Oberstleutnant d.R. Dipl.-Ing. Günter Holzhauser

Risikoquelle Mensch

Manipulation durch Human-Based Social Engineering

Heute und in Zukunft stellt der Mensch die Risikoquelle Nummer 1 für Organisationen und Unternehmen dar. An 70-80% aller Straftaten ist der Mensch beteiligt. Dies berichten Sicherheitsbehörden, Nachrichtendienste und eine Vielzahl von Fachstudien. Der Autor schreibt für das cpm forum in unregelmäßigen Abständen über Gefahren in Bezug auf die IT und Aspekte der IT-Sicherheit.

Grafik: pinstake.com

RISIKOQUELLE MENSCH: WER VERFÜGT ÜBER WELCHES WISSEN UND WIE KANN MAN DIES ABGREIFEN?

Bei der Aufklärung, der Ausspähung und der Vorbereitung von Angriffen durch professionelle Angreifer, spielt der Mensch eine entscheidende Rolle. Menschen werden angegriffen, weil sie organisations- oder firmenspezifisches Know-how, Zugang zu Wissensträgern (dort ist Know-how manifestiert) und die Zugänge zur internen IT-Systemarchitektur haben. Diese Zugänge sind der Grund, warum Menschen zu den bevorzugten Angriffszielen zählen. Im Vorfeld von IT-Angriffen werden in sehr vielen Fällen das Unternehmen und die IT-Architektur über den Menschen respektive die Mitarbeiter einer Organisation oder eines Unternehmens ausgespäht. Die in Erfahrung gebrachten Informationen bilden die Grundlage für einen professionellen und komplexen Angriff auf eine Organisation.

In der öffentlichen Berichterstattung lesen wir sehr viel über Cyber-Angriffe und IT-Kriminalität, über den ungewollten Abfluss von Daten und Informationen, die Sabotage oder die Übernahme von Internet-Plattformen. Aktuelle Beispiele sind die Angriffe auf den französischen Sender TV5, die deutschen Zulassungsstellen, den hessischen Rundfunk und den Deutschen Bundestag. In dieser Wahrnehmung wird oft vergessen oder nicht gesehen, dass im Vorfeld von solchen Angriffen Menschen/Mitarbeiter erfolgreich manipuliert wurden. Um die oben erwähnten Angriffe durchführen zu können, benötigen die Angreifer sensible Informationen aus der Organisation oder dem Unternehmen, diese Informationen sind öffentlich nicht zugänglich. Die für diese Angriffe notwendigen und wichtigen Insiderinformationen geben die angegriffenen Menschen oder Mitarbeiter oft unbewusst und ungewollt an die Angreifer weiter. Die Manipulation dieser Menschen vollzieht sich auf einer professionellen Ebene. In Fachkreisen wird diese Form des Angriffs als Human-Based Social Engineering bezeichnet.

Die Münchner Firma Corporate Trust hat in ihrer Studie Industriespionage 2014 ausgeführt, dass fast 40% der befragten deutschen Unternehmen Angriffe über Social Engineering zu verzeichnen hatten. Ausgeführt wurden die Angriffe über das geschickte Ausfragen von Mitarbeitern am Telefon, in sozialen Netzwerken, Internetforen, im privaten Umfeld und auf Messen oder Veranstaltungen. Deutsche Unternehmen, die sich nicht mit der eigenen Gefährdungslage auseinandersetzen und in diesem Kontext nicht hinreichend sensibilisiert sind, unterliegen einer hohen Gefährdung.

Die Manipulation des Menschen – Das Human-Based Social Engineering

Unter Human-Based Social Engineering verstehen wir die gezielte Manipulation von Menschen unter Ausnutzung der in uns einprogrammierten sozialen Heuristiken (automatisches Verhalten) mit dem Ziel, Menschen zu einer unbewussten oder ungewollten Handlung zu veranlassen. Ziele und Motive von Angreifern können sehr unterschiedlich sein. Im Kontext von zum Beispiel Wirtschaftsspionage und Konkurrenzausspähung können Angreifer aus dem Spektrum fremder Nachrichtendienste, Wettbewerbern oder beauftragten Dritten (Crime as a Service) kommen.

Warum Social Engineering so erfolgreich ist, hat viel mit Evolution, Sozialisation, Psychologie, Typologie und damit menschlichen Strukturen zu tun.

Auf höherer Abstraktionsebene betrachten wir die in uns verankerten evolutionären Heuristiken. Welche sozialen Heuristiken sind dafür verantwortlich, dass Menschen so einfach zu manipulieren und Angriffe über das Social Engineering meist erfolgreich sind? Wissenschaft und Experten haben sechs Verhaltensmuster identifiziert.

Reziprozität

Reflex der Gegenseitigkeit und Wechselwirkung. Die inhärente Erwartung des Angreifers, dass Verhalten gespiegelt wird, ist meist erfolgreich, da der Angegriffene aus seiner evolutionären Programmierung das Verhalten spiegeln möchte. Wenn ihnen ein anderer Mensch etwas Gutes tut, dann möchten sie sich ihm zum Ausgleich ebenfalls positiv und hilfreich zeigen. Bei diesem Gegengefallen fließen oft Insiderinformationen zum Angreifer.

SOZIALE BEWÄHRTHEIT: DER EINZELNE STELLT SICH SELTEN GEGEN EINE ECHTE ODER VERMEINTLICHE MEHRHEIT

Foto: artibeau.de

Foto: redensarten.net

EINE LÖSUNGSMÖGLICHKEIT FÜR DEN UMGANG MIT DER ZUNEHMENDEN KOGNITIVEN BELASTUNG

Commitment & Konsistenz

„Wer A sagt, muss auch B sagen". Menschen haben den Drang nach konsistentem Verhalten, Einstellungen und tatsächliches Verhalten sollen kongruent sein. Ein Angreifer versucht, mit einem Menschen ein Commitment (eine Handlungsverpflichtung) einzugehen. Diese Handlungsverpflichtung ist im Hintergrund ein Vorteil für den Angreifer. Bekommt der Angreifer dieses Commitment, wird der Angegriffene im Nachgang bestrebt sein, sich konsistent zu seiner Entscheidung zu zeigen. Widersprüche oder Auffälligkeiten werden dann vom Angegriffenen oft verdrängt.

Soziale Bewährtheit

„Eine Million Hausfrauen kann sich nicht irren." Soziale Bewährtheit wird verwendet, um den Angegriffenen argumentativ von einem Sachverhalt zu überzeugen. Es wird zum Beispiel suggeriert, dass eine Menge von Fürsprechern belastbares Indiz für die Richtigkeit einer Sache sei. Diese Methode ist erfolgreich, da sich der Einzelne selten gegen eine echte oder vermeintliche Mehrheit zu stellen wagt.

Sympathie

Menschen haben eine Affinität zu Menschen, die sie mögen oder die ihnen ähnlich sind. Aus diesem Grunde lassen sich Angegriffene leichter von Menschen lenken und beeinflussen, die sie mögen. Zum Beispiel kaufen Menschen gerade fragwürdige Produkte eher von Menschen, die ihnen ähnlich oder sympathisch sind.

Autorität

Soziale Positionierung, die einer Institution oder einer Person zugeschrieben wird. Menschen richten sich in ihrem Denken und Handeln oft nach einer solchen Positionierung. Angreifer versuchen mit Autoritätsattributen in einem konstruierten Kontext (z.B. Regierung, Behörde, Organisation, Hierarchie, akademischer Grad, Chef, Titel, Uniform, usw.) bei einem anderen Menschen Unterwürfigkeit zu erzeugen. Zum Beispiel werden mit dieser Methode Anweisungen einer autoritär auftretenden Person (der Angreifer) oft ausgeführt, ohne den Hintergrund des Angreifers zu überprüfen.

Foto: kostenlos-fotos.de

WACHSAMKEIT AUCH INNERHALB DES UNTERNEHMENS IST UNUMGÄNGLICH

Knappheit

Limitierte Verfügbarkeit löst Impuls der Attraktivität aus. Mit künstlicher Verknappung werden Anreize geschaffen, die einen anderen Menschen befürchten lassen, dass zu einem späteren Zeitpunkt eine Gegebenheit nicht mehr verfügbar sei. Ein Angreifer möchte zum Beispiel den Impuls des Handelns oder des Ausführens bei einem anderen Menschen umgehend auslösen.

Wirkungen des Social Engineering

Da die oben geschilderten sozialen Heuristiken unbewusst und auch ungewollt ablaufen und von fast allen Menschen (außer, sie sind gegen solche Angreifer geschult) nicht erkannt werden, ist Social Engineering eine sehr effektive und gefährliche Waffe für die Manipulation von Menschen.

Der Erfolg von Human-Based Social Engineering wird durch unsere immer schneller werdende Gesellschaft begünstigt. Das Leben in unserer heutigen Zeit unterscheidet sich nennenswert von der Zeit vor etwa zehn Jahren. Der enorme technische Fortschritt sorgt dafür, dass Informationen, Wissen, Prozesse und Entscheidungen explosionsartig zunehmen und sogar zunehmen müssen. Diese Veränderung führt zu einer Beschleunigung unserer Tagesabläufe, ob privat oder geschäftlich. Unsere kognitive Überbeanspruchung führt dazu, dass die Entscheidungsfindung im Schnellverfahren durchgeführt wird. Es bleibt wenig Zeit sich über Sachverhalte und Hintergründe zu informieren oder sie zu objektivieren. Aus diesem Grunde haben es Angreifer immer leichter, Menschen zu schnellen Entscheidungen und Handlungen zu veranlassen.

Für viele Organisationen und die Unternehmen der Wirtschaft stellt diese Entwicklung und das Social Engineering eine enorme Bedrohung dar. Umso wichtiger wird es sein, in den Organisationen und den Unternehmen Sicherheitsprozesse und Trainingsprogramme aufzusetzen, um das Risiko des ungewollten Informationsabflusses über das Human-Based Social Engineering zu reduzieren. ■