Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Überblick
- Phishing
- Schützen Sie sich

Phishing

Überblick

E-Mail ist heutzutage eines der wichtigsten Kommunikationsmittel. Wir nutzen E-Mails nicht nur täglich beruflich, sondern auch, um mit unseren Freunden und unserer Familie in Kontakt zu bleiben. Darüber hinaus werden E-Mails auch von den meisten Unternehmen zur Kommunikation bei der Nutzung von Online-Diensten verwendet, beispielsweise zur Bestätigung eines Online-Kaufs oder als Benachrichtigung zur Verfügbarkeit Ihrer Kontoauszüge. Aufgrund dieser weltweiten Abhängigkeit von E-Mail haben Cyberkriminelle E-Mail als Hauptangriffsmethode für sich entdeckt.

In diesem Newsletter erklären wir das sogenannte Phishing, eine gängige E-Mail-basierte Angriffsmethode, sowie die Schritte, die Sie ergreifen können, um E-Mail sicher zu nutzen.

Gastautor

Dr. Lance Hayden ist ein Geschäftsführer der Berkeley Research Group. Als Experte für Sicherheitskultur und -verhalten ist er auch Autor des Buchs People-Centric Security: Transforming Your Enterprise Security Culture von McGraw-Hill. Sie finden Ihn unter **www.linkedin.com/in/drhayden**.

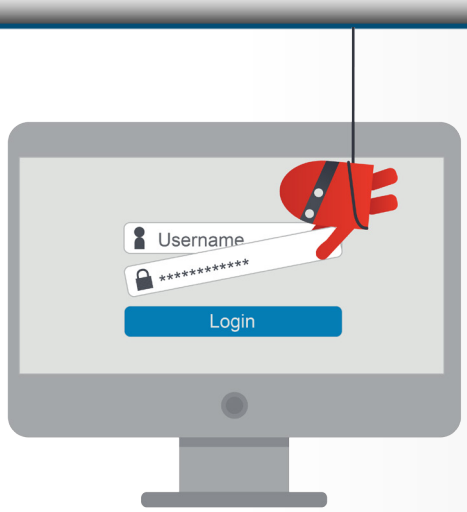
Phishing

Phishing bezieht sich auf einen Angriff, der E-Mail oder einen Messaging-Dienst verwendet, um Sie dazu zu verleiten eine Aktion auszuführen, wie zum Beispiel einen Klick auf einen Link oder das Öffnen eines Anhangs. Wenn Sie Opfer eines solchen Angriffs werden, laufen Sie Gefahr, dass Ihre hoch sensiblen Daten gestohlen und / oder Ihr Computer infiziert wird. Angreifer arbeiten hart, um überzeugende Phishing-E-Mails zu erstellen. Zum Beispiel werden sie ihre E-Mail aussehen lassen als sei sie von einem Ihnen bekannten Absender, wie z.B. einem Freund oder einem vertrauenswürdigen Unternehmen mit dem Sie häufiger kommunizieren. Sie werden sogar Logos Ihrer Bank hinzufügen oder die Absender E-Mail Adresse so manipulieren, dass die E-Mail noch legitimer erscheint. Dann schicken die Angreifer diese Phishing-E-Mails an Millionen von Menschen. Sie wissen nicht wer genau darauf hereinfällt, aber sie wissen, dass sie um so mehr Erfolg haben, je mehr E-Mails sie versenden. Phishing ist vergleichbar mit einem Netz, um Fische zu fangen. Man weiss vorab nicht was man fängt, aber je größer das Netz ist um so mehr Fische werden sich darin verfangen. Angreifer verwenden Phishing auf verschiedene Art, um zu bekommen was sie wollen:

- **Informationen sammeln**: Das Ziel der Angreifer ist es, möglichst viele Ihrer persönlichen Daten zu sammeln, darunter Ihre Passwörter, Kreditkartennummer und Kontodaten. Um das zu erreichen senden sie Ihnen einen Link der Sie auf eine Webseite führt die legitim erscheint. Die Webseite fordert Sie dann auf, bestimmte persönliche Daten einzugeben. Diese Seite ist aber gefälscht, jede eingegebene Information geht direkt an die Angreifer.

Phishing

- **Bösartige Links**: Ziel der Angreifer ist es, die Kontrolle über Ihre Geräte zu erlangen. Sie senden Ihnen hierzu eine E-Mail mit einem Link zu, der Sie nach dem Anklicken auf eine Webseite führt. Die Seite greift das von Ihnen genutzte Gerät an und infiziert es, oft unbemerkt von Ihrem Virenscanner.
- **Bösartige Anhänge**: Ziel der Angreifer ist es wiederum, Ihr Gerät zu infizieren und die Kontrolle darüber zu erlangen. Anstelle eines Links senden die Angreifer Ihnen jedoch eine infizierte Datei zu, wie z.B. ein Word Dokument. Das Öffnen dieses Anhangs löst den Angriff aus, der den Angreifern bei Erfolg die Kontrolle Ihres Systems ermöglicht.
- **Betrug**: Einige Phishing E-Mails sind nichts weiter als eine digitale Form des Trickbetrugs. Sie versuchen Sie zu überlisten, indem Sie Ihnen vorgaukeln, Sie hätten in der Lotterie gewonnen, oder sie wären eine Wohltätigkeitsorganisation die Ihre Hilfe benötigt, um Millionen Dollar oder Euro zu überweisen. Wenn Sie darauf antworten, werden sie sagen sie benötigen zunächst eine Überweisung als Bezahlung ihrer Dienste, oder Zugriff auf Ihr Bankkonto, von dem sie sich dann natürlich frei bedienen werden.



Ihre beste Verteidigung ist Ihr gesunder Menschenverstand. Wenn eine E-Mail oder Nachricht ungewöhnlich, verdächtig oder zu gut um wahr zu sein erscheint, könnte es sich um einen Phishing Angriff handeln.

Schützen Sie sich

In fast allen Fällen ist das Lesen von E-Mails oder Nachrichten gefahrlos. Damit ein Phishing Angriff funktioniert, müssen die Angreifer Sie zu einer Aktion verleiten. Es gibt glücklicherweise mehrere Anzeichen, dass eine Nachricht ein Angriff sein könnte. Hier sind die gängigsten:

- Die E-Mail erzeugt eine Art von Druck oder Eile, fordert “sofortiges Handeln” bevor etwas Schlimmes geschieht, wie z.B. das Sperren Ihres Bankkontos. Die Angreifer wollen Sie dazu drängen einen Fehler zu machen, bevor Sie zu lange darüber nachdenken.
- Sie erhalten eine E-Mail mit einem Anhang, die Sie nicht erwartet haben, oder der Text der E-Mail fordert Sie zum Öffnen des Anhangs auf. Das könnte z.B. eine E-Mail mit “unangekündigten Entlassungen” sein, mit Gehaltsabrechnungen aus Ihrem Unternehmen, oder eine Nachricht vom Finanzamt die Ihnen mitteilt, dass gegen Sie ermittelt wird.
- Statt Ihres Namens nutzt die E-Mail eine generische Anrede wie “Werter Kunde”. Die meisten Unternehmen und Freunde sprechen Sie mit Ihrem Namen an, wenn sie Sie kontaktieren.
- Die E-Mail fordert hoch sensible Informationen an, wie z.B. Ihre Kreditkartennummer oder ein Passwort.
- Die E-Mail gibt vor von einer offiziellen Organisation zu stammen, weißt aber Rechtschreib- oder Grammatikfehler auf

Phishing

oder nutzt eine persönliche E-Mail Adresse die z.B. auf web.de, @gmail.com oder @hotmail.com endet.

- Der Link erscheint merkwürdig. Ein guter Tip ist, mit der Maus nur auf den Link zu zeigen ohne zu klicken, sodass ein Popup erscheint das Ihnen das wahre Ziel des Links anzeigt. Auf Mobilgeräten halten Sie mit dem Finger einfach länger auf den Link gedrückt, um dieses Popup angezeigt zu bekommen. Ein noch sicherer Schritt ist es, den Link zu kopieren und in die Adresszeile Ihres Browsers einzufügen - dann sehen Sie wohin er wirklich zeigt. Oder Sie tippen die Adresse einfach ab - Ihr Browser vervollständigt bereits bekannte, vertrauenswürdige Adressen meist sehr schnell.
- Sie erhalten eine Nachricht von jemandem den Sie kennen, aber die Wortwahl oder der Umgangston ist nicht wie Sie es erwarten würden. Wenn Sie hier einen Verdacht haben, rufen Sie den Absender auf einer Ihnen bereits bekannten Nummer an um zu erfragen, ob er die E-Mail wirklich geschickt hat. Es ist für Cyberangreifer ein Leichtes, eine E-Mail zu generieren die von einem Freund oder Arbeitskollegen zu kommen scheint.

Wenn Sie befürchten, dass eine E-Mail oder Nachricht ein Phishing Angriff sein könnte, löschen Sie sie einfach. Gesunder Menschenverstand ist oft die beste Verteidigung.

Weiterführende Informationen

Social Engineering:	https://www.securingthehuman.org/ouch/2014#november2014
Sicher in Fünf Schritten:	https://www.securingthehuman.org/ouch/2014#october2014
Ich wurde gehackt - was nun?:	https://www.securingthehuman.org/ouch/2014#may2014
BSI für Bürger - Phishing:	https://goo.gl/7W8jKt
SANS Sicherheitstip des Tages (engl.):	https://www.sans.org/tip_of_the_day.php

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis