Was ist Phishing?
Bitdefender E-Guide

Inhalt

Bitdefender

Was ist eigentlich Phishing?

Auf den ersten Blick scheint alles in Ordnung zu sein: In einer freundlichen E-Mail wird Leon von seiner Bank oder einem Online-Versandhaus aufgefordert, er möge doch seine Daten verifizieren, also Anmeldenamen, Passwort, PIN et cetera. Als Grund wird angeführt, es sei ein "Zugriff Unbefugter" auf das Konto von Leon erfolgt. Und um ihm das "Verifizieren" so einfach wie möglich zu machen, enthält die Nachricht einen Link zu einer Internet-Seite mit einem Online-Formular. Dort möge er doch die entsprechenden Daten eingeben.

Sollte Leon das tun, wird er kurze Zeit später feststellen, dass tatsächlich "Unbefugte" auf sein Konto bei der Bank zugegriffen haben - und es leer geräumt haben. Oder die Täter kaufen auf seine Kosten bei einem Online-Händler ein, vorzugsweise teure Unterhaltungselektronik-Geräte und Computer. Kurzum: Leon ist Opfer einer Phishing-Attacke geworden.

Nach Passwörtern und PINs "angeln"

Der Begriff Phishing leitet sich aus zwei englischen Wörtern ab: "Password" und "Fishing". Das Angeln nach Passwörtern und anderen Account-Daten erfreut sich in Kreisen von Cyber-Kriminellen großer Beliebtheit. Laut dem "E-Threat Landscape Report" von Bitdefender stieg im ersten Halbjahr 2012 der Anteil der Phishing-Nachrichten unter den Spam-E-Mails um 1 Prozent auf 2,5 Prozent. Ein Ende dieser Entwicklung ist nicht abzusehen.

Die Masche, die Internet-Betrüger bei Phishing verwenden, ist immer dieselbe: Das potenzielle Opfer erhält eine Nachricht von einem vermeintlich seriösen Absender, etwa einer Bank, einem Bezahldienst wie PayPal oder einem Online-Auktionshaus. Beliebt sind auch Betreiber großer Online-Spieleplattformen wie Battlenet. In der E-Mail wird der Empfänger gebeten, seine Daten zu aktualisieren. Der Grund: Die Kreditkarte des Empfängers sei abgelaufen, oder ein Passwort müsse aus Sicherheitsgründen erneuert werden. In einem anderen Fall sind angeblich die Zugangsdaten durch einen technischen Fehler verloren gegangen.

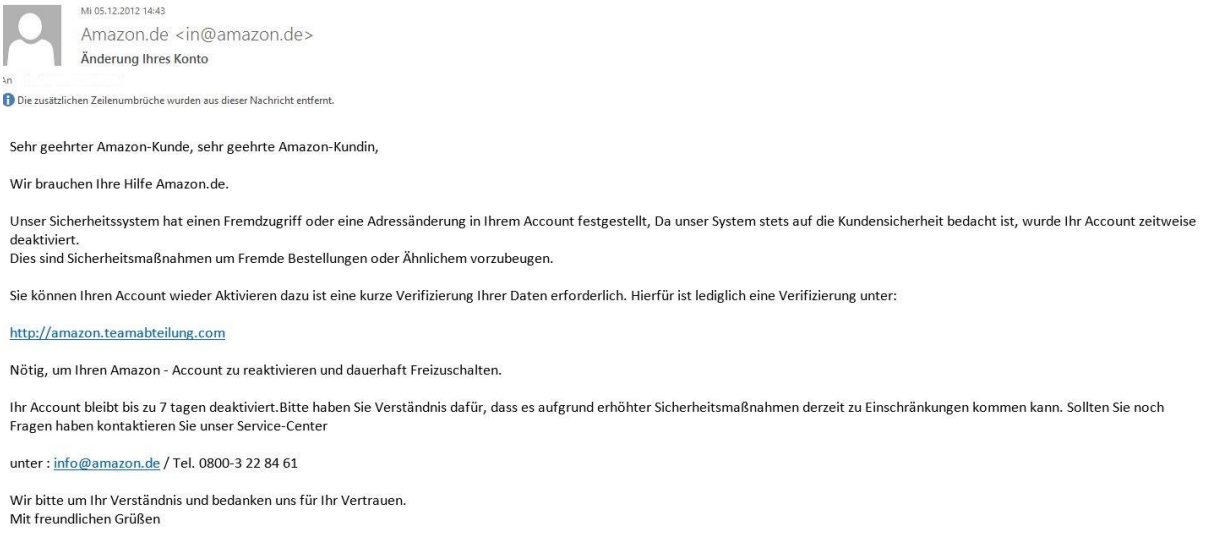
Einige dieser E-Mails sind leicht als Fälschungen zu erkennen, vor allem dann, wenn der Adressat ein Benutzerkonto bei einer Bank oder einem Online-Versender verifizieren soll, dessen Kunde er gar nicht ist. Deshalb bevorzugen Phishing-Betrüger Unternehmen als Tarnmantel, die über eine große Zahl von Kunden verfügen. Das erhöht die Wahrscheinlichkeit, dass sich der Empfänger von der Phishing-Nachricht angesprochen fühlt.

Perfekte potemkinsche Dörfer

Die meisten Phishing-E-Mails sind kaum von "richtigen" Nachrichten zu unterscheiden: Schrift, Aufmachung, Absenderangaben und Firmenlogo sind exakt dieselben, die renommierte Unternehmen wie beispielsweise Amazon, eBay oder PayPal verwenden.

Der wichtigste Bestandteil einer Phishing-E-Mail ist jedoch ein integrierter Internet-Link. Er führt angeblich zu einer Web-Seite des betreffenden Unternehmens. Dort soll der Adressat seine Daten eingeben.

Wer diesen Link anklickt, landet jedoch auf einer Seite, welche die Cybercrime-Fachleute zu diesem Zweck angelegt haben. Oft sind diese Web-Seiten nur wenige Stunden lang online. Gibt der Empfänger der Phishing-Nachricht dort Kreditkartennummern, Passwörter et cetera ein, liefert er diese Daten den Kriminellen gewissermaßen frei Haus. Ein Hinweis, dass es sich um eine nachgebaute Firmen-Web-Seite handelt, ist in manchen Fällen die angegebene Internet-Adresse: Wenn beispielsweise statt www.amazon.de/... eine eigenartige Adresse wie http://www.xyzkarsyzsykwaro-23incorp.ca auftaucht, ist Vorsicht angesagt. Allerdings gehen Profis dazu über, mithilfe von Javascripts die Adressleiste seriöser Unternehmen "nachzubauen" oder scheinbar echte Internet-Adressen zu verwenden, die in Wirklichkeit auf eine Phishing-Web-Seite verweisen. Ein Beispiel aus der Praxis ist http://amazon.teamabteilung.com – eine Seite, die im Dezember wenige Tage lang aktiv war, um die Account-Daten von Kunden von Amazon "abzusaugen".



Mi 05.12.2012 14:43

Amazon.de <in@amazon.de>

Änderung Ihres Konto

An

Die zusätzlichen Zeilenumbrüche wurden aus dieser Nachricht entfernt.

Sehr geehrter Amazon-Kunde, sehr geehrte Amazon-Kundin,

Wir brauchen Ihre Hilfe Amazon.de.

Unser Sicherheitssystem hat einen Fremdzugriff oder eine Adressänderung in Ihrem Account festgestellt, Da unser System stets auf die Kundensicherheit bedacht ist, wurde Ihr Account zeitweise deaktiviert.
Dies sind Sicherheitsmaßnahmen um Fremde Bestellungen oder Ähnlichem vorzubeugen.

Sie können Ihren Account wieder Aktivieren dazu ist eine kurze Verifizierung Ihrer Daten erforderlich. Hierfür ist lediglich eine Verifizierung unter:

http://amazon.teamabteilung.com

Nötig, um Ihren Amazon - Account zu reaktivieren und dauerhaft Freizuschalten.

Ihr Account bleibt bis zu 7 tagen deaktiviert.Bitte haben Sie Verständnis dafür, dass es aufgrund erhöhter Sicherheitsmaßnahmen derzeit zu Einschränkungen kommen kann. Sollten Sie noch Fragen haben kontaktieren Sie unser Service-Center

unter : info@amazon.de / Tel. 0800-3 22 84 61

Wir bitte um Ihr Verständnis und bedanken uns für Ihr Vertrauen.
Mit freundlichen Grüßen

Bitdefender

Mit Spear Phishing gezielte Angriffe starten

Ein neues und von Phishing-Betrügern mittlerweile hoch geschätztes Betätigungsfeld sind Social-Media-Plattformen wie Facebook, Google+ und LinkedIn. Die Zugangsdaten von Nutzern solcher Dienste sind deshalb interessant, weil sie die Basis für ganz spezielle Phishing-Angriffe bilden: Spear Phishing.

Normale Phishing-Angriffe erfolgen nach dem Gießkannen-Prinzip: Die Angreifer versenden die Nachrichten wahllos an eine große Zahl von E-Mail-Adressen, frei nach dem Motto: "Irgendjemand wird schon anbeißen!". Bei Spear Phishing handelt es sich um zielgerichtete Attacken auf einzelne oder wenige Personen. Diese sind häufig Mitarbeiter von Firmen oder Behörden.

Ein Krimineller kann dazu beispielsweise einen gekaperten Facebook-Account nutzen: Als "Freund" des Empfängers getarnt, sendet er diesem eine Nachricht. Darin bittet er den "Kollegen", ihm ein – angeblich – vergessenes Passwort für einen Rechner mitzuteilen, oder er übermittelt mit der Nachricht ein Dokument, das mit Schadsoftware infiziert ist. Das Ziel solcher Angriff ist, an verwertbare interne Informationen zu gelangen, etwa Kundendaten oder Entwicklungsunterlagen.

Schutz vor Phishing-Angriffen

Die erste und wichtigste Maßnahme, um Phishing-Angriff abzuwehren, besteht darin, auf jedem Endgerät die Schutzsoftware eines etablierten IT-Sicherheitsunternehmens zu installieren, beispielsweise Bitdefender Total Security 2013, Bitdefender Sphere 2013 oder Bitdefender Mobile Security. Und "jedes" Endgerät bedeutet auch "jedes": PCs, Macs, Smartphones und Tablet-Rechner, und das unabhängig davon, ob darauf Windows, Android, iOS oder andere Betriebssysteme laufen. Solche Sicherheitssoftware analysiert alle eingehenden E-Mails und filtert Spam-Nachrichten und Phishing-Mails aus.

Zudem analysieren IT-Sicherheitsunternehmen wie Bitdefender ständig IP-Adressen und Internet-Seiten daraufhin, ob sie von Cyber-Kriminellen für ihre Zwecke genutzt werden. Die Resultate werden umgehend in Form von Updates in die Schutzsoftware integriert. Ruft ein Anwender dann eine dubiose Web-Seite auf, warnt ihn das Programm.

Wichtige Tipps zum Schutz vor Phishing

- Höchste Vorsicht bei E-Mails walten lassen, in denen Links zu Web-Seiten enthalten sind.
- Die IT-Sicherheitssoftware regelmäßig aktualisieren beziehungsweise die automatische Update-Funktion aktivieren.
- IT-Sicherheitssoftware einsetzen, die nicht nur vor Viren, Würmern und anderer Schadsoftware schützt, sondern auch Spam-E-Mails blockt und Schutz in sozialen Netzwerken bietet.
- Internet-Adressen der eigenen Bank oder von Bezahldiensten von Hand in den Browser eingeben und nicht auf den Link in einer – verdächtigen – E-Mail klicken.

Wichtig ist zudem, dass Internet-Nutzer ein gesundes Misstrauen an den Tag legen. Seriöse Unternehmen fordern ihre Kunden niemals per E-Mail auf, spezielle Links anzuklicken und auf den entsprechenden Internet-Seiten vertrauliche Daten einzugeben. Nötigenfalls lieber direkt bei der Bank oder der Servicestelle des betreffenden Unternehmens anrufen. Keinesfalls sollte er der Empfänger ein Unternehmen über die E-Mail-Adresse kontaktieren, die in einer verdächtigen E-Mail angeführt ist. In diesem Fall erhält er zwar eine Antwort, jedoch vom Cyber-Kriminellen.