ALLGEIER
secion

# Social Engineering Methoden

Die 10 häufigsten Social Engineering Methoden - und wie man sich davor schützt

**Wer bei dem Thema Cyberangriff an hoch technisierte Hacker denkt, die mit modernsten Schadprogrammen die Sicherheitsmaßnahmen von Unternehmen umgehen, um Daten abzugreifen oder Erpressungsversuche durchzuführen, liegt nicht unbedingt falsch. Allerdings nutzen Cyberkriminelle für ihre Machenschaften deutlich häufiger eine ganz andere Schwachstelle aus: den Menschen und dessen Fehler. Social Engineering ist eine Form der Cyberkriminalität, die aktuell für 98 % aller Angriffe verantwortlich ist. Was die 10 häufigsten Social Engineering Methoden sind und wie Sie Ihr Unternehmen zuverlässig davor schützen, erfahren Sie in diesem Beitrag.**

## **Methode 1:** Phishing

Phishing ist ein Kunstwort, das aus dem englischen „fishing“ für „angeln“ abgeleitet ist. Beim Phishing werden massenhaft Nachrichten versendet, die einen realen Absender vorgaukeln und den Empfänger zu der Eingabe von Passwörtern oder Bankdaten auffordern. Andere Phishing-Nachrichten beinhalten Links zu kompromittierten Webseiten. Das Perfide an den Phishing-Nachrichten: sie sind in vielen Fällen nicht von „echten“ Nachrichten zu unterscheiden. Die Angreifer setzen hier auf Psychologie und zwischenmenschliche Manipulation, häufig unterstützt von Emotionalität und perfekt gefälschten Logos oder direkter Ansprache des Empfängers oder der Empfängerin. Je professioneller der Social Engineer hinter den versendeten Phishing-Nachrichten agiert, desto schwerer ist es, die Betrugsversuche zu erkennen.

### Wie schützen Sie sich vor Phishing?

*Wie bei allen Aktivitäten im Internet gilt auch bei empfangenen Nachrichten: Zuerst denken, dann klicken. Schauen Sie sich vor allem den Absender der Nachricht an. Stimmt die Absenderadresse mit den bei Ihnen hinterlegten Daten überein? Bei dem geringsten Zweifel sollten Sie vor dem Öffnen der Nachricht persönliche Rücksprache mit dem Absender halten.*

# **Methode 2:** Spear Phishing

Nochmals deutlich perfider geht es beim Spear Phishing zu. Spear Phishing ist eine deutlich gezieltere, individuellere Form des Phishings, bei der die Angreifer es auf ein ausgewähltes Opfer abgesehen haben. Während es beim konventionellen Phishing zumeist um das Abgreifen von Zugangsdaten oder Bankverbindungen geht, zielen Social Engineers beim Spear Phishing darauf ab, ein Unternehmen zu infiltrieren. Dem eigentlichen Angriff geht dabei eine intensive Überwachung des Opfers voraus - hierbei kann es sich um eine Zielperson oder eine Zielorganisation handeln. In dieser Phase sammeln die Angreifer Insider-Informationen über das Unternehmen, spähen Mitarbeiter aus oder fragen bei Lieferanten vertrauliche Daten ab. Mit dem gewonnenen Wissen werden dann gezielt ausgewählte Personen innerhalb des Unternehmens ins Visier genommen. Das Ziel der Angreifer: der unerkannte Einstieg in ein Unternehmens-Netzwerk.

### Wie schützen Sie sich vor Spear Phishing?

*Da sich die Angreifer vor ihren eigentlichen Aktivitäten bestens über den Status Quo eines Unternehmens, seine Struktur und internes Wissen informieren, sind Spear Phishing Angriffe unglaublich schwer zu erkennen. Der beste Schutz ist hier gesundes Misstrauen!*

# **Methode 3:** Quid pro quo

Kostenlose Sicherheitsüberprüfungen des Firmen-Netzwerkes, gratis Produkte oder Hilfe bei der Abarbeitung dringender Aufgaben: Quid-pro-quo-Angriffe setzen auf das Vertrauensprinzip. Eine Hand wäscht die andere, beide Seiten profitieren davon – eigentlich eine gute Sache. Eigentlich, denn hinter dem vermeintlich guten Tauschgeschäft steckt in der Realität viel zu oft ein Social-Engineer-Angriff. Die Angreifer verlangen im Tausch für die kostenlosen Leistungen gerne Anmeldedaten oder Passwörter – mit denen im Nachgang zum Quid-pro-quo-Angriff dann der eigentliche Cyberangriff durchgeführt werden kann.

### Wie schützen Sie sich vor Quid-pro-quo-Angriffen?

*Der alte Spruch „Was nichts kostet, ist auch nichts“ gilt auch und insbesondere im geschäftlichen Umfeld. Werden Ihnen kostenlose Dienstleistungen oder Produkte angeboten, für die Sie „nur“ Ihre Anmeldedaten zu Ihrem Netzwerk oder Ihr Passwort abgeben müssen, sollten Sie hellhörig werden.*

# **Methode 4:** Baiting

Eng mit der Quid-pro-quo-Methode verwandt ist das Baiting. Bei dieser Methode legen die Social Engineers „Köder“ in Form von kostenlosen Downloads oder Gratis-Produkten aus, die ganz einfach und bequem über ein Online-Formular oder via Klick auf einen Link angefordert werden können. Hinter dem vermeintlichen Geschenk steckt Malware, die den Rechner der Zielperson kompromittiert – oder die eingegebenen Daten werden gleich abgegriffen und für weitere Cyberangriffe missbraucht.

### Wie schützen Sie sich vor Baiting?

*Niemand hat etwas zu verschenken – auch im Internet nicht. Wenn Ihnen kostenlose Software oder Produkte angeboten werden, können Sie eigentlich immer von einem Betrugsversuch ausgehen. Löschen Sie entsprechende Nachrichten, ohne auch nur einen weiteren Gedanken daran zu verschwenden.*

# **Methode 5:** Pretexting

Pretexting übernimmt gleich zwei Funktionen. Einerseits ist Pretexting für sich genommen bereits ein Social-Engineering-Angriff, andererseits bildet die Methode die Grundlage für viele andere der hier genannten Cyberangriffe. Pretexting lässt sich am besten mit dem Erfinden umfangreicher Szenarien rund um ein Unternehmen beschreiben, mit dem Betrüger ihre Opfer dazu bringen können, persönliche Daten freizugeben. Die Cyberangreifer entwickeln hierbei teils extrem komplexe Geschichten rund um die geschäftliche oder auch persönliche Beziehung zu dem ausgewählten Opfer. Pretexting setzt dabei auf Vertrauen. Die Lügengebilde kennen dabei so gut wie keine Grenzen – von extra für den Angriff aufgesetzten Webseiten, über eigens angelegte E-Mail-Adressen, bis hin zur perfekten Verkleidung für den „Besuch vor Ort“ wird keine kreative Möglichkeit ausgelassen, um an Zugangsdaten oder Firmeninterna zu gelangen. Der freundliche Service-Techniker, der sich um den Firmen-Server kümmern will, kann genauso ein Social Engineer sein wie der Lieferant, der beim Pförtner um Einlass bittet oder der Finanzbeamte, der mit der Buchhaltung „einige offene Fragen zur letzten Bilanz“ klären möchte.

### Wie schützen Sie sich vor Pretexting?

*Social Engineers, die Pretexting betreiben, sind leider zumeist Meister ihres Fachs. Entsprechend schwierig ist es, die Angreifer zuverlässig zu enttarnen. Bleiben Sie auch bei vermeintlich seriösen Besuchern, die Sie nicht persönlich kennen, immer misstrauisch – und fragen Sie lieber einmal mehr telefonisch nach, ob der vor Ihnen stehende Mitarbeiter wirklich von dem genannten Unternehmen gesendet wurde.*

# **Methode 6:** Tailgating

Social Engineers sind nicht immer rein digital unterwegs, wie wir gerade am Beispiel des Pretextings gesehen haben. Auch beim Tailgating verlässt der Social Engineer die digitale Welt, um physisch in eigentlich abgeschottete Bereiche eines Unternehmens einzudringen. Ob als neuer Kollege im Konzern, als Lieferant Ihrer Zulieferer oder als Service-Techniker: Prinzipiell kann sich auch hinter der vertrauenswürdigsten Fassade ein Social Engineer verbergen.

### Wie schützen Sie sich vor Tailgating?

*Prüfen Sie bei neuen Kontakten, die vor der Unternehmensforte stehen, unbedingt den Hintergrund und vermeiden Sie es auf jeden Fall, vorschnell Daten herauszugeben oder gar die Freigabe für den Zutritt zu sensiblen Bereichen Ihres Unternehmens zu autorisieren.*

# **Methode 7:** Media Dropping

Eventuell haben Sie schon mal einen USB-Stick oder eine Daten-CD verlegt oder vielleicht sogar verloren. Das passiert – und jeder ist froh, wenn die kleinen Datenträger wieder aufgefunden werden. Bei Media Dropping „verlieren“ Social Engineers Datenträger innerhalb ihres Unternehmens – und zwar so, dass die Möglichkeit sehr groß ist, dass die Datenträger von Mitarbeitern gefunden werden. Unterstützt wird die Methode dadurch, dass die Datenträger häufig mit Beschriftungen oder Aufdrucken versehen werden, die die Neugier wecken und den Finder dazu animieren, den Datenträger zu öffnen. Findet der Datenträger den Weg in den Rechner des Finders, wird Schadsoftware installiert oder Bots für DDoS-Angriffe aktiviert.

### Wie schützen Sie sich vor Media Dropping?

*Vorsicht vor allen „gefundenen“ Datenträgern! Auch wenn Neugier mehr als menschlich ist – unterbinden Sie es auf jeden Fall, gefundene USB-Sticks oder CDs auf Ihrem Unternehmens-Rechner zu öffnen!*

# **Methode 8:** Scareware

Angst ist ein starker Motivator – und ein überaus beliebtes Mittel für Social Engineers, um an ihr Ziel zu gelangen. Scareware nutzt die Angst der Menschen aus – in dem die automatisiert ablaufenden Tools eine Gefahr simulieren, die in Wahrheit gar nicht existiert. Bekannt ist hier beispielsweise ein plötzlich aufpoppendes Fenster auf dem Bildschirm, dass vor einem Befall des Systems mit gefährlichen Viren warnt – oder den Angreifer darauf hinweist, dass strafrechtlich relevante Inhalte auf dem System gefunden wurden. Durch den aufgebauten Druck sollen die Opfer zu unüberlegten, vorschnellen Handlungen genötigt werden – beispielsweise zum Herunterladen des „einzigen Virenscanners, der das Problem lösen kann". Hinter dem hoffnungsvollen Klick lauert dann Schadsoftware, die auf den Rechner heruntergeladen wird.

### Wie schützen Sie sich vor Scareware?

*Lassen Sie sich von den Hiobsbotschaften auf Ihrem Bildschirm nicht erschrecken – und klicken Sie vor allem nicht auf die Links, die Ihnen angeboten werden.*

# **Methode 9:** Honeypots

Honeypots sind Gelegenheiten, die als überaus attraktiv und unwiderstehlich wahrgenommen werden. Im wirtschaftlichen Sektor sind die „Honigtöpfe" vorrangig vorgegaukelte Geschäftsbeziehungen, die einmalige, rentable Gelegenheiten versprechen. Im privaten Bereich zeigen sich Honeypots häufig als einsame Menschen auf der Suche nach der großen Liebe. In beiden Fällen steckt hinter dem Honeypot aber ein Social Engineer, der auf diesem Wege an Unternehmensinterna, sensible Daten oder kompromittierendes Material gelangen möchte.

### Wie schützen Sie sich vor Honeypots?

*Eine Gelegenheit ist zu gut, um wahr zu sein? Dann können Sie davon ausgehen, dass Sie ein Social Engineer übertölpeln möchte. Lassen Sie die Gelegenheit verstreichen und ignorieren Sie alle Versuche der Kontaktaufnahme.*

# **Methode 10:** CEO Fraud

Beim CEO Fraud (auch als "Chef-Trick" bekannt) geben sich die Angreifer per Mail oder auch am Telefon als direkter Vorgesetzter aus und setzen den Kontaktierten unter immensen Druck. Zu den Druckmitteln kann die Aufforderung zur Zahlung einer hohen Summe auf ein unbekanntes Konto im Ausland gehören, das Weiterleiten von Daten, an denen „der unmittelbare Geschäftserfolg" hängt oder die Aushändigung von Zugangsdaten an einen Techniker, der einen dringenden Notfall im Serverraum beseitigen muss. Das perfide Spiel mit Autoritäten, starkem Druck und größter Eile basiert auf der Annahme, dass Anliegen selten abgeschlagen werden, wenn sie direkt „von oben" aufgetragen werden. CEO Fraud ist deswegen so erfolgreich, weil sich die Angreifer bereits im Vorfeld genauestens und detailliert in die Gegebenheiten des Unternehmens einarbeiten – und dadurch mit Detailwissen in den CEO Fraud einsteigen können, das auch den skeptischsten Mitarbeiter überzeugen kann.

### Wie schützen Sie sich vor CEO Frauds?

*Bei allem Respekt vor den Vorgesetzten – bei allen Angelegenheiten, die teilweise oder sogar deutlich von den gewohnten Arbeitsabläufen abweichen, ist Vorsicht geboten. Suchen Sie im Zweifel das direkte, persönliche Gespräch mit dem Vorgesetzten und vergewissern Sie sich, dass das Anliegen echt ist.*

# Fazit zu den 10 häufigsten Social Engineering Methoden

*Social Engineering verbindet auf hinterhältige, aber leider auch kreative Art und Weise digitale und analoge Formen der Cyberkriminalität. Viele der hier aufgeführten Methoden werden von den Hackern auch miteinander verknüpft – was Social Engineering nochmals eine Ecke tückischer machen kann. Mit einer ausgeprägten Cyber Security Awareness und dem Wissen über die perfiden Taktiken der Social Engineers können sich Nutzerinnen und Nutzer vor dieser Form der Cyberkriminalität schützen. Was genau bedeutet das für Organisationen und Unternehmen? Zum einen heißt es mehr denn je, wachsam zu sein – und die Mitarbeitenden für aktuelle Gefahren aus dem Netz zu sensibilisieren. Schulungen, die auf Angriffe vorbereiten, sensibilisieren und bereiten Mitarbeiter darauf vor, im Fall der Fälle schnell und frühzeitig auf Cyberangriffe zu reagieren. In Kombination mit breit aufgestellten Informationskampagnen rund um Cyber Security lässt sich so ein kontinuierliches Awareness-Building innerhalb eines Unternehmens oder einer Organisation erzielen.*

ALLGEIER
secion

**Allgeier secion GmbH**

Tel.: 040 38 90 71 - 0
Fax: 040 38 90 71 - 299

info@secion.de
www.secion.de

Paul-Dessau-Str. 8
22761 Hamburg

**© Copyright 2022**

Urheberrechtshinweis
Alle Inhalte dieses Dokuments, insbesondere Texte, Fotografien und Grafiken, sind urheberrechtlich geschützt. Das Urheberrecht liegt, soweit nicht ausdrücklich anders gekennzeichnet, bei der Allgeier secion GmbH.

Stand: September 2022