Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Social Engineering
- Erkennung von Social Engineering Angriffen
- Schutz vor zukünftigen Angriffen

Social Engineering

Überblick

Viele Menschen unterliegen dem Irrtum, dass Cyberangreifer nur fortschrittliche Hackerwerkzeuge und ausgefeilte Technologie benutzen, um in PCs, Benutzerkonten und Mobilgeräte einzubrechen. Dies entspricht jedoch nicht ganz der Realität. Die Angreifer haben schon früh gelernt, dass einer der einfachsten Wege Informationen über ihre Opfer zu bekommen darin besteht, mit ihnen zu sprechen oder sie in die Irre zu führen. Dieser Newsletter beschreibt die gängigsten Verfahren dieses sogenannten „Social Engineering“ (deutsch: Soziale Manipulation) und wie Sie sich dagegen schützen können.

Gastautor

Alissa Torres ist zertifizierte SANS Ausbilderin, spezialisiert auf fortgeschrittene Computerforensik und Incident Response. Ihre berufliche Erfahrung umfasst zum einen Einsätze an vorderster Front als Incident Handler und das Arbeiten als forensische Ermittlerin. Alissa ist auf Twitter als **@sibertor** aktiv.

Social Engineering

Social Engineering, zu Deutsch am besten als „zwischenmenschliche Manipulation“ zu umschreiben, ist eine Art psychologischer Angriff bei dem Sie verleitet werden etwas zu tun, das sie nicht tun wollten. Social Engineering wird schon seit tausenden von Jahren angewandt, die Idee jemanden steuern oder betrügen zu wollen ist also nicht neu. Cyberangreifer haben deshalb schon früh festgestellt, dass diese Angriffsform äußerst effizient ist und über das Internet damit Millionen von Anwendern als Ziel ins Auge gefasst werden können. Wie diese Angriffe funktionieren kann am einfachsten an einem Beispiel aus unser aller Alltag demonstriert werden.

Sie erhalten einen Anruf von jemandem, der vorgibt von einer Firma zur PC-Betreuung, Ihrem Internetanbieter oder gar vom technischen Support von Microsoft zu sein. Der Anrufer erklärt Ihnen, dass er bemerkt hätte, dass Ihr Computer durch merkwürdiges Verhalten auffällt wie z.B. dem Versenden von Spam-E-Mails, oder dass er glaubt der Rechner sei mit Schadsoftware infiziert. Er hat angeblich den Auftrag, den Vorfall zu untersuchen und Ihnen zu helfen die Schadsoftware zu entfernen und Ihren Rechner wieder in einen sicheren Zustand zu versetzen. Dabei nutzt er eine Vielzahl technischer Fachbegriffe und führt Sie durch unzählige Arbeitsschritte an Ihrem Computer, um Sie zu überzeugen, dass dieser infiziert ist.

Er lässt Sie beispielsweise verschiedene Dateien auf dem Computer suchen und erklärt Ihnen, wie diese zu finden sind. Wenn Sie die Dateien finden, erklärt der Anrufer Ihnen, dass diese ein Zeichen für eine Infektion sind – in Wirklichkeit sind die Dateien jedoch auf jedem Computer zu finden und legitim. Sobald man Sie überzeugt hat, dass Ihr Computer infiziert ist, wird man versuchen Sie zum Aufruf einer Webseite zu bewegen, um eine Sicherheitssoftware zu kaufen oder Sie auffordern einen Fernzugriff auf Ihren Computer zuzulassen um das Problem zu beheben.

Social Engineering

Die auf der Webseite angebotene Software ist jedoch ein bösartiges Programm. Wenn Sie dieses tatsächlich kaufen und installieren, hat man Sie nicht nur verleitet Ihren Computer zu infizieren, sondern Sie haben auch noch Geld dafür bezahlt. Wenn Sie Fernzugriff auf Ihren Computer zulassen um die Probleme zu beheben, werden die Angreifer in Wahrheit dauerhafte Kontrolle darüber übernehmen.

Social Engineering Angriffe wie diese beschränken sich natürlich nicht nur auf Telefonanrufe, sie können mit fast jeder Technologie durchgeführt werden, wie z.B. E-Mail, Textnachrichten, Facebook- oder Twitter Nachrichten und viele mehr. Es ist daher essentiell zu wissen, worauf man achten muss.

Das Wissen, wie man Social Engineering Angriffe verhindert, erkennt und unterbindet, ist eine der wichtigsten Fähigkeiten um sich selbst zu schützen.

Erkennen und Unterbinden von Social Engineering Angriffen

Die einfachste Abwehrmethode ist die Anwendung des gesunden Menschenverstands. Wenn ihnen etwas verdächtig oder einfach „komisch“ erscheint, könnte es ein Angriff sein. Einige gängige Anzeichen sind zum Beispiel:

- Jemand drängt sehr zur Eile. Wenn Sie genötigt werden sehr schnell eine Entscheidung zu treffen, seien Sie misstrauisch.
- Jemand fragt nach Informationen, auf die er keinen Zugriff haben sollte oder die ihm in seiner vorgeblichen Position bereits zur Verfügung stehen sollte.
- Etwas ist zu gut um wahr zu sein. Ein gängiges Beispiel ist, dass Sie über den Gewinn einer Lotterie informiert werden, obwohl Sie nie daran teilgenommen haben.

Wenn Sie den Verdacht haben, dass jemand Sie zum Opfer eines Social Engineering Angriffs machen will, beenden Sie sofort jegliche Kommunikation mit der Person. Legen Sie einfach auf, wenn es sich um einen Anruf handelt oder beenden Sie den Chat. Eine nicht vertrauenswürdige E-Mail können Sie einfach löschen. Wenn der Angriff Bezug zu Ihrem Beruf hat, melden Sie ihn umgehend dem zuständigen Helpdesk oder dem Informationssicherheitsteam.

Schutz vor zukünftigen Social Engineering Angriffen

Es gibt einige Vorsichtsmaßnahmen, die Sie ergreifen können um Ihre Angriffsfläche für zukünftige Social Engineering Angriffe zu verringern:

- **Niemals Passwörter weitergeben**: Keine Organisation wird sie jemals kontaktieren und nach Ihrem Passwort fragen. Wenn jemand nach Ihrem Passwort fragt, handelt es sich um einen Angriff.

Social Engineering

- **Teilen Sie nicht zu viele Informationen**: Je mehr ein Angreifer über Sie weiß, desto leichter fällt es ihm Sie zu kontaktieren und Sie dazu zu verleiten das zu tun, was der Angreifer von Ihnen möchte. Schon kleine Details über sich selbst können im Laufe der Zeit zu einem umfänglichen Bild zusammengesetzt werden. Je weniger Sie öffentlich teilen, z.B. in sozialen Medien, Produktbewertungen, öffentlichen Foren und Mailinglisten, desto geringer ist die Wahrscheinlichkeit eines Angriffs.

- **Überprüfen Sie Kontaktanfragen**: Sie werden wahrscheinlich irgendwann von Ihrer Bank, Ihrem Mobilfunkanbieter oder anderen Organisationen aus legitimen Gründen kontaktiert. Wenn Sie irgendeinen Zweifel an der Rechtmäßigkeit einer Anfrage haben, bitten Sie den Anrufer um seinen Namen und seine Durchwahl. Suchen Sie dann die Telefonnummer des Unternehmens in einer vertrauenswürdigen Quelle wie z.B. den „Gelbe Seiten“, Telefonbüchern, der Webseite des Unternehmens (deren Adresse sie von Hand in den Browser tippen sollten) oder Ihren Unterlagen. Wenn Sie die so erhaltene Telefonnummer anrufen, können Sie sicher sein, wirklich mit einem Mitarbeiter dieses Unternehmens zu sprechen. Obwohl es nach viel Mühe aussieht ist der Schutz Ihrer Identität und Ihrer persönlichen Daten diesen Mehraufwand absolut wert.

Weiterführende Informationen

E-Mail Phishing Angriffe: http://www.securingthehuman.org/ouch/2013#february2013

Sicher in sozialen Netzwerken: http://www.securingthehuman.org/ouch/2013#march2013

Gefahren im Netz: https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/gefahren_node.html

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

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters 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