Social Engineering

Einleitung

Dieses Referat beschäftigt sich nicht mit der üblichen Auflistung der Arten von Social Engineering gibt es. Denn zum einen kennen Sie diese, zumindest teilweise, schon von den anderen Referaten, weiters ist es doch viel interessanter ein wenig hinter die Kullisen zu blicken und sich die Frage zu stellen "Warum funktionieren Social Engineering Angriffe eigentlich?". Doch zuerst trozdem eine kurze Klarstellung worum es sich bei Social Engineering überhaupt handelt.

Was ist Social Engineering eigentlich?

Bei Social Engineering handelt es sich sozusagen um die Kunst der Täuschung. Diese Formulierung habe ich ganz absichtlich gewählt, denn es gibt Social Engineers welche sich gewissermaßen als Künstler betrachten wobei ein Angriff dann ihrem persönlichen Kunstwerk entspricht. Daher gibt es eine wichtige grundsätzliche Unterscheidung zwischem dem Gauner, also Personen, welche jemanden anschwindeln und sie damit um ihr Geld betrügt und, für dieses Referat relevant, den Social Engineer, welcher Täuschungs-, Betrugs- und Überredungsfähigkeiten einsetzt um an Informationen zu gelagen. Natürlich geht es nicht unbedingt darum sinnlos Informationen zu sammeln, sondern gezielt nach Informationen zu suchen, welche für den Angreifer nützlich, oder zumindest interessant sind, denn nicht jeder Social Engineer führt bösartiges im Schilde, zumindest laut Kevin Mitnick gibt es auch Personen, welche dies zum puren Vergnügen ausüben. (vgl. The Art of Deception, Kevin Mitnick)

Man kann die Social Engineers in zwei Kategorien einteilen:

- Angreifer, welche möglichst schnell irgendwie Informationen haben möchten, welche sie zu Geld machen können.
    - haben kein bestimmtes Opfer
    - senden z.B. Phishings-Mails an möglichst viele Email-Adressen
    - hoffen darauf, dass unter den Empfängern möglichst viele leicht auszutricksende Opfer sind
    - greifen nach der niedrig hängenden Frucht
- Angreifer, welche es auf ein bestimmtes Opfer (meistens ein Unternehmen) abgesehen haben

Was sind Informationen in diesem Zusammenhang?

Laut dem Duden handelt es sich bei einer Information um eine "auf Anfrage erteilte über alles Wissenswerte in Kenntnis setzende [...] Mitteilung über etwas". Besser könnte man es eigentlich auch im Bezug auf Social Engineering nicht beschreiben. Denn der Social Engineering kommuniziert mit einem Opfer, daher eine handelt es sich um eine Mitteilung, und auf Anfrage des Social Engineers, er beginnt den Anruf, wird er über führ ihn wissenswerte Firmengeheimnisse in Kentnis gesetzt. Praktisch gesehen handelt es sich dabei unteranderem um Dokumente, Präsentation, Passwörter und Sourcecode.

Wie "leicht" Social Engineering oft ist

Meist muss ein Social Engineer gar nicht lange irgendwelche hochkomplexen, perfekt ausgeklügelten Maschen und Tricks verwenden. Es genügt im Normalfall sich einfach als eine bestimmte Person auszugeben, welche offensichtlich berechtigt ist, auf die Informationen zuzugreifen. Denn Menschen haben die Neigung es

einfach zu glauben, wenn sich jemand als eine bestimmte Person am Telefon ausgibt. (Vorallem neue) Mitarbeiter werden oft nicht lange darüber nachdenken, wenn sich eine Person mit dem Satz "Hallo, hier spricht Claudia Schwarz vom Management in Perg." vorstellt. Etwas vorsichtigere Mitarbeiter werden im Mitarbeiterverzeichnis nachsehen, doch spätestens wenn sie dort tatsächlich eine Claudia Schwarz in der Managementabteilung in Perg finden werden sie ihre Zweifel verwerfen.

In der Kurzfassung:

- sich als jemand Anderes ausgeben
- nach Informationen fragen Oder um Kevin Mitnick zu zitieren: "You just need to ask for it."

Warum funktioniert Social Engineering?

Zumindest ein Teil von Ihnen haben sich bestimmt schon einmal gedacht, warum fällt man auf so etwas herein. Das ist doch irgendwie offensichtlich, oder? Doch wie Albert Einstein sagte: "Zwei Dinge sind unendlich: das Universum und die menschliche Dummheit. Aber bei dem Universum bin ich mir noch nicht ganz sicher." Oft führt Dummheit oder eher Unwissenheit zum Erfolg eines Angriffs, doch so einfach auf Dummheit und "Der kennt sich nicht aus" schieben sollte man Social Engineering auch nicht. Denn auf solche Tricks können unter Umständen auch Experten wie Linus Neumann reinfallen, zumindest wenn sie müde sind. (vgl. 36C3: Wenn der Ransomware-Support plötzlich Russisch spricht, Stefan Krempl)

Vertrauen

So ist es z.B. sehr naheliegend kritisch zu sein wenn gerade in den Nachrichten die Rede von falschen Microsoftmitarbeitern ist und ein paar Tage später werden sie von einem angeblichen Microsoftsupport mit indischem Akzent angerufen, welcher kaum einen deutschen Satz herausbringt. Wobei hier angemerkt sei, dass Microsoft Teile seines Supports in Indien hat. So unlogisch ist das Szenaria also doch wieder nicht, es könnte doch sein das einer Ihrer Kollegen, welcher heute krank ist, angerufen hat. Wollen Sie ihm nicht aushelfen, er wartet doch schon so lange auf einen Anruf des Supports?

Zeitdruck

Oder stellen sie sich vor sie arbeiten in einem sehr großen Unternehmen und Ihr Vorgesetzer hat einen sehr autoritär ausgeprägten Führungsstil. Ihr Vorgesetzer ist gerade bei einem potenziellen Kunden zu Besuch und bittet Sie ihm ein wichtiges Dokument per Email weiterzuleiten. Ihr Vorgesetzer hat sie mit seiner üblichen Telefonnummer angerufen spricht Sie mit Ihrem Namen an und kennt den Ort an dem das Dokument zu finden ist. Klingt doch so als ob es wirklich Ihr Vorgesetzer ist, oder? Würden sie wirklich riskieren Ihren, nicht gerade freundlichen, Vorgesetzten zu verärgern und noch dazu Ihrem Unternehmen zu schaden, weil es einen potenziellen Kunden verlieren könnte? Würden Sie überhaupt auf die Idee kommen, dass es sich nicht um Ihren Vorgesetzten handelt? Viele Menschen würden in so einem Moment nicht lange Nachdenken. Doch dazu später mehr.

Ein geübter Social Engineer hat eine Trickkiste voll mit solcher Komponenten wie Autorität, Vertrauen, Eile und (zeitlichem) Druck. Aus dieser Trickkiste sucht er gezielt die passenden Schwächen für das jeweilige Opfer, denn wie allgemein bekannt ist, ist nicht jeder Mensch gleich. Dabei tappt auch einmal der geübte Nutzer in die Falle. (vgl. 36C3: Wenn Ransomware-Support plötzlich Russich spricht, Stefan Krempl)

Intuition und Ignoranz

Nun wissen wir also, dass der Erfolg von Social Engineering nicht immer etwas mit der "Dummheit" des Opfers zu tun hat. Weiters sollte nun allerdings auch so ziemlich jeder über die Existenz von Phishing-Mails bescheid wissen. Doch warum fallen trozdem noch so viele Personen, einschließlich Experten, auf diese Attacken herein? Dafür müssen wir etwas in die Welt der Phsychologie eintauchen. "Der Mensch ist ein Gewohnheitstier." Dieses Zitat von Gustav Freytag könnte nicht besser passen. Laut Linus Neumann besitzt das menschliche Gehirn zwei Systeme. Das erstere funktioniere schnell und intuitiv. Das zweitere langsam, analytisch und schließe die Vernunft beim Denkprozess mit ein. Jedoch greife etwa bei Angst oder Langeweile das schnelle, intuitive System. Das zweitere bleibe bei einer Konfrontation mit Phishing-Mails außen vor. (vgl. 36C3: Wenn der Ransomwore-Support plötzlich Russisch spricht, Stefan Krempl) Der Mensch handelt also so wie er es gewohnt ist und einem Kollegen etwas per Email zu senden oder eine Nachricht von Paypal ist nun grundsätzlich nichts Ungewöhnliches. Somit haben wir wieder einen weiteren Grund warum Opfer nicht an Sätze wie "Warum holt er sich das nicht selbst per VPN vom Server? Der hat doch sowieso mehr Rechte als ich und um die Email zu empfangen benötigt er sowieso Internetzugang. Ist doch sinnlos wenn ich ihm das sende. Da stimmt etwas nicht" denken. Denn das wäre wohl Aufgabe des, nicht eingeschalteten, analytischen Gehirnsystems.

Scheinbare Harmlosigkeit

Oft ist den Opfern der eigentliche Wert von bestimmten Informationen nicht bewusst. Der Social Engineer ist nicht immer sofort auf das Passwort oder den Quellcode einer Software aus. Oft beginnt er damit quer durch ein Unternehmen zu telefonieren und nach scheinbar harmlosen Informationen zu fragen. Die meisten Mitarbeiter sehen keinen Grund dafür warum diese harmlosen Informationen schützenswert sind. Warum sollte es z.B. einem Angreifer etwas bringen zu wissen das Max Mustermann im Management am Firmenstandort in Perg arbeitet. Leider sind gerade diese Informationen für einen Social Engineer von sehr hohem Wert. Sie helfen ihm nähmlich dabei dem nächsten Opfer im Unternehmen einen besseren Anschein von Glaubwürdigkeit zu vermitteln. Das vorher erwähnte Beispiel mit einem Anruf von Ihrem Vorgesetzten ist doch gleich viel glaubwürdiger wenn dieser Sie mit Ihrem Namen anspricht und seinen eigenen Namen kennt sowie auch noch über einen Kunden spricht mit welchem sie tatsächlich Geschäfte machen.

Links

Motorola Attack, Kevin Mitnick

36C3: Wenn der Ransomware-Support plötzlich Russich spricht, Stefan Krempl