

Zusammenfassung

In diesem Themenbeitrag geht es um Angriffstechniken, die unter dem Namen «Social Engineering» zusammengefasst werden. Wir werden Ihnen zeigen, wie es Angreifern gelingt, gutgläubige,

zugriffsberechtigte Internetnutzer zu manipulieren und sich unbefugten Zugang zu vertraulichen Ressourcen zu verschaffen.

Inhalt

- 1 Was ist Social Engineering?
- 2 Wie funktioniert das Ganze?
- 3 Wer ist betroffen?
- 4 Beispiel: Scammer
- 5 Empfehlungen



1 Was ist Social Engineering?

Es handelt sich dabei um Manipulation durch Täuschung. Die Angreifer versuchen, Zugang zu vertraulichen Informationen oder zugriffsbeschränkten Ressourcen zu bekommen, indem sie Personen manipulieren, die direkten oder indirekten Zugriff darauf haben. Zu dieser Angriffsart gehört auch «Phishing».

Social Engineering gibt es nicht nur im Bereich der Informatik, sondern auch im alltäglichen Leben und vor allem auch am Arbeitsplatz. Sobald es um Ressourcen geht, die für irgendjemanden interessant sein könnten, kommt es zu Angriffen dieser Art.

Nicht umsonst sind große Organisationen oft Ziel von Angriffen, weil dort viele Menschen beschäftigt sind und Informationen schnell verbreitet werden.

Der menschliche Faktor steht im Mittelpunkt der Social Engineering-Techniken. Dabei werden mit Kalkül und Berechnung Vertrauensbeziehungen aufgebaut, oft einfach nur durch Gespräche. Diese Beziehungen werden dann ausgenutzt, um Kapital aus den Informationen zu schlagen.

2 Wie funktioniert das Ganze?

Für die Social Engineering-Techniken werden Schwächen im menschlichen Verhalten und in der Art und Weise, wie Unternehmen organisiert sind, ausgenutzt. So liegt es in der Natur des Menschen, anderen helfen zu wollen und freundlichen und sympathisch erscheinenden Menschen sein Vertrauen zu schenken, auch wenn man sie nicht kennt. Letztendlich hängt alles davon ab, in welcher Situation und mit welcher Herangehensweise die Angreifer sich das Vertrauen ihrer Opfer erschleichen. Oft reicht eine ganz einfache direkte Bitte aus.

Das Ziel des Angriffs besteht darin, jemanden dazu zu bringen, eine bestimmte Handlung vorzunehmen, zu der die betreffende Person unter normalen Umständen nie bereit wäre. Auf diese Weise

will sich der Angreifer Informationen beschaffen, an die er sonst nicht herankommt. In unserer zunehmend computergesteuerten Welt geht es meist (aber nicht immer) um die Beschaffung von Authentifizierungsdaten.

Ein Angreifer kann z. B. versuchen, zunächst eine Vertrauensbeziehung zu einem Mitarbeiter aufzubauen und ihm nach und nach Informationen über das Unternehmen zu entlocken. Es kommt gar nicht so selten vor, dass sich Angreifer mit dem Jargon im Unternehmen und den betrieblichen Abläufen auskennen. Das erleichtert die Kontaktaufnahme mit Mitarbeitern und verhindert, dass jemand bei bestimmten Fragen hellhörig wird.

Für den Mitarbeiter stellt sich die Sache so dar, dass er / sie es offensichtlich mit jemandem zu tun hat, der die innerbetrieblichen Abläufe kennt und sich im Jargon des Unternehmens ausdrückt. In einem großen Unternehmen, in dem nicht jeder jeden kennen kann, hat der Mitarbeiter keinen Grund, misstrauisch zu sein, und gibt bereitwillig Auskunft. Schließlich möchte er ein hilfsbereiter Kollege sein! Oft machen sich die Betroffenen erst hinterher Gedanken über die Sicherheit, aber dann ist der Angreifer bereits über alle Berge, ohne Spuren zu hinterlassen – mit wertvollen Informationen in der Tasche.

In einem solchen Fall hat der Angreifer sein Ziel ohne Umwege erreicht, weil er sich auskannte.

Es gibt noch weitere Ansätze, insbesondere wenn es um das Ausspionieren von Informationen geht. Der Angreifer kann so

tun, als ob er beauftragt wäre, eine Umfrage über den Tätigkeitsbereich des Opfers durchzuführen. Er stellt dann eine ganze Reihe harmloser Fragen, unter die er auch die Frage schmuggelt, deren Antwort für ihn besonders wichtig ist. Das kann z. B. eine Frage über den Jargon im Unternehmen oder zu bestimmten unternehmensspezifischen Konventionen (wie etwa Konventionen zur Produktbenennung) sein.

Der Angreifer schwenkt dann auf eine ganz andere Strategie um, indem er sein Opfer in eine vermeintliche Problemsituation versetzt und dann seine Hilfe anbietet. In den meisten Fällen zeigt sich das Opfer kooperationsbereit und beantwortet ohne Wenn und Aber alle Fragen des Angreifers

3

Wer ist betroffen?

Grundsätzlich kann jeder Opfer solcher Angriffe werden, ob Privatperson oder großes Unternehmen. Dabei muss noch nicht einmal ein Computer oder das Internet im Spiel sein, um Opfer von Social Engineering zu werden. Die neuen Technologien bieten lediglich neue Möglichkeiten, solche Angriffe durchzuführen. Der direkte Kontakt, das Telefon und auch die gute alte Post werden nach wie vor für Social Engineering-Angriffe genutzt.

Auch die Kunden eines Unternehmens können ins Visier von Angreifern geraten. In diesem Fall dient das Unternehmen selbst als Vektor, um an die Kunden und die Ressourcen heranzukommen, zu denen es Zugriff hat.

4

Beispiel: Scammer

Mit dem Begriff «Scammer» werden Personen bezeichnet, die andere Menschen betrügen wollen, indem sie diese per E-Mail um Hilfe bitten, weil sie angeblich große Mengen an Geld an den Behörden vorbei anlegen möchten. Um das Opfer zu ködern, schlägt der Scammer ihm vor, einen gewissen Geldbetrag auf sein Bankkonto zu überweisen. Um die Bitte seriös aussehen zu lassen, gibt der Scammer vor, mit irgendeiner offiziellen Stelle zusammenzuhängen, und verwendet echt aussehende Dokumente.

Hier ein Beispiel für eine E-Mail von einem Scammer:

From: <christelle.eyadema@jumpy.it>
Sent: Friday, 01 April, 2005 2:43
Subject: Vertraulich

« Ich wende mich mit diesem Schreiben an Sie, weil ich gerne eine Geschäftsbeziehung zu Ihnen aufbauen möchte. Mein Name ist Christelle EYADEMA. Ich bin die Tochter des Präsidenten Gnassingbé EYADEMA, und meine Mutter stammt von der Elfenbeinküste... »

Der Scammer möchte auf diese Weise Geld bei seinem Opfer locker machen. Er gibt vor, dass bei dem angeblichen Geldtransfer, von dem beide Parteien profitieren sollen, Kosten entstehen, die das Opfer übernehmen soll.

5

Empfehlungen

5.1 Woran erkenne ich Social Engineering-Angriffe?

Social Engineering-Angriffe müssen nicht immer komplex sein. Es kann durchaus sein, dass sie in Form einer einfachen, harmlosen Bitte um Informationen stattfinden. Ein Angriff kann auch dazu

dienen, Informationen zu beschaffen, mit deren Hilfe letztendlich ein ganz anderes Opfer angegriffen wird. Jede Bitte einer unbekanntenen, fremden Person um Informationen über betriebliche Abläufe, Gepflogenheiten oder den betriebsinternen Jargon ist verdächtig.

5.2 Wie kann ich mich davor schützen?

Jede Information, auch wenn sie noch so unbedeutend erscheint, muss als wichtig betrachtet werden. Die Mitarbeiter von Unternehmen müssen für diese Art von Problemen sensibilisiert werden, da jeder so manipuliert werden kann, dass ein Angreifer wichtige Informationen entlocken kann.

Wenn es in dem Unternehmen eine Sicherheitspolitik gibt, müssen die entsprechenden Verfahren streng eingehalten werden. Das gilt insbesondere für neue Mitarbeiter, die mit ihrem neuen Arbeitsumfeld noch nicht vertraut sind und daher beliebtes Ziel von Angriffen sind. Die Sicherheitspolitik muss auch von Mitarbeitern eingehalten werden, die keinen Zugriff auf EDV-Geräte haben. Eine Person, die den Jargon, die Abläufe und die Gepflogenheiten eines Unternehmens kennt, ist deswegen noch lange nicht vertrauenswürdig.

Im Zweifelsfall sollte immer die Identität überprüft werden. Am Telefon sollten Sie den Gesprächspartner um dessen Telefonnummer bitten und die betreffende Person nach Prüfen der Nummer zurückrufen. Bei dieser Prüfung geht es darum herauszufinden, ob der Gesprächspartner tatsächlich befugten Zugriff auf den Telefonanschluss hat, von dem aus er angerufen hat. Was Computer anbelangt, gibt es ein paar einfache Regeln, mit denen Sie sich vor Social Engineering schützen können.

Dabei geht es vor allem um den gesunden Menschenverstand, von dem Sie nicht nur am Arbeitsplatz, sondern auch vor dem heimischen Computer Gebrauch machen sollten. Schützen Sie Ihre Kennwörter, und geben Sie diese niemals an andere weiter. Das bedeutet auch, dass Sie keine Befehle ausführen dürfen, die Ihnen eine unbekannte Person vorgibt. Öffnen Sie keine Datei, die an eine E-Mail eines zweifelhaften Absenders angehängt ist. Das gilt auch für Dateien von zweifelhaften Internetseiten. Solche Dateien sehen auf den ersten Blick harmlos aus. In Wirklichkeit aber können sie Dokumente des Nutzers zerstören, Dokumente an eine Internetseite schicken, die von einem Angreifer gesteuert wird, und sogar die Kontrolle über den Rechner übernehmen. Unsere letzte Empfehlung gilt Papierdokumenten. Lassen Sie solche Informationsquellen nicht für jeden sichtbar herumliegen. Das gilt auch für Dokumente im Papierkorb. Machen Sie Dokumente, die Sie nicht mehr benötigen, unlesbar, indem Sie sie verbrennen oder mit einem Aktenvernichter vernichten.