Vorsicht beim Weihnachtsshopping:
Betrüger nutzen PayPal mit neuer Masche

Die eigene (Cyber)Sicherheit im Blick – das muss auch in der hektischen Festsaison Priorität sein. Denn die Betrüger setzen bei Routine und Bekanntem an – für Ungeübte kaum zu erkennen. Sophos gibt Tipps anhand des aktuellen Fallbeispiels PayPal.

In Weihnachtsgeschenke – auch in diesen besonderen Zeiten – wird in Deutschland gern investiert und für die Liebsten oder sich selbst tief in die Tasche gegriffen. Die Kaufsaison wird spätestens im November intensiv mit Black Friday-, Cyber Monday- und unzähligen weiteren Schnäppchen-Angeboten beworben. Das Risiko, einem Betrüger auf den Leim zu gehen, ist in dieser Zeit noch höher als sonst, denn für Cybergangster besteht jetzt Hochsaison.

Der Zahlungsdienstleister PayPal wurde von Betrügern nun für eine besonders gemeine Trickserei benutzt, die zum Glück aber einen entscheidenden Vorteil hat: man erkennt relativ einfach, dass es sich um einen Bluff handeln muss. Was aber leider kein Garant dafür ist, dass die Kriminellen nicht doch den einen oder anderen unvorsichtigen Nutzer an die Angel bekommen. Allerdings offenbart der Betrug auch, dass es für die Kriminellen erstaunlich leicht war, diesen aufzusetzen und weder gefälschte E-Mails noch getürkte Webseiten notwendig waren. Denn die Betrüger nutzen einen PayPal Service, um ihren initialen Kontakt via offizieller PayPal-Server herzustellen.

Bevor die neuen Verfahren beschrieben werden, noch schnell ein Ausflug in die „traditionelle“ Scam-Werkstatt mit gefälschten E-Mails und gefälschten Websites:

Eine ***gefälschte E-Mail*** tut so, als sei sie von bekannten Unternehmen oder Domains, indem sie typischerweise eine glaubhafte E-Mail-Adresse in das Von:-Feld setzt. Zudem untermauert sie ihre Herkunft mit Logos, Slogans oder anderen Kontaktdetails, die sie von der Marke kopiert hat. In die Absendezeile lässt sich nahezu alles einsetzen, völlig unabhängig von der tatsächlichen Adresse, von der die E-Mail geschickt wird.

Eine ***gefälschte Webseite*** imitiert das Aussehen einer echten Webseite, indem sie deren genauen Web-Content und Bilder kopiert, um das Erscheinungsbild so Pixel-genau wie möglich zu machen.

Betrugs-Seiten versuchen auch, den Domain-Namen in der Adresszeile zumindest vage realistisch erscheinen zu lassen, zum Beispiel indem sie das kopierte Logo auf die linke untere Seite zu setzen (paypal.com.bogus.example), in der Hoffnung, dass der Nutzer die rechte untere Seite nicht noch einmal überprüft. Auf der ist nämlich der wahre Name zu erkennen. Andere Betrüger wiederum versuchen ähnliche Namen zu basteln, mit skurrilen Ideen: für ein W zwei VV oder statt kleinem L (l) ein großes I (I).

Solche „traditionellen“ Tricks der Webseitenfälscher lassen sich mit kleinen Kniffen schnell entlarven, hier einige Tipps von Sophos:

- Es lohnt sich, den ***Header (also die Kopfzeile der E-Mail) genau zu studieren***: Hier wird der wahre Server genannt, von dem die Nachricht geschickt wurde, und nicht, welche der Absender angibt.

- ***Einen E-Mail-Filter einrichten***, der automatisch den Header und den Text jeder einzelnen Nachricht, auf Betrug scannt.

- ***Nur im Internet surfen mit einer Netzwerk- oder Endgeräte-Firewall***, die ausgehende Webanfragen an gefälschte Webseiten blockiert und eingehende Webantworten mit riskanten Inhalten verwirft.

- ***Ein Passwort-Manager*** verknüpft Nutzernamen und Passwörter mit bestimmten Webseiten. Er kann daher gar nicht von gefälschten Inhalten oder ähnliche Namen reingelegt werden.

Der Betrug per E-Mail, wie in diesem PayPal-Fall, ist ebenfalls sehr ausgeklügelt
E-Mail-Betrüger gehen viel näher an ihr Opfer heran und verschicken beim Erstkontakt Nachrichten, die tatsächlich von echten Webseiten oder Online-Diensten stammen und auf Server verweisen, die wirklich von denselben legitimen Webseiten betrieben werden. Allerdings muss der Betrüger danach einen Weg finden, mit dem Opfer weiterhin in Kontakt zu bleiben, um den Betrug fortzuführen.

Und so funktioniert der aktuelle „Geld anfordern"-Betrug via PayPal:

1. Der Betrüger erstellt sich ein PayPal-Konto und nutzt die Funktion „Geld anfordern", um dem Opfer eine offizielle PayPal-E-Mail zu senden, die dazu auffordert, dem Betrüger Geld zu schicken.

2. Er stellt die Anfrage wie eine bestehende Rechnung für ein echtes Produkt oder einen Service dar, auch wenn dieses gar nicht bestellt wurde und wahrscheinlich auch für einen unwahrscheinlichen oder unangemessenen Preis.

3. Schlussendlich fügt der Kriminelle der Nachricht eine Telefonnummer bei, wo er zum Schein einen einfachen Weg anbietet, die Bezahlung zu stornieren, falls man das Ganze für einen Betrug hält.

Die E-Mail kommt also tatsächlich von PayPal mit einem Hauch von Authentizität, aber: sie leitet das Opfer dazu an, die Betrüger tatsächlich anzurufen. Anstatt einfach auf die E-Mail selbst zu antworten oder sich an PayPal zu wenden. Das Perfide ist hier, dass die Betrüger einen Weg gefunden haben, via offizielle Quelle (PayPal) in den direkten Kontakt mit dem Opfer zu kommen und nun abseits der Plattform und ohne Kontrolle durch diese mit ihm zu kommunizieren.

Was kann man tun?
Zunächst einmal nichts. PayPal Geldanfragen sind wie der Name schon sagt, Anfragen, keine Rechnungen, keine Forderungen, keine Quittungen. Wenn man also so eine Nachricht erhält und sich selbst aber keines kürzlichen Kaufs bewusst ist, einfach nichts machen, besonders nicht die angegebene Telefonnummer kontaktieren. Dann läuft der Betrug ins Leere.

Nichtsdestotrotz sollte man den Betrug in jedem Fall PayPal melden, damit der entsprechende Account geschlossen und sichergestellt werden kann, dass kein anderer Nutzer darauf hereinfällt. Bei Verdacht sollte man sich an die Adresse spoof@paypal.com wenden.
Auch Behörden wie Polizei (diese haben oft eigene Cybercrime-Abteilungen) oder Bundesnetzagentur verfügen über Meldeservices. Je mehr Auffälligkeiten bei offiziellen Stellen ankommen, desto größer ist die Wahrscheinlichkeit, dass diese den Fall ernst nehmen und es publik wird.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de