Admins Albtraum: Die psychologischen Grundlagen des Social Engineering

Mittels Social Engineering kann ein Angreifer über Hochstapelei und Trickbetrug umfangreiche Informationen aus Mitarbeitern herausholen, die ihm weitere Angriffe ermöglichen oder sogar schon die gewünschten Zielinformationen sind. Der erste Teil des Artikels geht auf zahlreiche psychologische Grundlagen ein, die sich Angreifer zu nutze machen. Im zweiten Teil werden weitere Beeinflussungsmethoden beschrieben, sowie wie Vorschläge zu Gegenmaßnahmen gemacht.

Zitation:

- Schumacher, S. (2009a). Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil I. *Informationsdienst IT-Grundschutz*, *7*, 11–13. Verfügbar 22. Juli 2009 unter http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_7-2009_11_13.pdf

- Schumacher, S. (2009b). Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil II. *Informationsdienst IT-Grundschutz*, *8*, 8–9. Verfügbar 24. August 2009 unter http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_8-2009_8_9.pdf

- Schumacher, S. (2009c). Admins Albtraum: Die psychologischen Grundlagen des Social Engineering, Teil III. *Informationsdienst IT-Grundschutz*, *10/11*, 21–22. Verfügbar 29. Oktober 2009 unter http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_10-2009_10_11.pdf

Admins Albtraum

Die psychologischen Grundlagen des Social Engineering, Teil I

Stefan Schumacher, Sicherheitsberater, Kaishakunin.com

Mittels Social Engineering kann ein Angreifer über Hochstapelei und Trickbetrug umfangreiche Informationen aus Mitarbeitern herausholen, die ihm weitere Angriffe ermöglichen oder sogar schon die gewünschten Zielinformationen sind. Der erste Teil des Artikels geht auf zahlreiche psychologische Grundlagen ein, die sich Angreifer zu nutze machen. Im zweiten Teil werden weitere Beeinflussungsmethoden beschrieben, sowie wie Vorschläge zu Gegenmaßnahmen gemacht.

Social Engineering ist eine Angriffsstrategie, die nicht die Technik als Opfer auserkoren hat. Stattdessen wird hier viel lieber - und vor allem effizienter - der Mensch, bzw. sein Verhalten angegriffen. Gerade in größeren Organisationen kann ein Angreifer über Methoden des Social Engineering notwendige Aufklärungsarbeiten für technische Angriffe leisten oder direkt wichtige Informationen abschöpfen. Dazu benötigt er in der Regel Informationen über die Organisation. Diese sammelt er meist aus frei zugänglichen Quellen wie Webseiten, Werbebroschüren, Dienstvorschriften oder aus den Mülltonnen. Diese Einstiegsinformationen ermöglichen es dem Angreifer, erste Kontakte zu Organisationsmitgliedern zu knüpfen. Dazu gibt er sich als jemand anderes aus, beispielsweise als Systemadministrator, entfernter Vorgesetzter oder potentieller Kunde.

Für die Mitarbeiter mag ein Verzeichnis der Systemadministratoren auf der Webseite nützlich sein - für einen Social-Engineer ist es das auch. Denn mit den Informationen kann er in einem Telefongespräch mit einem Angestellten die Identität eines Administrators annehmen und so unter anderem Zugangsdaten aushorchen.



Stefan Schumacher ist selbständiger Unternehmensberater im Bereich Security Awareness und Security Management. Er studiert zur Zeit Bildungswissenschaft und Psychologie in Magdeburg und befasst sich mit der IT-Sicherheit aus sozialwissenschaftlicher Sicht.

Psychologie der Manipulation

Ein Social-Engineer (oder auch Trickbetrüger oder Hochstapler) verwendet als Angriffstechnik verschiedene Beeinflussungsmethoden. Robert Cialdini, Professor für Psychologie an der Arizona State University, beschreibt in seinem Buch »Die Psychologie des Überzeugens« die psychologischen Mechanismen des Überzeugens. Demnach sei der Mensch das am höchsten entwickelte Lebewesen auf dieser Welt. Wir verfügen zwar über eine enorme psychische Energie und Kapazität, würden aber auch in einer sehr komplexen und schnellen Welt leben. Daher seien wir gezwungen, mentale Arbeit (»nachdenken«) über Faustregeln abzukürzen. Unsere Faustregeln und Stereotype sind feste Handlungsmuster, also Verhaltensweisen, die praktisch jedes Mal gleich ablaufen. Sie verkürzen und vereinfachen anhand von Urteilsheuristiken die gedanklichen Prozesse zur Entscheidungsfindung. Hervorgerufen werden sie durch ein oder mehrere Auslösemerkmale. Man bezeichnet eine derartig mechanische Reaktion auf bestimmte Informationen als automatisches Verhalten. Reaktionen anhand einer gründlichen Analyse aller verfügbaren Informationen nennt man kontrolliertes Verhalten. Verschiedene Studien haben gezeigt, dass Menschen Entscheidungen viel bewusster treffen, wenn sie motiviert und fähig zu einer sorgfältigen Analyse sind. Je wichtiger also eine Entscheidung für einen Menschen ist, desto eher analysiert er die Situation gründlich. Welche Folgen automatische Reaktionen haben können, zeigt ein



Verbotenes Spielzeug: Vernunft funktioniert besser als Verbote. Quelle: Stock.xchng

Unfall während des Zweiten Weltkrieges. Uzal Ent, General der US-Luftwaffe, flog während eines Einsatzes mit einem neuen Co-Piloten, da sich sein Stamm-Co-Pilot krank gemeldet hat. Während des Starts summte der General ein Lied und nickte dazu rhythmisch mit dem Kopf. Der Co-Pilot, der diese Angewohnheit nicht kannte, zog daraufhin das Fahrwerk des Flugzeuges ein, obwohl der Startvorgang noch nicht abgeschlossen war. Die Maschine stürzte ab und Ent wurde durch Trümmerteile schwer verletzt und querschnittsgelähmt. Nach dem Unfall wurde der Co-Pilot befragt, warum er das Fahrwerk eingezogen hatte, obwohl der Start noch nicht abgeschlossen war. Er antwortete daraufhin, dass er dachte, der General wolle das so, schließlich habe er mit dem Kopf genickt. Man mag dieses Verhalten dumm nennen, es ist aber verständlich, wenn man die Grundlagen menschlichen Verhaltens kennt.

Reziprozität

Die Regel der Reziprozität (Wechselseitigkeit) besagt, dass wir uns für erhaltene Gefälligkeiten, Geschenke und dergleichen revanchieren müssen. Diese Regel ermöglichte es, komplexe Gesellschaften aufzubauen, die auf Gegenseitigkeit, also Treu und Glauben, basieren. Daher legen alle Kulturen wert darauf, dass sie eingehalten wird. Mehrere Studien untersuchten die Wirksamkeit der Reziprozität, und bestätigten ihre Schlagkraft. Selbst vergleichsweise wertlose Geschenke können dazu führen, dass der Beschenkte einen großen bzw. wesentlich teureren Gefallen zurück erweist und dabei sogar Antipathie gegenüber dem Beschenkten überspielt. Daher setzen Vertreter oder Verkäufer häufig Gratisproben als Geschenk ein, um ihre Verkaufschancen zu erhöhen.
Eine weitere Verkaufsmasche ist die so genannte »Neuverhandeln-nach-Zurückweisen-Taktik«. Dazu macht ein Verkäufer ein überteuertes Angebot, das er nach der Ablehnung durch den Kunden durch ein besseres ersetzt. Dieses »Zugeständnis« ist ein Geschenk, das beim Kunden die Reziprozitätsregel in Gang setzt. Zusätzlich dazu wirkt der so genannte Wahrnehmungskontrast. Die menschliche Wahrnehmung reagiert wesentlich stärker auf relative Reizänderungen und nicht auf absolute Werte. Ein einfaches Experiment verdeutlicht das Prinzip: man füllt drei Eimer mit eiskaltem, heißen und lauwarmen Wasser. Die linke Hand steckt man ins eiskalte Wasser, die rechte ins Heiße. Nach einer kurzen Gewöhnungszeit steckt man beide Hände ins lauwarme Wasser. Obwohl beide Hände im selben Wasser sind, erscheint es jedoch an der linken Hand als heiß und an der rechten als kalt.

Jedem Menschen wohnt ein Zwang inne, konsistent - also übereinstimmend - mit bisher getroffenen Entscheidungen bzw. gemachten Aussagen zu handeln. Der evolutionäre Nutzen liegt hierbei in der Zusammenarbeit von Menschen. Diese wird erheblich vereinfacht, wenn alle zu ihrem Wort stehen. Eine Studie zu Pferdewetten wies nach, dass sich Menschen selbst davon überzeugen, die richtige Entscheidung getroffen zu haben. Thomas Moriarty wies 1975 in einem Experiment nach, wie stark der Konsistenzzwang sein kann. Ein Assistent legte sich an einem Strand neben einer zufällig ausgewählten Versuchsperson zum sonnenbaden hin. Dazu breitete er ein Handtuch aus und baute ein Kofferradio auf. Nach ca. 10 Minuten ging der Assistent weg und ließ das Radio zurück. Ein zweiter Assistent tauchte nach kurzer Zeit auf und rannte mit dem Kofferradio davon. In 20 Durchläufen wurde der zweite Assistent nur einmal aufgehalten.

Wer A sagt - Commitment und Konsistenz

Im zweiten Experiment wurden die Bedingungen geändert: bevor der Radiobesitzer wegging, bat er seine Nachbarn, die Versuchsperson, darum, auf das Radio zu achten, da er kurz weg müsse. Wieder erschien der zweite Assistent und versuchte das Radio zu stehlen. Diesmal wurde er 19-mal gestoppt, teilweise sogar unter Einsatz körperlicher Gewalt.

Ausgelöst wird konsistentes Verhalten durch ein so genanntes Commitment, eine Art Verpflichtungserklärung oder Bekenntnis. Jede Überzeugungsstrategie, die Konsistenz einsetzt, baut auf diesen Bekenntnissen auf. So fragen z.B. Spendensammler am Telefon, ob es dem Angerufenen gut gehe. Antwortet der Befragte mit Ja, hat er ein Bekenntnis abgegeben, mit dem gearbeitet werden kann.

Viele Verkäufer beginnen so eine »Spirale der Willfährigkeit« in Gang zu setzen. Dazu drängen Sie den Kunden dazu, eine Reihe kleinerer Bindungen abzugeben. Beispielsweise kann man Kunden Fragen, ob er Tiere mag, ob er findet das Tiere geschützt werden sollen, ob Tierschutz wichtig ist, ob man Tierschutz unterstützen soll, ob er denn bereit wäre, mit einer kleinen Spende zu helfen, ob er auch in Zukunft helfen möchte usw. Diese Taktik mit einer kleinen Bitte zu beginnen, um sich dann zur Großen vorzuarbeiten wird in der Sozialpsychologie und im Marketing »Fuß-in-der-Tür-Taktik« genannt. Dabei zeigten einige Experimente, dass die Spendenbereitschaft teilweise verfünffacht werden kann.

Schriftliche Verpflichtung am effektivsten

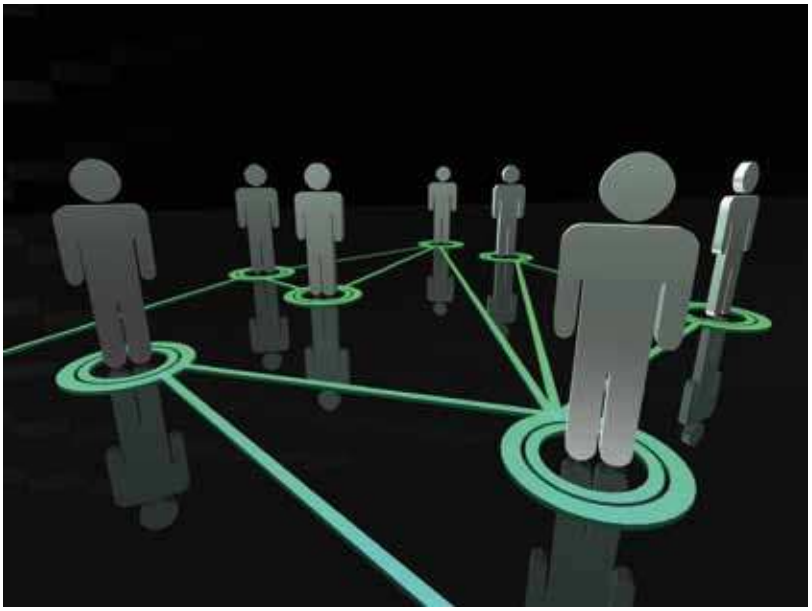
Manipulativ gefährlich ist hierbei, dass durch solche Bindungen und dem folgenden Konsistenzverhalten das Selbstbild einer Person verändert werden kann. Hat sich das Selbstbild erst einmal geändert, möchte die Person damit konsistent bleiben. Allerdings gibt es Randbedingungen für solche Bekenntnisse: es muss aktiv, öffentlich, mit Anstrengung verbunden und freiwillig sein. Erst damit zeigt ein Bekenntnis Wirkung.

Ein aktives Bekenntnis ist das Versprechen etwas zu tun. Ein öffentliches Bekenntnis zeigt mehr Wirkung als ein nichtöffentliches, schließlich wird dieses nicht bekannt und kann so das Bild einer Person nicht ändern. Am effizientesten ist eine schriftliche Verpflichtung. Dies ist ein unbestreitbarer materieller Beweis für eine Festlegung. Deshalb empfehlen auch viele Diät- oder Anti-Rauch-Ratgeber die gefassten Vorsätze schriftlich niederzulegen und bekanntzumachen. Wichtiger noch als die bisher besprochenen Eigenschaften eines Commitments - es muss aktiv, öffentlich und mühevoll sein - ist, das es kein »Belohnungs-Hintertürchen« geben darf. Jemand, der ein Commitment nur wegen einer hohen Belohnung abgegeben hat, wird nicht so stark daran gebunden sein, wie jemand der keine oder nur eine niedrige Belohnung bekommt. Es geht nicht darum, jemandem irgendein Bekenntnis abzuringen, sondern er muss die volle Verantwortung dafür übernehmen. Ein Versuch von Freedman (1965) beweist diese These. Er verbot mehreren 7 bis 9-jährigen Jungs mit einem besonders interessanten Spielzeug zu spielen. Und wer Jungs kennt, insbesondere 7 bis 9-jährige, weiß dass Verbote etwas nur wesentlich interessanter machen. Eine Gruppe wurde mit einer Drohung dazu gebracht, die andere mit einer Begründung. In beiden Gruppen, jeweils 22 Jungs stark, spielte nur ein Einziger verbotenerweise mit dem Spielzeug.

Begründen statt verbieten

Interessant wurde es aber erst im zweiten Teil. Sechs Wochen nach dem Test wurden dieselben Gruppen wieder in Kontakt mit dem Spielzeug gebracht. Diesmal wurde kein Verbot ausgesprochen, so dass 17 Jungs aus der »Drohungsgruppe« sofort zum verbotenen Spielzeug griffen. Da sie nun nicht mehr mit der Bestrafung rechnen mussten, wurde das sechs Wochen vorher ausgesprochene Verbot quasi wirkungslos. In der zweiten Gruppe, die mit einer Begründung vom Spielzeug abgehalten worden waren, griffen nur sieben Jungs zum verbotenen Spielzeug.

Die erste Gruppe hatte also sehr schnell erkannt, dass der Testleiter nicht mehr da war, um seine Drohung wahr zu machen. Nur wenn die Jungs befürchteten, ertappt und bestraft zu werden, hielten sie sich an das Verbot. Die zweite Gruppe hingegen wurde nicht mit einer Strafandrohung vom Spielzeug ferngehalten, sondern mit einer Begründung. Das erste Testergebnis entsprach dem der ersten Gruppe: nur jeweils ein Junge spielte mit dem verbotenem Spielzeug. Das entscheidende spielte sich im Inneren der Jungs ab. In der zweiten Testgruppe gelangten sie zu dem Entschluss, nicht mit dem Spielzeug spielen zu wollen. Sie waren also von sich aus davon überzeugt, auf das verbotene Spielzeug verzichten zu können. Weiterführende Studien zeigten, dass eine angebotene Belohnung den Konsistenzeffekt eines Bekenntnisses sogar mindern kann.



Social Engineering: Informationen durch Kontakte zu Mitarbeitern erschleichen. Quelle: Stock.xchng

professionelle praktische IT-Sicherheitsprüfungen durchzuführen. Die Bankenaufsicht prüft das IT-Sicherheitsniveau kleinerer Institute gar nicht oder nur mit sehr großen Zeitabständen.

IT-Grundschutz: Und was sagt der IT-Sicherheitsbeauftragte im Institut?

Schartner: Abhängig von der Besetzung der Position erleben wir oft, dass dieser sagt: Was soll ich denn noch alles machen? Häufig wird ein IT-Administrator zum IT-Sicherheitsbeauftragten berufen, erhält aber keine zusätzlichen Ressourcen.

IT-Grundschutz: Kommen wir zur Lösung. Was können Banken tun?

Schartner: Eigentlich ist es ganz einfach: Der erste und wichtigste Schritt ist der Aufbau eines funktionierenden IT-Sicherheitsmanagements. Parallel dazu sollte mit der regelmäßigen Durchführung von IT-Sicherheitstests begonnen werden, um die eigenen Schwachstellen kennen zu lernen. Nehmen Sie die Funktion des IT-Sicherheitsbeauftragten ernst. Er darf nicht in der IT-Abteilung angesiedelt werden sondern muss, unabhängig von ihr, direkt dem Vorstand unterstellt sein.

IT-Grundschutz: Was ist mit der richtigen Strategie?

Schartner: Es gibt ja mit den IT-Grundschutzkatalogen des BSI sehr gute Literatur zum Thema. Und meist haben Banken bereits ein funktionierendes Risikomanagementsystem, in das sollten auch die IT-Risiken integriert werden. Zusätzlich muss das notwendige Fachwissen über IT-Sicherheit in den Abteilungen und nicht nur bei den IT-Fachleuten aufgebaut und weiterentwickelt werden.

IT-Grundschutz: Herr Schartner, wir danken Ihnen für das Gespräch.

Symposium Banken

Götz Schartner wird auf der it-sa im Rahmen des Symposium Banken am 12. und 13. Oktober 2009 mehrere Live-Hacking Sessions zum Thema „Angriffe auf Netzwerke deutscher Kreditinstitute“ zeigen.

Admins Albtraum

Die psychologischen Grundlagen des Social Engineering, Teil II

Stefan Schumacher, Sicherheitsberater, Kaishakunin.com

Social Engineering ist vielen IT-Sicherheitsbeauftragten als Gefahr bekannt, doch was sich im Detail dahinter verbirgt, wissen die wenigsten. Im zweiten Teil seiner Artikelserie beschreibt Stefan Schumacher weitere Beeinflussungsmethoden und ihre Hintergründe.

In den letzten 45 Jahren haben sich viele Experimente und Feldstudien mit Autorität befasst. Einige Verhaltensbiologen untersuchten beispielsweise Affengruppen in Nordjapan, bei denen neues Essen (Karamellbonbons) in der Gruppe eingeführt wurde. Boten die Forscher die Bonbons zunächst einem niedrigrangigen Tier an, verspeiste es diese mit offensichtlichem Genuss. Allerdings breitet sich der Verzehr der Bonbons kaum in der Gruppe aus. Nach 18 Monaten mochten und verspeisten lediglich 51% der Herdenmitglieder die neuartigen Karamellbonbons. Anders verhielt es sich, wenn die höchstrangigen Tiere angelernt wurden: Nach nur vier Stunden waren die Bonbons in der gesamten Herde bekannt und beliebt.

Kleider machen Gehorsam

Besonders interessant in Bezug auf Autorität ist, dass wir nicht nur auf „echte“ Autorität wie gewünscht reagieren, sondern auch auf zur Schau gestellte. So warb in den USA ein bekannter Schauspieler mehrere Jahre lang in seiner Rolle als Arzt für entkoffeinierten Kaffee und verhalf dem Produkt so zum Durchbruch. Verschiedene Studien untersuchten und identifizierten daher drei Autoritätssymbole: Titel, Uniformen und Luxus. Ein Experiment über Fehlmedikamentierungen in Krankenhäusern kam dabei zu einem erschreckenden Ergebnis. Ein Forscher rief in 22 Krankenhausabteilungen an und gab sich als dortiger Arzt aus. Anschließend wurde einer Krankenschwester oder einem Pfleger aufgetragen, einem bestimmten Patienten 20 mg Astrogen zu verabreichen.

Die Schwester bzw. der Pfleger hätten der Anweisung aus mehreren Gründen widersprechen müssen:

1. die Anordnung erfolgte per Telefon, und war damit per se verboten
2. der anrufende Forscher war der Pflegekraft nicht persönlich bekannt
3. das Medikament war nicht freigegeben
4. die verschriebene Dosis war zu hoch, es sind nur 10 mg pro Tag erlaubt.

Trotzdem marschierten 95% der Schwestern und Pfleger sofort zum Medikamentenschrank und dann zum Patienten. Dort wurden sie von einem Assistenten abgefangen und über das Experiment aufgeklärt.

Ein anderes Autoritätssymbol ist die Kleidung. Verschiedene Studien zum Gehorsam zeigten, dass lediglich 42% der Bitte eines Mannes in Straßenkleidung nachkamen, aber 92%, wenn der Mann eine Wachdienstuniform trug.

Je knapper ein Gut ist, desto wertvoller erscheint es uns. Daher sind limitierte Sonderangebote ein beliebter Verkaufstrick. Ähnliches gilt auch für Informationen - je stärker eingeschränkt sie sind, desto wertvoller erscheinen sie. Besonders stark wirkt dabei die sogenannte Reaktanzreaktion, das heißt, Dinge oder Privilegien, die wir einmal besessen haben und uns nun genommen werden, werden stärker bewertet, als Dinge die wir niemals hatten.

Wo ist John?

Ein Beispiel für den Einsatz solcher Methoden entstammt in Teilen Kevin Mitnicks Buch „Die Kunst des Einbruchs“. Mitnick war in den Neunzigern einer der am meisten gefürchteten Hacker in Amerika. Im Buch beschreibt er zahlreiche Angriffsmethoden, die nur zum Teil oder gar keine technischen Hintergründe haben. Sein Beispiel handelt davon, dass ein kleines amerikanisches Ingenieurbüro eine neue Antriebstechnik für Kleinflugzeuge entwickelt hat. Ein Konkurrent möchte diese haben und setzt dazu Social Engineering Techniken ein.

Durch eine Meldung auf der Webseite bringt der Angreifer in Erfahrung, dass John Smith, der Chef des Ingenieurbüros auf einer Flugschau in Europa weilt, also ein paar Tage nicht verfügbar sein wird. In dieser Zeit mietet der Angreifer eine teure Limousine samt Chauffeur, außerdem kauft er sich teure Kleidung und lässt sich professionell frisieren. Er möchte den Eindruck eines gut bezahlten (und entsprechend wichtigen) Managers machen. Er lässt sich beim Ingenieurbüro vorfahren und stellt sich an der Rezeption als Bob von Boeing vor, der die Handbücher abholen möchte, die Johnny ihm versprochen hat.

Die Rezeptionistin weiß natürlich von nichts und blockt Bob zunächst ab. Dieser legt daraufhin seine (gefälschte) Visitenkarte von Boeing vor und stellt sich als leitender Entwicklungsingenieur vor. Er habe Johnny, den Chef, auf einer Flugschau getroffen und sich mit ihm über die neue Antriebstechnik unterhalten. Inzwischen sei man sich handelseinig geworden, Bob habe die Technik bei Boeing vorgestellt und Boeing möchte sie nun für sehr viel Geld kaufen. Allerdings benötigt Bob dringend, am besten sofort, die technischen Handbücher dazu, da er noch einige Kritiker bei Boeing überzeugen muss.

Die Rezeptionistin ist erstaunt und erfreut, schließlich hat Bob ihrer Firma ein erfreuliches Angebot unterbreitet. Daher leitet sie Bob an den stellvertretenden Chef weiter. Diesem erzählt Bob die gleiche Geschichte und bittet darum, möglichst sofort die Handbücher zu bekommen. Da der stellvertretende Chef John wegen der Zeitverschiebung nach Europa nicht sofort erreichen kann, ist Bob verstimmt und droht damit, dass Geschäft platzen zu lassen. Nach einigem Hin und Her übergibt der Stellvertreter Bob die Handbücher. Einige Wochen später patentierte der Konkurrent die Technik, einige Monate später ging das Angriffsopfer in Konkurs.



Stefan Schumacher ist selbständiger Unternehmensberater im Bereich Security Awareness und Security Management. Er studiert zur Zeit Bildungswissenschaft und Psychologie in Magdeburg und befasst sich mit der IT-Sicherheit aus sozialwissenschaftlicher Sicht.

Trau, schau, wem

Dieses Beispiel nutzt mehrere Social-Engineering-Techniken aus. Der Angreifer informiert sich auf der Webseite des Unternehmens darüber, das der Chef in Europa weilt und daher zumindest telefonisch nicht sofort erreichbar ist (passive Informationssuche). Heute würde man solche Infos wohl in Rekordzeit bei Twitter finden. Dann verkleidet er sich als Top-Manager (Autorität) und authentisiert sich mit einer Visitenkarte, die man für ein paar Dollar herstellen kann. Er macht der Firma ein lukratives Kaufangebot, zieht es aber später wieder zurück, als er die Handbücher nicht bekommen soll (Reaktanzreaktion). Dadurch setzt er den stellvertretenden Chef unter Druck. Außerdem spricht er von Johnny, gibt also vor mit dem Chef auf einer eher jovialen Ebene zu verkehren.

In der nächsten Ausgabe stellt der dritte Teil der Serie weitere Techniken und Beispiele für Angriffsmethoden vor.

Admins Albtraum

Die psychologischen Grundlagen des Social Engineering, Teil III

Stefan Schumacher, Sicherheitsberater, Kaishakunin.com

Mittels Social Engineering kann ein Angreifer über Hochstapelei und Trickbetrug umfangreiche Informationen aus Mitarbeitern herausholen, die ihm weitere Angriffe ermöglichen oder sogar schon die gewünschten Zielinformationen enthalten. Der dritte Teil nennt weitere psychologische Grundlagen, die sich Angreifer zu nutze machen.

Mitte der 1960er erregte in New York ein Mord öffentliches Aufsehen. Dabei wurde eine junge Frau auf offener Straße von einem Messerstecher angegriffen - obwohl 38 Zeugen von ihren Wohnungen aus zusahen. Grund für das „nicht-sehen-wollen“ ist die so genannte Verantwortungsdiffusion. Die Zuschauer waren von der außergewöhnlichen Situation verunsichert und wussten nicht, wie sie sich verhalten sollten. Sie beobachteten die Reaktionen der anderen Zeugen, um sich an diesen zu orientieren. Da alle Zeugen so reagierten, entstand eine Art psychologischer Gridlock. Jeder versuchte aus dem Verhalten der anderen, eigene Regeln abzuleiten. Weil niemand die Initiative ergriff, griff auch niemand ein. Diese Theorie, der „passive bystander effect“ wurde in Dutzenden weiterer Experimente bestätigt und ausgebaut.

Soziale Bewährtheit

Unsicherheit verstärkt die Orientierung an anderen Personen. Wenn wir nicht wissen, wie wir uns verhalten sollen, machen wir eben das, was alle machen. Das muss nicht unbedingt zum besten Ergebnis führen, zumindest kann einem aber niemand das eigene Verhalten vorwerfen, man sticht nicht negativ aus der Menge heraus.

Eine weitere Einflussgröße ist die Ähnlichkeit innerhalb der Vergleichsgruppe (engl. peer group). Je ähnlicher die Vergleichsgruppe dem Individuum ist, desto höher ist ihr Einfluss. Dies wurde erstmals im 18. Jahrhundert als sog. Werther-Effekt beobachtet. Nachdem Goethe sein Buch „Die Leiden des jungen Werther“ veröffentlicht hatte, in dem sich der Protagonist das Leben nimmt, schwappte eine Suizidwelle junger Männer erst durch die deutschen und dann durch die europäischen Staaten. Teilweise trugen dabei die Suizidenten dieselbe Kleidung wie Werther im Roman.

Nicht wirklich überraschend ist es, dass uns sympathische Menschen eher zu etwas verleiten können als abstoßende. Jeder Verkäufer versucht daher, dem Kunden gegenüber besonders sympathisch zu erscheinen, denn Sympathie verstärkt alle anderen eingesetzten Überzeugungstricks. Sympathie ist sehr gut erforscht, insbesondere die Auslösemerkmale sind bekannt. Mehrere Versuche mit Fotos ergaben, dass attraktiven Personen generell positivere Eigenschaften zugeschrieben werden, selbst wenn diese eigentlich gar nicht beurteilt werden können. So werden attraktivere Menschen bei Vorstellungsgesprächen oder von Geschworenen-Gerichten bevorzugt, verdienen



Steht Ihre Verteidigungslinie?

Hält Sie einem Angriff stand? **Probieren Sie es aus!**

Beweisen Sie, wie schnell Sie auf einen Angriff reagieren...

Ganz einfach bei einem Besuch am Stand des Informationsdienstes IT-Grundschutz auf der IT-Security-Messe it-sa in Halle 6 Stand 629. Spielen Sie eine Runde Tischfußball an unserem nagelneuen „Kicker“ – treffen Sie am Stand andere Leser, die an einem kleinen Match Spaß haben. Vielleicht treffen Sie dort auch den ein oder anderen interessanten Gesprächspartner.

Mit dem IT-Grundschutz sind Sie auf alle Angriffe gut vorbereitet!

Für Abonnenten: Am Stand erhalten Sie im Tausch gegen den in dieser Ausgabe beiliegenden Gutschein Ihre VIP-Bons für die it-sa VIP-Lounge! Sie sind noch nicht Abonnent? Dann ist das die Gelegenheit, unsere günstigen Messeangebote kennen zu lernen!

IT·Grundschutz Informationsdienst

Halle 6 Stand 629

it sa Die IT-Security-Messe

mehr, oder haben mehr Erfolg bei Wahlen. Der Halo-Effekt ist nicht nur auf Menschen beschränkt, sondern kann auch bei der Konstruktion von Fragebögen eine Rolle spielen. Dabei überstrahlt eine Frage emotional alle Nachfolgenden.

Ebenso wichtig ist die Ähnlichkeit in Erscheinung, Herkunft oder Interesse. Damit lassen sich Sympathie und Hilfsbereitschaft steigern. Autohändler versuchen beispielsweise aus dem Wagen des Kunden Rückschlüsse auf dessen Hobbys zu ziehen und sprechen diese Themen im Verkaufsgespräch an. Eine Analyse von Versicherungsdaten zeigte, dass Kunden eher eine Versicherung abschlossen, wenn zum Vertreter Ähnlichkeit hinsichtlich Alter, Religion, politischer Einstellung bestand. Selbst die Frage ob er Raucher oder Nichtraucher war, beeinflusste das Ergebnis.

Komplimente lassen niemanden kalt – selbst wenn wir wissen, das sie nicht ernst gemeint sind. So zeigte ein Experiment mit einer Gruppe von Männern, dass eine Person, die positive Äußerungen über Testkandidaten abgab, am beliebtesten war, sogar wenn den Versuchspersonen bewusst war, dass sie sich damit nur einschmeicheln will. Die Komplimente wirkten auch wenn sie total übertrieben oder offensichtlich unwahr waren.

Jawohl, Herr General

Wirkungsvoll ist auch das Prinzip der Autorität. Stanley Milgram führte 1974 ein Experiment durch, das die gesamte Psychologie beeinflusste. Er suchte per Zeitungsannonce nach Versuchspersonen für ein Lern-Experiment. Im Laufe des Experiments wurde die Versuchsperson als Lehrer eingeteilt und musste eine zweite Person abhören und bei Fehlern bestrafen. Zur Strafe verteilte ein Generator Stromschläge von 15 Volt. Die Spannung stieg mit jedem Fehler um 15 Volt an. Ein Versuchsleiter ermunterte die Kandidaten, die Spannung zu steigern und weitere Strafen zu verteilen. Das „Opfer“ wurde natürlich von einem Schauspieler dargestellt, der die Schmerzen der Stromschläge nur simulierte.



Stefan Schumacher, Sicherheitsberater, Kaishakunin.com

Von insgesamt 40 Versuchspersonen gingen 26 bis zur höchsten Stufe von 450 Volt. Alle 40 gingen bis 300 Volt, erst darüber brachen die ersten ab und weigerten sich weiterzumachen. Die Frage, warum die Versuchspersonen Stromschläge auch gegen ihre eigene Überzeugung verteilten, wurde mit dem Autoritätsprinzip beantwortet. Die Versuchspersonen gerieten in ein Dilemma: Sie merkten, dass sie dem „Opfer“ ernsthafte Schmerzen zufügten, wussten aber nicht, wie sie sich verhalten sollten. Daher wendeten sie sich an den Versuchsleiter und ließen diesen entscheiden. In anderen Experimentaldurchgängen stand der Versuchsleiter nicht mehr als klischeehafter Universitätsdozent vor den Versuchspersonen, sondern als privater Forscher in Jeans und T-Shirt. Dies hatte zur Folge, dass die Anzahl der Versuchspersonen, die bis 450 Volt gingen, dramatisch sank.

Angriffe erfordern Vorbereitung

Für gewöhnlich setzen erfolgreiche Social Engineering Strategien mehrere lokale Geplänkel ein, die sich über einen längeren Zeitraum erstrecken. Ein Angreifer könnte den Namen einer ranghohen Sekretärin googeln und so herausfinden, das diese ein Reitpferd hat. Dann ruft er die Sekretärin an und stellt sich als neuer Mitarbeiter vor. Er kann ein einfaches Computerproblem vortäuschen, um Hilfe bitten und dabei beiläufig erwähnen, dass er früher nach Hause geht, weil das Pony der Tochter noch zum Tierarzt muss. Sicherlich wird die Sekretärin auf diesen Reiz reagieren und das Gespräch auf Pferde lenken. Ein paar Tage später ruft er bei der Sekretärin an und berichtet von der Behandlung des Ponys, Details dazu hat er sich wieder ergoogelt. Wieder ein paar Tage später ruft er erneut mit einem Netzwerkproblem an und versucht im Laufe des Gesprächs die Namen und Telefonnummern von Administratoren, Security Managern oder gar direkt Passwörter zu erbeuten.

Auch bei Ausnutzung aller psychologischen Grundlagen gibt es kein Schema F für Social Engineering Angriffe und daher auch nicht für deren Abwehr. Der Angreifer muss sich auf seine Intuition und seine soziale Kompetenz verlassen, das Zielobjekt hingegen benötigt die Fähigkeit, soziale Beziehungen und Kontexte zu deuten. Daher ist es notwendig, in Organisationen eine Sicherheitskultur zu etablieren. In Awareness-Schulungen kann Sicherheitsbewusstsein hergestellt oder geschärft werden. Hilfreich ist es auch, sinnvolle Authentifizierungsmechanismen wie Dienstausweise, Anruf-Parolen oder TAN-Listen zu etablieren. Diese helfen aber nur, wenn sie nicht zu restriktiv eingesetzt und sozial akzeptabel gestaltet werden.