Phishing

Informationspapier zur Problematik des Phishing

Was bedeutet Phishing?

„Phishing“ bezeichnet eine Methode des Diebstahls vertraulicher Daten von Internet-Nutzern, z. B. Kreditkartennummern, Bankverbindungen, PIN oder auch Zugangsdaten zu Internetdiensten.

Der Begriff „Phishing“ stammt dabei aus der Hacker-Szene: Der Angreifer präsentiert dem Internetnutzer einen Köder (eine gefälschte Webseite) und „fischt“ so nach dessen persönlichen Daten. Der Begriff Fishing wurde zu „Phishing“ (*F*ischen nach *P*asswörtern) verfremdet.

Wie funktioniert Phishing?

Beim Phishing werden von Angreifern gefälschte E-Mails an zahlreiche Nutzeraccounts versendet, mit der Aufforderung sich beim Kreditinstitut, dem Online-Shop usw. zu identifizieren. Beigefügt ist meist eine URL (d.h. ein Internet-Link) auf eine entsprechend gefälschte Webseite, die auf den ersten Blick wie die Originalseite aussieht. Die Anfrage ist meist als dringlich oder wichtig formuliert und gibt technische oder organisatorische Maßnahmen als Grund an. Der Internetnutzer sieht sich daher u. U. genötigt, seine vertraulichen Daten einzugeben. Diese werden vom Angreifer auf der gefälschten Webseite gesammelt und können später für einen Missbrauch verwenden werden.

Entwicklung von Phishing

Anfänglich sind Phishing-Mails noch im fehlerhaften Deutsch, Englisch oder in einem auffallend schlechtem Layout verschickt worden, so dass für den Internetnutzer diese Fälschungen leicht erkannbar waren. In letzter Zeit fällt dies immer schwerer, da die Angreifer beim Fälschen der E-Mail immer professioneller werden.

Auch die Gefährlichkeit steigt: Phishing-Mails werden im zunehmenden Maß mit anderen Angriffen wie Computerviren, Trojanern und Würmern kombiniert. Durch den Verbindungsaufbau zur gefälschten Webseite können automatisch Schadprogramme auf dem Nutzer-PC installiert werden. Diese sammeln im Hintergrund Informationen und senden sie an den Angreifer. Er erhält damit zusätzliche Daten vom Internetnutzer, noch über Identitätsdaten aus der gefälschten Webseite hinaus. Je nach Umfang der gestohlenen Daten kann der Angreifer Transaktionen, Bestellungen usw. zu seinen Gunsten unter der Identität des Nutzers durchführen.

Nach Aussage der „Anti-Phishing-Working-Group“[1] (www.antiphishing.org) ist weltweit seit Monaten ein Zuwachs an Vorfällen zu verzeichnen, aktuell monatlich bis zu 24%. Wie auch bei Spam gestaltet es sich beim Phishing schwierig, den Absender gefälschter E-Mails sowie den Inhaber der gefälschten Webseite ausfindig zu machen. Dies liegt unter anderem daran, dass die Täter sehr oft aus dem Ausland agieren.

[1] Die Anti-Phishing-Working-Group ist eine Wirtschaftsinitiative zur Bekämpfung von Phishing-Mails.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Postadresse: Postfach 640144, 10047 Berlin
Hausadresse: Albrechtstr. 10, 10117 Berlin
Tel.: 030/27576-0, Fax: -400
E-Mail: bitkom@bitkom.org
Internet: www.bitkom.org

Präsident:
Willi Berchtold

Geschäftsführung:
Dr. Bernhard Rohleder (Vors.)
Dr. Peter Broß

Ansprechpartner:
Dr. Sandra Schulz
Bereichsleiterin
Sicherheit
Postfach 640144, 10047 Berlin
Tel.: 030/27576-242, Fax: -247
E-Mail: s.schulz@bitkom.org

Rechtssituation in Deutschland

Phishing-Mails sind nach aktueller Rechtslage nicht strafbar, da nur eine straflose Vorbereitungshandlung vorliegt. Erst wenn die gestohlenen Daten tatsächlich für einen Betrug mit Vermögensschaden genutzt werden, liegt ein Computerbetrug nach § 263a StGB vor. Auch erst dann kann die Strafverfolgungsbehörde aktiv werden. Ein solches nachträgliches Eingreifen ist in der Regel nicht aussichtsreich, da der Schaden bereits eingetreten ist, z. B. bei Transaktionen vom Bankkonto des bestohlenen Internetnutzers zu Gunsten des Angreifers.

BITKOM setzt sich daher dafür ein, dass schon die Phishing-Attacke selbst unter Strafe gestellt wird. Damit können Strafverfolgungsbehörden auch schon vor dem Eintreten eines konkreten Schadensfalls aktiv werden. Weitere Informationen zur bisherigen Rechtssituation sowie zu rechtlichen Lösungsmöglichkeiten sind im BITKOM-Positionspapier zur fehlenden Strafbarkeit von Phishing- und Spoof-Attacken im Internet zu finden.

Technisch-organisatorischer Schutz

Technisch-organisatorische Schutzmaßnahmen spielen neben der Nuterzaufklärung eine zentrale Rolle bei der Verhinderung von Phishing-Mails.

Herkömmliche Sicherheitstechniken wie beispielsweise Firewalls oder Virenschutzprogramme bieten einen grundsätzlichen Schutz gegen Phishing-Attacken. Phishing-Mails, die mit Schadprogrammen kombiniert sind, können erkannt und herausgefiltert werden. Eine regelmäßige Aktualisierung der Firewall bzw. des Virenschutzprogramm ist dabei notwendig.

Im Mittelpunkt allgemeiner technischer Lösungen stehen aber - wie auch bei Spam - Filtersysteme, wie sie von vielen Anbietern im Rahmen von E-Mail-Diensten oder als separate Programme angeboten werden. Den größten Erfolg versprechen dabei Systeme, die die verschiedenen Kennzeichen von Phishing-Mails (bestimmte Kennwörter, Layout-Elemente, spezielle Absender) in einem intelligenten Analyseverfahren kombinieren. Bei allen Ansätzen zur Ausfilterung von Phishing-Mails sind die Rechte des Nutzers zu beachten. Hier sei auf die Stellungnahme des BITKOM zu Spam verwiesen.

Unternehmen, deren Webseiten oft gefälscht werden, bieten zudem spezielle technische Lösungen an. Diese stellen etwa sicher, dass eine vertrauliche direkte Kommunikation gewährleistet ist und somit kein sogenannter „Man in the Middle“ Angriff erfolgen kann. Andere Ansätze setzen dabei Kennzeichnungssysteme (Sicherheitssymbole: Schloß, Schlüssel) ein, die im Browser anzeigen, ob man sich tatsächlich auf einer Seite des jeweiligen Anbieters befindet.

Parallel setzen die Unternehmen verstärkt auf Nutzeraufklärung, indem sie durch Informationen auf den Unternehmenswebseiten, in Leitfäden und durch redaktionelle Berichte in den Medien dazu beitragen, die Nutzer für die Phishing-Gefahr zu sensibilisieren und zu angemessenen Vorsichtsmaßnahmen anzuhalten.

Wie schützt man sich gegen Phishing?

Wie auch in der realen Welt sollte man im Internet vertrauliche Daten nur an absolut vertrauenswürdige Stellen übermitteln, über deren Authentizität (Echtheit) man sich im Klaren ist. Der Internetnutzer muss vor allen Dingen einen bewussten Umgang mit seinen persönlichen Daten pflegen.

Folgende Verhaltensregeln sind zu beachten, um nicht Opfer eines Phishings-Betruges zu werden:

- Misstrauen Sie grundsätzlich *allen* unangekündigten E-Mails, die Daten von Ihnen abfragen, auch wenn die E-Mail scheinbar von einer vertrauenswürdigen Adresse stammt. Besonderes Misstrauen ist angesagt, wenn eine E-Mail ihren Empfänger zu sofortigem Handeln auffordert und andernfalls negative Konsequenzen, zum Beispiel die Sperrung des Zugangs, androht.
- Kreditinstitute versenden in der Regel keine unverlangten E-Mails an ihre Kunden. Von daher die E-Mail nicht öffnen, gleich löschen. Ist sie doch geöffnet, auf keinen Fall den Anhang öffnen.
- Antworten Sie nicht auf verdächtige E-Mails, da die Antworten als Lebenszeichen verstanden werden und weitere Phishing-Mails nach sich ziehen könnten. Vermeiden Sie daher auch automatische Antworten, wie z. B. Abwesenheitsnotizen. Verwenden Sie besser eine sogenannte "Positivliste", d. h. die Abwesenheitsnotiz wird nur an die in Ihrem Adressbuch gespeicherten Adressen gesendet.
- Nutzen Sie, wenn Sie Zweifel an der Echtheit einer Mail haben, nicht den in der Mail integrierten Link, sondern geben Sie die Ihnen bekannte Startadresse des jeweiligen Angebots selbst in die Adresszeile des Browsers ein.
- Fragen Sie im Zweifel telefonisch oder persönlich bei Ihnen bekannten Ansprechpartnern oder Kontaktnummern nach, wenn Sie über Folgen der Nichtbeachtung von unklaren E-Mails sind: Verwenden Sie NICHT die in der E-Mail angegebenen Kontaktpunkte.
- Gehen Sie grundsätzlich auf sensible Webseiten nur über eine eigene Eingabe der Adresse in das Adressfeld im Browser oder steuern Sie diese über die Favoriten in ihrem Internetbrowser an.
- Achten Sie bei der ersten Eingabe von Webseiten auf die korrekte Schreibweise. Auch ein kleiner Rechtschreibfehler kann Sie auf eine gefälschte Webseite führen.
- Nutzen Sie gegebenenfalls sogenannte “Password Manager“-Produkte, die vor der Eingabe Ihrer persönlichen Daten die Webseite auf Korrektheit prüfen.
- Achten Sie bei der Eingabe von vertraulichen Daten auf das Sicherheitssymbol Ihres Browsers[2]. Es zeigt an, dass die Seite über ein Sicherheits-Zertifikat verfügt und die Daten verschlüsselt übertragen werden. Eine Überprüfung des Sicherheits-Zertifikats ist sinnvoll. Details zum Zertifikat erhalten Sie durch einen Doppelklick auf das Sicherheitssymbol. Vergleichen Sie die dortigen Angaben (Zertifikatseigentümer, Ausgabestelle, Gültigkeitsdatum) mit denen, die Sie von Ihrer Bank erhalten haben bzw. fragen Sie dort nach. Nur so können Sie sicher sein, dass die verschlüsselte Verbindung nicht zu einem Betrüger führt.

Falls sie den Verdacht haben, dass Sie Opfer eines Phishingbetruges geworden sind, melden Sie sich umgehend beim entsprechenden Unternehmen.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt 1300 Unternehmen, davon 700 Direktmitglieder mit etwa 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

[2] Internet Explorer: Geschlossenes Vorhängeschloss; Netscape Navigator: ungebrochener Schlüssel, jeweils rechts unten im Browser-Fenster,