Kurzfassung

Der Hack des menschlichen Betriebssystems

Raj Samani, EMEA CTO

Charles McFarland, Senior Research Engineer für MTIS

intel Security

Viele Internetangriffe besitzen eine Social-Engineering-Komponente, bei der eine Zielperson von einer Aktion überzeugt werden soll, die zu einer Infektion oder Kompromittierung führt.

Obwohl sich die Behebung nach einem Angriff vor allem auf technische Aspekte konzentriert, steht auch die betroffene Person im Kreuzfeuer, was deutlich zeigt, wie wichtig adäquates Sicherheitsbewusstsein ist. Tatsache ist allerdings, dass sich die meisten Unternehmen herzlich wenig dafür interessieren, warum das Ziel ausgenutzt wurde und – wichtiger noch – was sie abgesehen von verstärkter Aufmerksamkeit dafür tun können, dass sich solche Angriffe nicht so schnell wiederholen können.

Der Begriff „Social Engineering“ kann wie folgt definiert werden:

> *Die absichtliche Nutzung von Täuschungstechniken, mit denen eine Person dazu verleitet werden soll, Informationen preiszugeben oder Aktionen auszuführen, die eine Preisgabe dieser Informationen ermöglichen können.*

Während eines Social-Engineering-Angriffs ist sich das Opfer nicht unmittelbar bewusst, dass seine oder ihre Aktionen schädlich sind. Der Angreifer nutzt nicht die kriminellen Instinkte seiner Zielperson aus, sondern ihre unschuldigen Reflexe. Angriffe können in zwei Kategorien eingeteilt werden:

- Das Jagen dient dem Entlocken von Informationen mit minimaler Interaktion mit der Zielperson. Bei diesem Ansatz kommt es meist nur zu einem einzigen Kontakt, bei dem der Angreifer die Kommunikation beendet, sobald er im Besitz der gewünschten Information ist.
- Beim Farmen soll eine Beziehung mit der Zielperson aufgebaut und dieser über einen längeren Zeitraum Informationen entlockt werden.

Social-Engineering-Angriffe, die E-Mails als Kommunikationsmedium nutzen, setzen als Angriffsmethode vor allem auf das Jagen. Natürlich gibt es auch hier Ausnahmen, beispielsweise die „Nigeria-Betrugsmasche“, bei der ein Angriff über einen längeren Zeitraum ausgedehnt wird, um so viel Geld wie möglich zu erschleichen. Beide Social-Engineering-Angriffsmethoden bestehen meist aus vier Phasen:

1. Nachforschung: In dieser optionalen Phase sollen so viele Informationen wie möglich über die Zielperson gesammelt werden. Der Angreifer sucht nach Informationen, von denen er sich einen erfolgreichen „Angelhaken“ verspricht, zum Beispiel die Hobbys der Zielperson, ihr Arbeitsplatz oder ihre Bank.
2. Angelhaken: Der Angelhaken versucht, ein erfolgreiches „Schauspiel“ aufzubauen, indem die Zielperson angesprochen und ein Vorwand zur Interaktion etabliert wird. Der Psychologe Robert Cialdini nennt vier Hebel zur psychischen Beeinflussung, mit denen das Unterbewusstsein der Zielperson angesprochen werden soll:
   - Gegenseitigkeit: Menschen wird ein Gefallen getan, bei dem sie sich verpflichtet fühlen, diesen Gefallen zurückzugeben.
   - Verknappung: Menschen lassen sich beeinflussen, wenn sie glauben, dass an etwas ein Mangel herrscht.
   - Verpflichtung: Sobald Menschen versprochen haben, etwas zu tun, halten sie sich an ihr Versprechen, da sie vertrauenswürdig erscheinen wollen.
   - Gefallen: Die Zielpersonen lassen sich eher von Menschen beeinflussen, die sie mögen.
   - Autorität: Nutzt die menschliche Tendenz zur Gehorsamkeit gegenüber Autoritätspersonen aus.
   - Social Proof: Die Tendenz, sich am Verhalten anderer Menschen zu orientieren.

3. Schauspiel: Führt den Hauptteil des Angriffs aus. Dabei kann es sich um die Offenlegung von Informationen, das Klicken auf einen Link oder die Überweisung von Geldern handeln.
4. Beenden: Die Interaktion nähert sich dem Endstadium. Auch wenn es bei vielen Farming-Angriffen von Vorteil sein kann, sich ohne Verdacht zu erregen zu verabschieden, ist das häufig unnötig. Das ist zum Beispiel der Fall, wenn Angreifer ihre Zielpersonen dahingehend manipulieren, dass diese Zahlungskarteninformationen weitergeben. Die Angreifer haben seltenst Interesse daran, den Verdacht ihrer Opfer zu erregen, damit diese nicht ihre Karten als verloren oder gestohlen melden und sie sperren. Wenn jedoch Angreifer an Quellcodes oder andere persönliche Informationen gelangen, kann die Zielperson selbst dann die Daten nicht zurückholen, wenn sie Verdacht schöpfen sollte.

Social-Engineering-Versuche erfolgen nicht unbedingt linear: Ein einzelner Angriff kann Teil einer erheblich größeren Kampagne sein, um an verschiedene Bruchstücke zusammenhängender Informationen zu gelangen. Beispielsweise könnten Angreifer einen Angriff durchführen, an die Information gelangen und sich dann aus dem Staub machen. Alternativ könnten sie auch bei zahlreichen Jagd-Angriffen Informationen sammeln und damit einen Farming-Angriff starten.

Angriffswege

Social-Engineering-Angreifer können mehrere Wege für ihre Angriffe wählen.

- Webseiten: Social-Engineering-Angriffe nutzen häufig böswillige Webseiten als Angriffsweg. Laut dem *2014 Verizon Data Breach Investigations Report* (Untersuchungsbericht von Verizon zu Datenkompromittierungen 2014) nutzen „20 Prozent der durch Spionage motivierten Angriffe eine strategische Web-Kompromittierung, um Malware zu übertragen".
- E-Mail: Die häufigste Form des Social Engineering per E-Mail sind Phishing sowie das gezieltere Spearphishing. E-Mails sind eine effektive Methode für Internetkriminelle, da laut dem Verizon-Bericht „18 Prozent aller Benutzer auf einen Link in einer Phishing-E-Mail klicken".
- Telefon: Dieser Weg wird von Informationshändlern gern genutzt.
- Angesicht zu Angesicht: Hier wird ein Mitarbeiter angesprochen und gezwungen oder überlistet, die gewünschten Informationen preiszugeben.
- Post: Obwohl dieser Angriffsweg weniger offensichtlich erscheint als die zuvor genannten, gibt es immer noch Berichte über Social-Engineering-Angriffe per Post.
- Fax: Hierzu zählen beispielsweise E-Mails, die sich als Nachrichten von Online-Zahlungsdiensten ausgeben.

Schutz vor Social-Engineering

Mit den folgenden Kontrollen können Sie die Risiken durch Social Engineering verringern. Diese Maßnahmen werden in drei Kategorien eingeteilt: Mitarbeiter, Prozesse und Technologien. Die Kontrollen bieten keinen umfassenden Schutz und sind nicht in allen Unternehmen anwendbar.

Mitarbeiter

- Legen Sie klare Grenzen fest: Alle Mitarbeiter sollten stets die Richtlinien zur Weitergabe von Informationen beachten und sich an feste Eskalierungsstufen halten, falls eine Anfrage außerhalb ihres Zuständigkeitsbereichs fällt.
- Laufende Schulungen: Starten Sie ein Programm zur Förderung des Sicherheitsbewusstseins, um die Mitarbeiter langfristig zu schulen. Nutzen Sie Mittel wie das McAfee-Phishing-Quiz, um bei Angriffen häufig eingesetzte Taktiken vorzustellen.

- Überprüfen von Berechtigungen: Geben Sie Ihren Mitarbeitern das Selbstvertrauen, auch scheinbar harmlose Anfragen zu hinterfragen. Beispielsweise sollten Ihre Mitarbeiter nachfragen, wenn fremde Personen im Schlepptau einer Gruppe in die Büroräume gelangen wollen.
- Betonung der Bedeutung von Informationen: Selbst scheinbar harmlose Informationen wie Telefonnummern (nutzbare Information) können der Durchführung eines Angriffs dienen.
- Aufbau einer Kultur der Schuldlosigkeit: Die Ziele der Social-Engineering-Angreifer sind Opfer. Durch die Bestrafung von Mitarbeitern, die auf einen solchen Angriff hereingefallen sind, werden die übrigen Mitarbeiter weitaus weniger gewillt sein, eine Informationsweitergabe zuzugeben. Sobald sie einmal hereingelegt wurden, könnten sie dadurch dauerhaft vom Social-Engineering-Angreifer erpresst werden.

Prozess

- Berichte zu Angriffsversuchen: Sobald Mitarbeiter eine verdächtige Aktivität bemerkt haben, sollten sie einen Bericht mit einer Beschreibung der Interaktion erstellen. Dies ist eine wichtige Hilfe bei Untersuchungen.
- Informative Blockierungsseiten: Schalten Sie eine Blockierungsseite, die angezeigt wird, wenn Mitarbeiter versuchen, eine böswillige Webseite zu öffnen. Diese Seite sollte über die Gründe für die Blockierung informieren, damit Ihre Mitarbeiter über die vorangegangene Aktion nachdenken. Zudem kann die Seite dabei helfen, die Quellen eines Angriffs zu ermitteln.
- Kundenbenachrichtigung: Wenn Anrufern Informationen verweigert werden, sollte sich das Unternehmen mit ihnen in Verbindung setzen und überprüfen, ob die Anrufer berechtigt waren, diese Informationen anzufordern. Unternehmen sollten auch darüber nachdenken, wie sie mit Kunden kommunizieren. Beispielsweise hat PayPal Richtlinien veröffentlicht, mit denen Benutzer erkennen können, ob die erhaltenen E-Mails echt sind. „In einer echten E-Mail werden wir niemals nach Ihrer Bankverbindung, Geld- oder Kreditkartennummer fragen. Ebenso werden wir niemals Ihren vollständigen Namen, Ihr Konto-Kennwort oder die Antwort auf Ihre PayPal-Sicherheitsfrage per E-Mail anfragen.“
- Eskalierungspfad: Eine bekannte Verbindung, über die Mitarbeiter melden können, wenn sie mit möglicherweise gefälschten Nachrichten zu tun haben.
- Tigertests: Testen Sie die Mitarbeiter routinemäßig auf Anfälligkeit für Social-Engineering-Angriffe über unterschiedliche Kommunikationskanäle. Dies bietet Ihnen eine Möglichkeit, die Effektivität Ihrer Schulungsprogramme zu ermitteln.

Technologie

- Anrufaufzeichnung: Zeichnen Sie routinemäßig eingehende Telefonanrufe auf, um Untersuchungen zu erleichtern.
- Verbindung für gefälschte Anrufe: Hierbei werden verdächtig erscheinende Anrufe an eine überwachte Verbindung weitergeleitet.
- E-Mail-Filterung: Löscht betrügerische E-Mails mit neuer oder bereits bekannter Malware.
- Web-Filter: Diese Filter blockieren den Zugang zu böswilligen Webseiten und erkennen Malware, die über den Internet-Datenstrom ins Unternehmen gelangt.
- Starke Authentifizierung: Obwohl die Mehrfachfaktor-Authentifizierung das Risiko nicht verringert, dass Benutzer bei einem Social-Engineering-Angriff ihre Anmeldeinformationen weitergeben, erschweren sie dem potenziellen Angreifer die Arbeit.

McAfee Labs folgen

Zusammenfassung

Die Bedrohung durch Social Engineering ist absolut real. Internetkriminelle nutzen diese Angriffsmethode, um unrechtmäßig und für böswillige Zwecke an Informationen zu gelangen. Das Problem lässt sich nur dann eingrenzen, wenn wir wissen, wie Social-Engineering-Angriffe durchgeführt werden. Das bedeutet, dass wir die wahrscheinlichsten Akteure, ihre Angriffsmethoden und Ressourcen definieren und entsprechende Kontrollen einrichten müssen, um das Risiko eines erfolgreichen Angriffs zu verringern.

Den vollständigen Bericht finden Sie unter **www.mcafee.com/hacking-human-os.**

Twitter@Raj_Samani

Twitter@CGMcFarland

1. **http://www.verizonenterprise.com/DBIR/2014/**
2. **https://www.paypal.com/gb/webapps/helpcenter/helphub/article/?solutionId=FAQ2061&m=HTQ**

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com