

Interne Spionageabwehr

Organisationen, die Mitarbeiter zur Abwehr von Industrie- und Wirtschaftsspionage befähigen wollen, kommen nicht mit vorrangig IT-bezogenen Awareness-Kampagnen aus. Sie müssen die Schulungen um den Aspekt Social Engineering ergänzen und zusätzliche organisatorische Massnahmen ergreifen, darunter die Einrichtung eines interdisziplinären Security-Helpdesks.



Bettina Wesselmann

ist freie Journalistin und Beraterin für Informationssicherheit mit den Spezialgebieten internationale Sicherheitskulturen und Social Engineering. Sie publizierte den Beitrag im März 2011 im Auftrag der KES.

Awareness-Kampagnen, die Mitarbeiter für Risiken in der Informationsverarbeitung sensibilisieren sollen, konzentrieren sich meist nur auf den richtigen Umgang mit technischen Kommunikationsmitteln wie E-Mail und Web. Schulungen, die sich auf das nichttechnische Kommunikationsverhalten beziehen – etwa in Kundengesprächen, in Chat-Rooms, am Telefon oder in sozialen Netzwerken – findet man deutlich seltener. Genau diesen Bereich müssen aber Unternehmen angehen, die Mitarbeiter gezielt auch für die Abwehr von Wirtschafts- und Industriespionage wappnen wollen. Spione versuchen nämlich Informationen nicht nur auf technischen Wegen, sondern auch durch das direkte Ausforschen von Mitarbeitern (sowie Dienstleistern, Kunden und anderen Menschen) zu erlangen. Gegen solche "Blended Threats" verfügen noch nicht viele Firmen über tragfähige Konzepte.

Mitarbeiter als Sensoren

Im Rahmen einer Abwehrstrategie gegen Industrie- und Wirtschaftsspionage ist es aus gleich zwei Gründen besonders sinnvoll, die Mitarbeiter einzubeziehen: Erstens ist die Ab-

wehr ausgefeilter technischer Angriffe auf diesem Gebiet – beispielsweise mit Abhörtechnik – nur mithilfe von Spezialisten und spezieller Ausrüstung zu bewältigen, was Gegenmassnahmen in Eigenregie erschwert. Aufmerksame Mitarbeiter können aber als "Sensoren" mit etwas Glück schon im Vorfeld verhindern, dass beispielsweise "Wanzen" überhaupt ins eigene Haus gelangen.

Zweitens sind die kombinierten Angriffsschritte professioneller Spione jeder für sich oft so unscheinbar, dass sie unter dem Radar der Sicherheitsspezialisten und der technischen Sensoren für IT-, Gebäude- und Personensicherheit bleiben: ein kleiner Hacking-Versuch hier, ein vermeintlich harmloser Anruf und die eine oder andere E-Mail dort, ein "Gedankenaustausch" in der S-Bahn und einer auf dem Golfplatz und dann noch ein Hausbesuch in der Maske eines Wartungsdienstleisters. Nur wenn aufmerksame Mitarbeiter routinemässig "Seltsames" melden, fügen sich solche Bausteine vielleicht zu einem alarmierenden Gesamt-Bild zusammen. Damit dies gelingt, muss jedoch eine Reihe von Voraussetzungen erfüllt sein:

- eine Unternehmensethik, die auch das Ziel "Informationsschutz" erfasst,
- eine effiziente Zusammenarbeit der Sicherheitsabteilungen,
- ein Helpdesk für Verdachtsfälle und
- die Vermittlung von Social-Engineering-Grundwissen an Führungskräfte und Mitarbeiter.

Der erste Punkt mag überraschen, ist aber durch Studien belegt (vgl. [1] S. 46f und [2]): In Unternehmen, in denen akzeptierte ethische Grundsätze für das Handeln als Organisation existieren, engagieren sich Mitarbeiter eher für die Sicherheit als in Firmen, in denen entsprechende Leitlinien fehlen. Dies ist nachvollziehbar, wenn man sich die Situation innovativer "Garagenfirmen" ins Gedächtnis ruft: Apple galt etwa in seiner Frühzeit als Standardbeispiel für ein Unternehmen, in dem die Mitarbeiter so sehr hinter "ihren" Produkten und "ihrer" Technik standen, dass kaum einmal Informationen über Neuentwicklungen verfrüht an die Öffentlichkeit drangen. In grossen, anonymen Organisationen bietet die Einführung einer zustimmungsfähigen Unternehmensethik – und damit einer gemeinsamen Handlungsbasis – offenbar die Möglichkeit, wenigstens ein Minimum des entsprechenden Zusammenhalts herzustellen.

Der zweite Punkt in der Liste ist ein Desiderat, das nicht überall leicht einzulösen ist: Spezialisten für Objekt- und Personenschutz auf der einen sowie IT- und Informationssicherheit auf der anderen Seite kommen oft aus so unterschiedlichen Kulturen, dass ihre Kommunikation echter Anstrengung bedarf (vgl. [3]). Gelingt das

allerdings, dann ist der dritte Punkt, die Einrichtung eines übergreifenden Security-Helpdesks für Mitarbeiter, nur noch ein organisatorisches Problem. In deutschen Unternehmen übernimmt diese Aufgabe zuweilen sehr erfolgreich der zentrale Datenschutzbeauftragte.

Es bleibt der vierte Aspekt, die Verwandlung der Mitarbeiter in "Sensoren": Das Aufspüren kleiner Unregelmässigkeiten, wie sie die Anwesenheit unangemeldeter Servicekräfte oder das gehäufte Auftreten ungewöhnlicher IT-Probleme darstellen, fällt Menschen gewöhnlich leicht. Mitarbeiter in ihrer Aufmerksamkeit für solche Ereignisse zu bestärken und die Hemmschwelle für Rückfragen zu senken, ist ebenfalls relativ einfach: Es gilt dazu das Bewusstsein zu schärfen, dass hinter Unregelmässigkeiten möglicherweise Tricks und Gefahren stecken, die sich durch das Engagement der Belegschaft verhindern oder reduzieren lassen. Hierzu müssen die Mitarbeiter natürlich wissen, wo sie bei entsprechenden Beobachtungen Gehör finden: Die Einrichtung der schon erwähnten "Hotline" für alle Sicherheitsfragen und die Ermutigung, dort lieber einmal zu viel als zu wenig um Rat zu fragen, fördern bereits recht effektiv das richtige Verhalten.

Entscheidungsfallen erkennen

Schwieriger ist der Umgang mit Fällen, bei denen Mitarbeiter durch Industrie- und Wirtschaftsspione direkt angegangen werden, um den Angreifern unberechtigt Zugang zu Informationen zu gewähren.

Das Mittel der Wahl ist hierbei die zwischenmenschliche Manipulation des Verhaltens, sprich: Social Engineering. Typisch dafür ist ein Vorgehen, das Menschen in einen so genannten heuristischen Entscheidungsmodus versetzt.

Mit "Heuristiken" im psychologischen Sinn verbindet man den automatischen Rückgriff eines Menschen auf bewährte Standardmodelle der Entscheidungsfindung, wenn in hektischen oder unübersichtlichen Situationen die Basis für analytisches Vorgehen fehlt. Diese Lösungswege sind im Menschen evolutionär fest angelegt oder beruhen auf sozialer Erfahrung (vgl. [4]).

Was dies bedeutet, lässt sich an einem häufig diskutierten Beispiel des Social Engineerings zeigen: Eine Person ruft einen Sachbearbeiter in einem Unternehmen an, der Zugang zu sensiblen Informationen hat. Der Angreifer behauptet, ein Vorgesetzter aus einer anderen Niederlassung zu sein, und gibt vor, bestimmte Daten sofort zu benötigen, um Schaden vom Unternehmen abzuwenden. Seine Berechtigung belegt er, indem er auf einen direkten Vorgesetzten des Opfers verweist – von dem er weiss, dass dieser zum fraglichen Zeitpunkt nicht zu erreichen ist.

In diesem Fall verhindert der Zeitdruck, dass das Opfer die Lage kühl abwägt und die Berechtigung der Anfrage überprüft. Stattdessen setzen zwei Heuristiken ein, und zwar eine "soziale" und eine "kognitive": Die erste besteht in der Tendenz, im Zweifelsfall lieber einer Autorität zu gehorchen als sie infrage zu stellen, die zweite im Wunsch, die am leichtesten zu bewältigende Handlung – mit

Informationen zu helfen – vorzuziehen, zumal sie häufig der eigenen Aufgabe entspricht. So ist die Wahrscheinlichkeit hoch, dass der Mitarbeiter im beschriebenen Szenario Informationen weitergibt. Das Unangenehme der Situation und die mögliche Sorge, vielleicht doch einen Fehler begangen zu haben, verhindern ausserdem recht effektiv, dass er den Vorfall später meldet.

Es gibt viele Heuristiken, die für Social Engineers nützlich sind. Nicht alle treten als Reaktionen auf Druck in Erscheinung; auch eine dringende Bitte um Hilfe oder der Aufbau einer Sympathiebeziehung verleiten Menschen dazu, zu vorprogrammierten Handlungsschemata überzugehen. Gerade am Beispiel der Hilfsbereitschaft zeigt sich, dass heuristisches Vorgehen an sich kein Fehler ist, denn in den meisten heiklen Situationen des Alltags ist es sinnvoll und ein wichtiger Bestandteil sozialen Lebens. Mitarbeiter zum Schutz gegen Beeinflussung lediglich dazu anzuhalten, heuristisches Vorgehen unter allen Umständen zu vermeiden und grundsätzlich analytisch vorzugehen, ist allein aus diesem Grunde zum Scheitern verurteilt. Hinzu kommt, dass Social Engineers als Angreifer die Chance haben, immer neue manipulative Szenarien zu entwickeln, auf die sich die Opfer nicht allesamt einstellen können.

Der Nutzen des "mulmigen Gefühls"

Ein Effekt allerdings ist in jedem Social-Engineering-Fall gleich: Irgendwann muss ein Manipulator mit Spionageabsichten sein Opfer zu einer Regelübertretung

bewegen oder es überreden, Sicherheitsbedenken ausser Acht zu lassen, um an sensitive Informationen zu gelangen. Spätestens an diesem Punkt entsteht beim Opfer fast unweigerlich ein "mulmiges Gefühl": Es befindet sich in einem Zwiespalt zwischen dem Wunsch, formal richtig zu handeln, und der verlockenden Alternative beim "programmierten" heuristischen Handlungsmodell zu bleiben.

Bei dieser Unsicherheit müssen Sensibilisierungsmassnahmen gegen Social Engineering ansetzen: Mitarbeiter müssen lernen, wie Social Engineers vorgehen, wie und wann Heuristiken eine Rolle spielen und dass das beschriebene Unbehagen – "hier stimmt etwas nicht" – ein ernst zu nehmendes Warnsignal ist. Je genauer die Mitarbeiter wissen, dass und wo für Spione interessante Informationen im Unternehmen vorhanden sind, desto treffsicherer reagieren sie auf die relevanten Situationen. Auf Interesse stossen Wissensvermittlung und Trainings gegen Social Engineering übrigens fast immer, denn einer Manipulation seines eigenen Handelns möchte jeder Mensch etwas entgegensetzen können.

Wenn ein Mitarbeiter trotz Trainings in einer Social-Engineering-Situation nicht weiter weiss, spielt wiederum der bereits geforderte Security-Helpdesk eine wichtige Rolle: Wird er auch dann als vertrauenswürdige Adresse für Rückfragen akzeptiert, erhöht sich für die Sicherheitsabteilungen signifikant die Wahrscheinlichkeit, von Spionageaktivitäten zu erfahren und rechtzeitig eingreifen zu können.

Literatur

[1]

Pricewaterhouse Coopers, Wirtschaftskriminalität 2007, Sicherheitslage der deutschen Wirtschaft, *nicht mehr verfügbar*

[2]

Bettina Palazzo, Unternehmensethik als Instrument der Prävention von Wirtschaftskriminalität und Korruption, Die Kriminalprävention 2/2001, S. 52

[3]

Bettina Weßelmann, Gemeinsam gegen gezielte Attacken, IT: Abwehr von Social Engineering, Sicherheitsforum 5/2007, S. 55,

www.mediasec.ch/mod_pdfbit/index.asp?cat=SicherheitsForum&mag=2007-5&page=57

[4]

Robert Cialdini, Die Psychologie des Überzeugens, Huber Vlg., 2009, ISBN 978-3-456-84834-1