Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

- **Was ist Social Engineering**
- **Social Engineering Angriffe erkennen und stoppen**

Social Engineering

Überblick

Ein häufiges Missverständnis vieler Menschen hinsichtlich Cyberangreifern ist, dass diese nur ausgefeilte Werkzeuge und Techniken nutzen, um anderer Leute Computer oder Onlinekonten zu hacken. Das ist jedoch schlichtweg falsch. Cyberangreifer haben schnell gelernt, dass der einfachste Weg um Ihre Benutzerkonten zu hacken, Ihre Daten zu stehlen oder Ihre Systeme zu infizieren meist darin besteht, Sie dazu zu verleiten Fehler zu begehen. In diesem Newsletter werden Sie lernen wie diese "Social Engineering" genannten Angriffe funktionieren und wie Sie sich dagegen schützen können.

Gastautor

James Lyne (**@jameslyne**) ist zertifizierter SANS Lehrer und Forschungsleiter bei Sophos. Er entdeckt und analysiert die neuesten Erfindungen der Cyberkriminellen. Zudem ist er Autor der SANS Kurse Metasploit (SEC580) und Social Engineering (SEC567).

Was ist Social Engineering

Social Engineering ist ein psychologischer Angriff, bei dem der oder die Angreifer Sie dazu bringen etwas zu tun, das Sie besser nicht getan hätten. Das Konzept von Social Engineering ist nicht neu, es existiert seit tausenden Jahren - denken Sie nur an Trickbetrüger aller Art. Was die heute verfügbaren Technologien für Cyberangreifer so viel interessanter macht ist, dass Sie die Angreifer nicht sehen können. Sie können sich daher leicht für jemand anderen ausgeben und so Millionen Menschen auf der ganzen Welt, Sie eingeschlossen, ins Visier nehmen. Um das Vorgehen zu verstehen, schauen wir uns im Folgenden einfach zwei echte Beispiele an.

Sie erhalten einen Anruf von jemandem, der vorgibt von einem Unternehmen wie Ihrem Internetanbieter oder gar von Microsoft anzurufen. Der Anrufer erklärt Ihnen, dass Ihr Computer bei ihren Sicherheitsüberprüfungen auffiel und wahrscheinlich infiziert ist. Er hätte den Auftrag, Ihnen bei der Absicherung Ihres Computers zu helfen. Dann nutzt er eine Vielzahl technischer Fachbegriffe und beschreibt Ihnen mehrere komplizierte Schritte, um Ihnen zu verdeutlichen, dass Ihr Computer infiziert ist. Er bittet Sie z.B. zu prüfen, ob Sie bestimmte Dateien auf Ihrer Festplatte finden, und erklärt Ihnen wo Sie dafür nachsehen müssen. Wenn Sie diese Dateien finden, versichert der Anrufer Ihnen, dass Ihr Computer infiziert ist, obwohl es sich in Wahrheit dabei lediglich um normale Systemdateien handelt die auf nahezu jedem Computer zu finden sind. Nachdem er Sie überzeugt hat, dass Ihr Computer infiziert ist, bringt er Sie dazu eine Sicherheitssoftware zu kaufen oder eine Software für den Zugriff über das Internet herunterzuladen, so dass er sich zur Behebung der Infektion auf Ihren Computer verbinden kann. Bei der Software, die er verkauft, handelt es sich jedoch um ein bösartiges Programm. Wenn

Social Engineering

Sie es kaufen und installieren, haben Sie nicht nur Ihren Computer selbst infiziert, sondern dafür auch noch Geld ausgegeben! Wenn Sie dem Angreifer Zugriff auf Ihren Computer ermöglichen, kann dieser die Kontrolle darüber übernehmen, Ihre Daten stehlen oder ihn für seine Zwecke verwenden.

Gesunder Menschenverstand ist Ihre mächtigste Verteidigungsmöglichkeit gegen die meisten Social Engineering Angriffe.

Ein anderes Beispiel sind E-Mail-Angriffe, die als “CEO Fraud”, zu deutsch “Manager-Betrug”, bezeichnet werden und häufig im beruflichen Umfeld geschehen. Hierbei forscht ein Cyberangreifer Ihr Unternehmen über öffentlich verfügbare Quellen aus und interessiert sich dabei insbesondere für den Namen Ihres Vorgesetzten oder Ihrer Kollegen. Der Angreifer präpariert dann eine E-Mail, die vorgibt von dieser Person zu stammen, und sendet sie Ihnen. In der E-Mail wird eine dringende Handlung gefordert, wie z.B. eine Überweisung oder das Zusenden vertraulicher Informationen. Oft geben diese E-Mails vor, dass es sich um einen Notfall handelt der schnelles Handeln unter Umgehung der üblichen (Sicherheits-)Verfahren erfordert. Man könnte Sie z.B. bitten, vertrauliche Unternehmensdaten an eine private @gmail.com Adresse zu senden. Was diese gezielten Angriffe so gefährlich macht ist die vorausgegangene gründliche Recherche der Angreifer. Zudem können gängige Sicherheitstechnologien wie Antivirus oder Firewalls diese Angriffe nicht erkennen oder gar unterbinden, weil keine manipulierten Anhänge oder Web-Links benötigt werden.

Machen Sie sich bewusst, dass derartige Social Engineering Angriffe nicht auf Telefonanrufe oder E-Mails beschränkt sind; sie können jegliche Form annehmen, darunter Textnachrichten, Soziale Medien oder sogar von Angesicht zu Angesicht. Wenn Sie wissen worauf Sie achten müssen, sind Sie Ihre beste Verteidigung.

Social Engineering Angriffe erkennen und stoppen

Glücklicherweise lassen sich solche Angriffe leichter abwehren als Sie vermuten, denn der gesunde Menschenverstand ist oft Ihre beste Verteidigung. Wenn Ihnen etwas verdächtig erscheint oder sich nicht richtig anfühlt, dann ist es möglicherweise ein Angriff. Die häufigsten Anhaltspunkte für einen Social Engineering Angriff sind:

- Jemand schafft ein enormes Gefühl der Dringlichkeit, damit Sie Fehler begehen.
- Jemand fragt Sie nach Informationen, zu denen er eigentlich keinen Zugriff haben sollte oder die er schon kennen sollte, wie zum Beispiel Ihre Kontodaten.

Social Engineering

- Jemand fragt Sie nach Ihrem Passwort, kein seriöses Unternehmen würde Sie so etwas fragen.
- Jemand setzt Sie unter Druck, damit Sie Sicherheitsprozesse oder -prozeduren umgehen oder ignorieren, die Sie laut Vorgaben Ihres Arbeitgebers befolgen müssen.
- Etwas klingt zu gut um wahr zu sein. Zum Beispiel wird Ihnen gesagt, dass Sie ein iPad oder in einem Gewinnspiel gewonnen haben, obwohl Sie gar nicht an einem Gewinnspiel teilgenommen haben.
- Sie erhalten eine merkwürdige E-Mail von einem Freund oder Arbeitskollegen, die nicht klingt als wäre sie von ihm. Ein Angreifer könnte sich Zugang zu seinem E-Mail-Postfach verschafft haben und versucht nun Sie reinzulegen. Versuchen Sie die entsprechende Person über einen anderen Kommunikationsweg (direkter Kontakt oder Telefon) zu erreichen, um zu verifizieren, dass die Nachricht tatsächlich von ihm kommt.

Wenn SIe vermuten, dass jemand versucht Sie auszutricksen, stellen Sie die Kommunikation mit dieser Person einfach ein. Wenn der Angriff einen Bezug zu Ihrer Arbeit hat, informieren Sie Ihren Helpdesk oder das Team, welches in Ihrem Unternehmen für die Informationssicherheit zuständig ist. Denken Sie daran, der gesunde Menschenverstand ist oft Ihre beste Verteidigung.

Weiterführende Informationen

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO Fraud:	https://securingthehuman.sans.org/ouch/2016#july2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH Archive:	https://securingthehuman.sans.org/ouch/archives

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 securingthehuman.sans.org/ouch/archives.

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, Cheryl Conley

