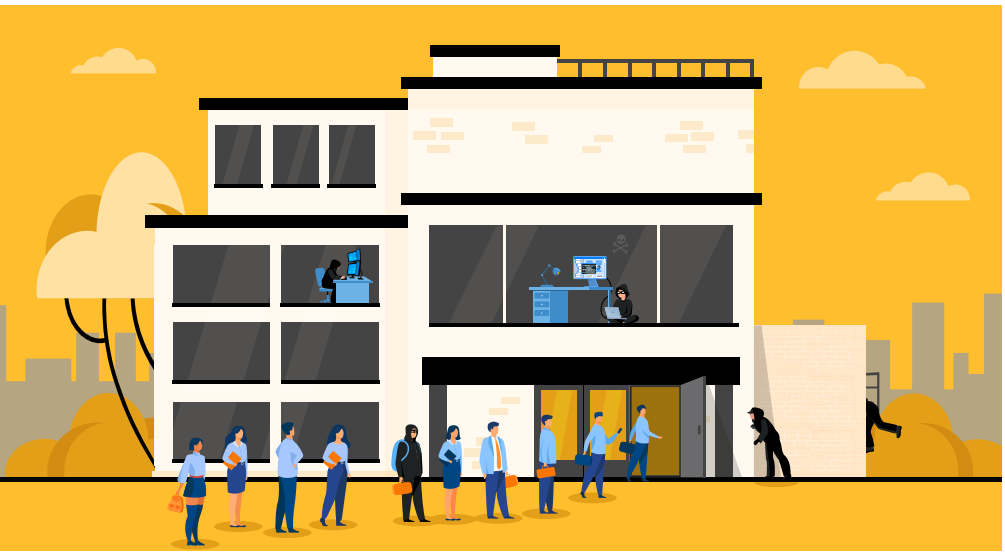


Layer 8 – Faktor Mensch

Social Engineering findet nicht nur hinter der Tastatur statt. Unser Autor dringt seit Jahren durch geschicktes Manipulieren von Menschen mithilfe psychologischer Tricks und Kenntnisse in Firmengebäude ein – selbst in gut gesicherte. Natürlich nur im Auftrag und zu Testzwecken.

Von Andreas Heideck

Der Mensch ist von Natur aus freundlich und hilfsbereit – auch wenn man das manchmal kaum glauben mag. Diese Freundlichkeit und Hilfsbereitschaft spiegeln jedoch meine Erfahrungen der letzten acht Jahre wider, bei denen ich diese positiven Eigenschaften ausgenutzt habe, um durch Social Engineering in unzählige Unternehmen und Organisationen wie Banken, Forschungseinrichtungen und Rechenzentren zu gelangen. Dieser Beitrag beschreibt das Vorgehen und die Einfachheit mancher Angriffe, die es mir unter anderem ermöglicht haben, selbst in hoch abgesicherte Infrastrukturen einzudringen. Wer befürchtet, dass Social Engineering, also die Manipulation von Menschen, immer funktionieren wird, dem soll dieser Artikel Wege zeigen, wie man den Faktor Mensch und das daraus resultierende Risiko minimiert und dabei freundlich und hilfsbereit bleibt.

Information Gathering: das Ziel kennen

Informationen sind das neue Gold, das gilt auch oder besonders beim Social Engineering. In einer ersten Phase werden so viele Informationen wie möglich gesammelt – über das Unternehmen, über Mitarbeiter, bevorstehende Events, das Verhalten der Mitarbeiter und den Slang des Unternehmens, über die Unternehmenskultur und vieles mehr. In dieser ersten Phase geht es darum, sich ein Bild über das Unternehmen zu machen, ein Gefühl zu bekommen, wie es tickt.

Dabei helfen Suchmaschinen wie Google, unter Zuhilfenahme von Google Dorking – also speziellen Google-Suchanfragen – oder die IoT-Suchmaschine Shodan, um relevante Informationen zu gewinnen. Diese unterstützen die Angreifer dabei, sich eine geeignete Vorgeschichte (Pretext) aufzubauen. Auch soziale Netzwerke wie Facebook, Xing und LinkedIn sowie Bewertungsplattformen wie kununu sind hilfreich, um ein Gesamtbild zu erhalten. Ebenso ermöglichen es Tools wie Maltego, in kurzer Zeit viele Informationen gebündelt zu sammeln. Dieses Information Gathering (auch OSINT für Open Source Intelligence) ist eigentlich keine Phase, sondern ein Kreislauf, der sich über das ganze Projekt erstreckt. Ob ein Angriff erfolgreich ist, steht oder fällt mit den Informationen, die ein Angreifer hat.

iX-TRACT

- Mit guter Vorbereitung und den richtigen psychologischen Tricks ist es häufig möglich, Menschen zu täuschen und selbst in gut gesicherte Gebäude und Einrichtungen einzudringen.
- Für solche Tests braucht es auf allen Seiten Empathie und Fingerspitzengefühl: Es geht nicht darum, Menschen bloßzustellen, sondern darum, fehlerhafte Prozesse zu finden.
- Sicherheitstests, kreative Schulungen und die richtige Unternehmenskultur bewirken bei Mitarbeitern mehr Sensibilisierung als stumpfes Papierlernen oder Webseitenklicken.

Methoden und Techniken

Social Engineering kann sehr komplex, aber auch sehr einfach sein. Die meisten Angriffe sind sehr einfach: Techniken wie Tailgating (Durchschlüpfen) und Piggybacking (unbefugtes Nachlaufen) helfen dabei, in einen gesicherten Bereich zu gelangen. Beim Tailgating folgt der Angreifer einer Person in einen geschützten Bereich, wobei diese Person nicht weiß, dass jemand ihr folgt. Man wartet also nur ab, bis eine berechtigte Person eine verschlossene Tür öffnet, um diese dann aufzuhalten, bevor sie sich wieder schließt.

Beim Piggybacking interagiert der Angreifer mit der Zielperson, um durch Vortäuschen falscher Tatsachen in einen geschützten Bereich einzudringen. Das kann bedeuten, dass der Angreifer zum Beispiel etwas trägt oder sich mit der Zielperson einfach unterhält. Das Opfer sieht also in diesem Fall den Täter, weiß aber nicht, dass diese Person nicht zum Unternehmen gehört und keine Berechtigung hat, den Bereich zu betreten. Diese beiden einfachen Techniken ermöglichten mir, in viele Unternehmen und Bereiche einzudringen und mein Ziel zu erreichen. Natürlich gehört auch ein sicheres Auftreten und ein guter Pretext, also eine gute Story, dazu, um nicht aufzufallen.

Die Wirkung auf andere kann man mit dem sogenannten Halo-Effekt beeinflussen. Darunter versteht man, dass ein bestimmtes Merkmal andere Merkmale überstrahlt. Wenn etwa jemand einen Anzug anhat, hat es den Effekt, dass andere diese Person zum Beispiel für jemanden in einer Führungsposition halten. Ist diese Person die einzige, die in gewissen Bereichen einen Anzug anhat und sich auch dementsprechend verhält, ist die Wahrscheinlichkeit sehr hoch, dass

andere sie mehr respektieren, auch wenn sie vorher noch nie da war. Die Auswirkungen des Halo-Effekts habe ich in vielen Fällen erfolgreich ausgetestet.

Zugehörigkeitsgefühl als Türöffner

Einige weitere psychologische Mechanismen beziehungsweise Verhaltensweisen helfen dem Social Engineer bei seiner Arbeit. Social Proof etwa im Zusammenhang mit Social Engineering bedeutet, sich so zu verhalten, wie andere das mutmaßlich gut finden. Ich passe mich also an eine Person oder eine Gruppe an und verhalte mich genauso wie sie. Zum Beispiel spreche in einem Raucherbereich über dieselben Themen wie alle anderen, und wenn sie wieder ins Gebäude gehen, gehe ich einfach mit, ich gehöre ja dazu.

Reziprozität ist die Erwartung beziehungsweise beim Social Engineering die Hoffnung, dass, wenn man jemandem etwas Gutes tut, man mit gleicher Münze bezahlt wird. Öffne ich also jemandem im Eingangsbereich einer Firma die Tür, ist die Wahrscheinlichkeit sehr hoch, dass diese Person mir die nächste Tür, durch die man vielleicht nur mit RFID-Karte kommt, freundlicherweise auch öffnet.

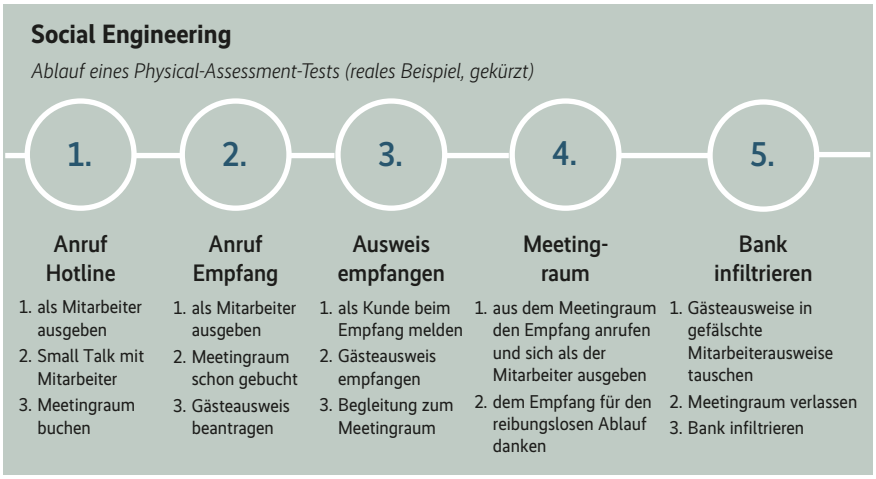
Priming bedeutet vereinfacht gesagt, dass vorausgehende Reize Einfluss auf die Verarbeitung nachfolgender Reize haben. Zum Beispiel kann eine Person durch den geschickten Einsatz von Wörtern, Bildern oder Tönen unterbewusst zu einer bestimmten Handlung verleitet werden.

Durch Elizitieren versucht man, dem Gesprächspartner vertrauliche oder hilfreiche Informationen zu entlocken. Bei einer Weihnachtsfeier, bei der Kollegen und ich uns selbst eingeladen hatten, konnten wir zum Beispiel durch lockere Gespräche mit den Mitarbeitern Produktinformationen erhalten, die nicht für die Öffentlichkeit bestimmt waren.

Beim Rapport geht es darum, zu jemandem eine Beziehung und somit Vertrauen aufzubauen, mit dem Hintergedanken, (vertrauliche) Informationen zu erhalten und dabei idealerweise beim Gesprächspartner noch ein gutes Gefühl auszulösen.

Aus der Ferne zum Erfolg

Etwas komplizierter ist es, beim Telefonieren mit einer Hotline, dem Empfang oder Wachpersonal vertrauliche Informationen herauszufinden oder eine Aktion des Personals auszulösen. Oft geben wir Social Engineers uns als Beschäftigte des Unternehmens aus, die um Hilfe bitten. Im Hintergrund nutzen wir YouTube als Geräuschkulisse, um unsere Aussage zu verstärken. Für das Personal klingt es dann zum Beispiel so, als wären wir gerade auf einer Messe, bei einem Workshop oder zu Hause mit einem schreienden Baby. Wir als „Mitarbeiter“ benötigen dann dringend Informationen, um zum Beispiel Gäste zu empfangen (Gästeausweis beantragen), Meetingräume zu buchen oder Informationen über „Kollegen“ und firmeninterne Abläufe herauszufinden.



Bei sorgfältiger Planung und glaubhafter Durchführung der einzelnen Schritte bestehen gute Aussichten, in das Zielobjekt, im konkreten Fall eine Bank, einzudringen.

Das Schwierige am Telefonat ist, dass man die Körpersprache und die Mimik (Makro- und Mikroexpressionen) des Gegenübers nicht sehen und somit auch nicht einschätzen kann. Wir hoffen jedoch, durch die Geräuschkulisse und unsere Stimmlage beim Opfer Empathie für uns und unsere Emotionen (Stress, Verzweiflung et cetera) auszulösen. Dabei spielt es keine Rolle, ob der Angerufene ein wenig skeptisch ist, was wir in diesem Fall sogar unterstützen und am Telefon bekräftigen, um vertrauenswürdiger zu wirken. Jede noch so kleine Information hilft einem Angreifer, seinen Pretext auszubauen.

Ein reales Beispiel: Ziel war es, in eine gut gesicherte Bank einzudringen, um Kundendaten abzugreifen. Um an Gästeausweise zu gelangen, die normalerweise nur durch einen Mitarbeiter beantragt werden können, versuchten wir uns als solcher auszugeben. Wir riefen zuerst die Hotline an, um uns einen Besprechungsraum zu buchen, der unsere Glaubwürdigkeit beim nächsten Telefonat mit der Wache verstärken und später als Backup dienen sollte. Ein kurzer Small Talk mit dem Hotline-Mitarbeiter überzeugte diesen, dass wir auch Mitarbeiter seien, gerade unterwegs seien und vergessen hätten, einen Besprechungsraum zu buchen. Da der Besprechungsraum keine Gefahr darstellte, wurde er freundlicherweise für uns gebucht, unter dem Namen eines real existierenden Mitarbeiters.

Die Falle schnappt zu

Im nächsten Schritt riefen wir die Wache an, gaben uns wieder als Mitarbeiter aus, die in einem wichtigen Meeting sitzen, und baten darum, Gästeausweise für zwei Kunden auszustellen. („Den Meetingraum haben wir schon gebucht, jedoch vergessen, die Gästeausweise zu beantragen“.) Nach einem kurzen Small Talk bat uns die Wache, unsere Anfrage noch einmal per E-Mail zu bestätigen. Dem kamen wir mit einer gefälschten E-Mail (Spoofing der E-Mail-Adresse) an den Empfangsmitarbeiter nach. Das Resultat: Wir konnten unsere selbst beantragten Gästeausweise am Empfang abholen und die Wache brachte uns in den von uns gebuchten Besprechungsraum.

Bevor wir die Bank betraten, riefen wir jedoch noch einmal als Mitarbeiter an und baten die Wache, die Kunden schon zum Besprechungsraum zu bringen, da es etwas später werden könne. Um keine böse Überraschung zu erleben, riefen wir später erneut als Mitarbeiter aus dem Besprechungsraum an und dankten der Wache, dass alles so gut funktioniert habe. Nun hatten wir gültige Gästeausweise und konnten uns frei in der Bank bewegen.

Keep it simple

Die einfachsten Angriffe sind meist die effektivsten. Wie erwähnt kann schon das einfache Hinterherlaufen Türen und

Tore öffnen. Ein einfacher Anruf als Mitarbeiter führt dazu, dass Gästeausweise bereitgestellt werden, die es ermöglichen, legitim das Gebäude zu betreten. Aber was, wenn man angesprochen wird oder sich in einem Bereich aufhält, in dem man eigentlich gar nicht sein darf? Was, wenn Mitarbeiter oder das Wachpersonal skeptisch sind, einen anschreien oder mit der Polizei drohen?

Auch hier gilt es, eine leicht verständliche Antwort oder Ausrede parat zu haben und vor allen Dingen Ruhe zu bewahren. Letzteres ist nicht immer einfach, da Puls und Adrenalinspiegel nach oben gehen. Ich habe Situationen erlebt, bei denen mich das Wachpersonal angeschrien hat, weil ich in einem Bereich war, in dem ich nichts zu suchen hatte. Eine Ablenkung, in diesem Fall ein Schlüssel, den ich angeblich vor der Tür gefunden hatte, verschob den Fokus weg von mir auf den Schlüssel. Der Wachmann beruhigte sich, sah mich nicht mehr als Bedrohung und versuchte nun, mir zu helfen. Ich erzählte ihm, dass ich den Schlüssel hier abgeben wollte. Nach einem kurzen Gespräch dankte er mir und ließ mich gehen – was für mich in diesem Fall auch sehr überraschend war. Dieser Trick, angeblich etwas gefunden zu haben, einen Schlüssel oder eine Zutrittskarte (ich habe immer mehrere gefälschte Karten in der Tasche), half mir schon in vielen Situationen.

> „Es liegt in der menschlichen Natur, vernünftig zu denken und unvernünftig zu handeln."
>
> *Anatole France*

Menschen wollen keine komplizierten Antworten, sondern leicht verständliche und nachvollziehbare. Wenn ich allein unterwegs bin und nicht möchte, dass ich angesprochen werde, gebe ich meistens vor, zu telefonieren, da man ungern jemanden unterbricht, der gerade spricht. Bin ich mit einem Kollegen unterwegs, unterhalte ich mich mit ihm, zum Beispiel über ein bevorstehendes Meeting. Das rechtfertigt unseren Aufenthalt und wendet Fragen ab.

Es gab auch Situationen, in denen ich mich selbst eingesperrt habe, also einen Bereich betrat, in dem sich kein Personal aufhielt und der Ausgang nur durch eine Chipkarten-gesicherte Tür möglich war. Da dies jedem einmal passieren kann, klopfte ich einfach an eine Scheibe und bat den nächsten Mitarbeiter, die Tür wieder zu öffnen. Meine Ausrede war, dass ich ganz sportlich die Treppe nutzen wollte und die falsche Tür erwischt hatte. Die Mitarbeiterin, die mir die Tür öffnete, wunderte sich nicht, dass ich keinen Ausweis hatte, um mir selbst die Tür zu öffnen, sondern lachte über meine Aussage und ging weiter.

Das Layer-8-Problem

Ob kleine Unternehmen, große Weltkonzerne, Forschungseinrichtungen, Banken oder Rechenzentren – meine Kollegen und ich schafften es jedes Mal, einzudringen. Bei manchen Firmen war es ein Kinderspiel, da Türen und Tore im wahrsten Sinne des Wortes offenstanden. Wir konnten einfach hereinspazieren, einen Keylogger anschließen, Rechner mitnehmen oder Fotos von Kundendaten machen. Manche Einrichtungen, zum Beispiel Rechenzentren, sind allerdings genauso gut abgesichert wie ein Gefängnis. Das bedeutet druckempfindliche Zäune, patrouillierende Wachen und Vereinzelungsschleusen. Unsere einzige Möglichkeit, besonders weil unsere Testzeit oft sehr kurz ist, ist der im OSI-Referenzmodell als fiktiver Layer 8 bezeichnete menschliche Faktor.

In keinem meiner Projekte nutzte ich Autorität, um ein Ziel zu erreichen. Menschen während eines Projektes zu manipulieren oder zu beeinflussen, heißt nicht, sie einzuschüchtern, sondern ihnen im Gegenteil ein gutes Gefühl zu geben. Dem Mitarbeiter soll es nach einem Gespräch besser gehen als vorher. Und dieses Gefühl wollen wir aus zweierlei Gründen vermitteln. Zum einen wollen wir niemanden auf einer seelischen Ebene angreifen und keine Ängste schüren, da er nur Mittel zum Zweck ist. Bei unseren Tests manipulieren wir zwar Menschen, aber eigentlich prüfen wir Prozesse, die nicht eingehalten werden oder die es gar nicht gibt.

Zum anderen würde ein Mitarbeiter das Vertrauen zu seinem Unternehmen verlieren, wenn wir durch persönliche Angriffe ein durch das eigene Unternehmen beauftragtes Projekt durchführen. Auch wenn wir mit versteckter Kamera unsere Einbrüche filmen, werden alle Personen in der Dokumentation unkenntlich gemacht und auch keine Zeiten notiert, wann wir wo waren. Natürlich kann der Kunde Letzteres durch Überwachungskameras herausfinden, es verschafft ihm jedoch keine Vorteile. Bei jedem Vorgespräch mit dem Kunden wiederhole ich mehrmals, dass es bei unseren Tests nicht um die Menschen geht, sondern um die Prozesse.

Kein Mensch ist davor gefeit, Opfer eines Social Engineers zu werden, jedoch können Prozesse geschaffen werden, die es einem realen Angreifer erschweren, seine Opfer zu manipulieren. Dazu zählen unter anderem Leitfäden, Schulungen, Awareness-Trainings und Maßnahmen, die die Mitarbeiter an die Gefahren erinnern (Schilder an Türen, Desktop-Wallpaper und so weiter). Mitarbeiter sollten wissen, wie Angreifer agieren, um darauf richtig zu reagieren. Bei den Unternehmen, die wir seit mehreren Jahren testen, tragen die eingeführten Prozesse dazu bei, dass wir immer kompliziertere Angriffe konzipieren müssen, um das Ziel zu erreichen, oder es in der vorgegebenen Zeit nicht mehr schaffen.

Der Faktor Erfahrung

Auch wenn sich manche Angriffe sehr leicht anhören, gehört sehr viel Erfahrung dazu. Auch sollte die Testzeit nicht zu kurz angesetzt werden. Ich habe Kollegen erlebt, die bei ihrem ersten Test Blut und Wasser geschwitzt haben. Ich musste den Test daraufhin unterbrechen und den Kollegen eine Auszeit gönnen. Andere Kollegen hingegen waren bei ihren ersten Tests so cool, als würden sie das schon seit Jahren machen. Auch wenn ich diese Tests schon seit sehr vielen Jahren durchführe, heißt es nicht, dass ich nicht auch überrascht werden kann und mir die Worte wegbleiben (was bisher allerdings noch nicht vorkam). Da hilft es, einen Kollegen dabeizuhaben, der in diesem Moment unterstützt, um die Situation zu retten.

Einen geeigneten Consultant zu finden ist nicht immer so einfach, da es bei einem solchem Test nicht darum geht, Menschen reinzulegen, sie fertigzumachen und zu demonstrieren, wie dumm sie sich verhalten haben. Es geht wie erwähnt darum, die Wirksamkeit von Prozessen und Maßnahmen zu testen. Bei manchen Aussagen in der Vergangenheit war von vornherein klar, dass der betreffende Consultant für solche Tests nicht geeignet war.

Eine der wichtigsten Voraussetzungen für einen erfolgreichen Test ist für beide Seiten, für den Auftraggeber (Kunden) sowie für uns als Testinstanz (Angreifer), Empathie für andere Menschen zu empfinden. Es geht darum, jederzeit den Menschen richtig einschätzen zu können und zu wissen, wie weit man gehen darf, damit ein Test auch nur ein Test bleibt. Beide Seiten sollen mit positiver Erfahrung aus diesem Test gehen. Er soll einen Mehrwert für alle generieren und das

Vertrauen der Mitarbeiter in das Unternehmen und das Vertrauen des Kunden gegenüber uns als Testpersonen stärken.

Der Faktor Zeit

Das Budget für solche Tests, wie auch für andere Sicherheitsanalysen, ist manchmal sehr knapp bemessen. Für einen Social-Engineering-Angriff sollte die Zeit jedoch nicht zu knapp kalkuliert sein. Um den Kunden einen Mehrwert zu bieten, sollten solche Angriffe realistisch durchgeführt werden. Das bedeutet, es sollte nicht einfach getestet werden, ob man irgendwo hineingehen kann und erwischt wird oder nicht. Das kann man auch billiger bekommen und dann entscheidet der Zufall, ob ein Angriff von Erfolg gekrönt ist oder nicht.

Für Zufall oder Glück sollte ein Kunde nicht bezahlen, sondern für einen professionell simulierten und gut vorbereiteten Angriff, der zwar in einer verkürzten, aber realistischen Testzeit durchgeführt werden kann. Denn wenn wir es in ein bis zwei Wochen schaffen, in einen Serverraum einzudringen, auf Kundendaten zuzugreifen, Zugriff selbst auf vertrauliche Daten zu erhalten und quasi zum Unternehmen zu gehören, dann schaffen es auch die echten Angreifer, die wesentlich mehr Zeit dafür haben.

Social Engineering missverstanden

Social Engineering ist an sich etwas Alltägliches. Als bestes Beispiel dafür dienen Kinder. Wenn meine Kinder etwas von mir wollen, ob es Süßigkeiten sind, eine Taschengelderhöhung oder das neue Spielzeug, werden sie zu Meistern der Manipulation. Durch Mimik und Gestik, durch Schmeicheleien und durch Ausnutzung von Gefühlen versuchen sie, mich zu etwas zu verleiten, um ihr Ziel zu erreichen.

Ein anderes Beispiel ist der Arzt, der mit allen Mitteln versucht, seine Patienten zu einer Ernährungsumstellung zu überreden, um dadurch zu erreichen, dass sie ein besseres und gesünderes Leben haben. Social Engineering dient also nicht notwendigerweise dazu, jemandem etwas Böses anzutun oder eine Situation auszunutzen, sondern auch dazu, jemandem zu helfen.

Da aber wie bei fast allem im Leben alles Gute auch zum Schlechten eingesetzt werden kann, ist es wichtig, den Unternehmen und Menschen zu zeigen, wie sie das Gute vom Schlechten unterscheiden können.

Eine oft geäußerter Satz lautet „Social Engineering wird doch immer funktionieren“. Genau wie es keine hundertprozentige (IT-)Sicherheit gibt, wird es auch immer einen Weg geben, menschliches Verhalten auszunutzen, um Schaden anzurichten. Jedoch ist der entscheidende Faktor, die Messlatte für einen Angreifer so hoch zu legen, dass er sein Ziel nur mit enormem Aufwand erreichen kann. Und die Kosten für ein Unternehmen, diese Sicherheit zu schaffen, sind wesentlich geringer als der Schaden, den ein Angreifer anrichten kann.

Was also tun?

Schaffen Sie eine Unternehmenskultur, die es erlaubt, Verhalten und Personen zu hinterfragen. Das bedeutet zum Beispiel, dass, wenn ein Mitarbeiter eine fremde Person bittet, den eigenen Sicherheitsausweis für die Tür zu nutzen, und diese Person eine dem Mitarbeiter im Unternehmen höhergestellte Person ist, der Mitarbeiter nicht mit Konsequenzen rechnen müssen sollte. Auch dann nicht, wenn es „nur“ um eine E-Mail geht, mit der er indirekt gerügt wird.

Schulen Sie Mitarbeiter auf eine kreative Art, zum Beispiel durch Rollenspiele oder durch interessante Auftritte von professionellen Angreifern. Ein Mitarbeiter, der mit IT-Sicherheit nichts am Hut hat, wird sich niemals freiwillig in eine einstündige Präsentation setzen oder eine Onlinepräsentation durchklicken. Eine interessante Schulung bietet auch Mehrwert im privaten Bereich, was den Mitarbeiter motiviert, zuzuhören und mitzumachen. Ziel einer solchen Schulung ist es nicht, alle Angriffstechniken zu erörtern und zum Schluss einen dicken Stapel Unterlagen zu verteilen, der sowieso im Müll landet, sondern das Grundverständnis dieser Angriffstechniken zu vermitteln [1].

Schaffen Sie Awareness durch realistisch simulierte Angriffe, die fehlerhafte Prozesse aufdecken und Maßnahmen zur Steigerung der Sicherheit nach sich ziehen. Jedem im Unternehmen muss klar sein, dass diese Art von Tests nur einen Zweck hat: die Unternehmenssicherheit zu verbessern.

Tragen Sie durch Awareness-Maßnahmen dazu bei, das Gelernte immer wieder aufzufrischen. Das können Plakate an der Wand oder an der Tür sein, die daran erinnern, auch einmal einen Blick über die Schulter zu werfen, wenn man in einen geschützten Bereich geht. Erstellen Sie Leitfäden, besonders für Hotline-Mitarbeiter und das Empfangspersonal (Wache), damit diese in fragwürdigen Situationen einem klar definierten Prozess folgen können.

All diese Maßnahmen sollen dazu dienen, aus dem Mitarbeiter keine Maschine zu machen, sondern eine freundliche und hilfsbereite Person, die sich der Gefahren aber bewusst ist und im Ernstfall richtig reagiert.

Fazit

Social Engineering ist keine hochkomplexe Tätigkeit und erfordert keinen Einsatz von Spezialwerkzeugen (obwohl diese auch zum Einsatz kommen können), sondern nutzt das menschliche Verhalten aus, um entweder ein positives oder ein negatives Verhalten auszulösen. Je mehr Zeit ein Social Engineer hat, desto besser kann er sich seinem Ziel anpassen und möglichst unauffällig agieren. Um Social-Engineering-Angriffe zu erkennen, sollten die Mitarbeiter die Gefahren und das Verhalten von Angreifern kennen.

Professionelle Angreifer agieren nicht aggressiv, sondern freundlich und hilfsbereit, bauen eine Beziehung zu ihren Opfern auf, um dann im geeigneten Moment einen Nutzen aus der Situation oder aus der Person zu ziehen. Unternehmen sollten für ihre Mitarbeiter, besonders für solche, die sehr viel Kontakt zu Personen haben, Leitfäden und Handlungsanweisungen erstellen, die ihnen in bestimmten Situationen als Unterstützung dienen. (ur@ix.de)

Quellen

[1] Werner Degenhardt; Vom Wissen zum Handeln; Awareness-Bildung im Security Learning Center; iX 10/2021, S. 119

[2] Christopher Hadnagy; Die Kunst des Human Hacking: Social Engineering in der Praxis; mitp-Verlag 2011

[3] Christopher Hadnagy; Social Engineering enttarnt: Sicherheitsrisiko Mensch; mitp-Verlag 2014

ANDREAS HEIDECK

ist Senior Client Service Manager und IT-Sicherheitsberater bei der Oneconsult. Er ist ein gefragter Spezialist im Bereich Physical Assessment und Social Engineering.