt wirkt wie der erhaltene Brief. Das Einzige, was solche Briefe und Websites als Betrugsmanöver entlarvt, ist ihr Inhalt selbst – nämlich die Aufforderung, Kartendaten einschließlich Prüfziffer und Geheimzahl auf einer bestimmten Internetseite einzugeben.

Wie kann ich mich vor solchen Straftaten schützen?

- Ignorieren Sie derartige Briefe und bedenken Sie: Niemals wird Ihre Bank, Sparkasse oder ein Kreditkartenunternehmen schriftlich, per E-Mail oder am Telefon von Ihnen verlangen, ihre Kartendaten preiszugeben.

- Steuern Sie die Internetseite Ihres Geldinstitutes ausschließlich über Ihre fest eingerichteten Bookmarks, die Favoritenliste oder per händischer Eingabe an. Folgen Sie insbesondere keinen Links in E-Mails.
- Überprüfen Sie regelmäßig sämtliche Stände Ihrer Konten. Stellen Sie Unregelmäßigkeiten fest, so setzen Sie sich unverzüglich mit Ihrem Geldinstitut in Verbindung.
- Grenzen Sie den Überziehungsrahmen oder das täglich verfügbare Überweisungslimit auf ein für Sie sinnvolles Maß ein. Ohne Begrenzung kann der Schaden meist wesentlich höher sein.