



Bond lässt grüßen

Das Spionagegeschäft boomt: Das Wissen um Informationen ist ein strategischer Wettbewerbsvorteil. Um sich vor der Mitnahme wertvoller Daten aus der Entwicklung oder vor einem geschäftsschädigenden Imageverlust zu schützen, sollte man zunächst wissen, wo und wie Gefahr droht. Es kann auch sinnvoll sein, mit Hilfe externer Berater Spionageangriffe zu simulieren.

Andreas Schnitzer, Michael Hochenrieder

Es ist kein Phänomen der modernen Welt: Einer der ersten Fälle von Industriespionage wurde bereits im 6. Jahrhundert nach Christus aktenkundig. Der römische Kaiser Justinian schickte seine Leute nach China, um das Geheimnis der Seidenherstellung zu erkunden.

Viele Jahrhunderte später wurde ein deutsches Unternehmen, das führend in der Technologie für Windkraftanlagen war, offensichtlich Opfer der Spionage eines Konkurrenz-Unternehmens aus den USA. Die Amerikaner waren dadurch schneller bei der Patentanmeldung und verboten den Deutschen den Vertrieb ihrer „eigenen“ Anlagen.

Industriespionage fand zu jeder Zeit statt und hat durch die Einführung moderner Technologien – fast alle Informationen werden heute digital gespeichert – einen zusätzlichen Auftrieb erhalten. Daher wird sie auch permanent in den Medien behandelt. Dennoch ist die Thematik zu vielen potenziell betroffenen Firmen noch nicht durchgedrungen. Zwar werden inzwischen bei Unternehmen, die schon angegriffen wurden und dadurch Verluste erlitten, entsprechende vorbeugende Maßnahmen eingesetzt. Bei Firmen, die durch Industriespionage bis dato keinen offensichtlichen Verlust erlitten haben, ist die notwendige Sensibilisierung jedoch noch nicht im notwendigen Maß vorhanden.

Der Schwerpunkt eines Spionageangriffes liegt meist auf dem Ziel „Mensch“ als schwächstem Glied in der

Sicherheitskette. Viele Unternehmen haben in den letzten Jahren in Sachen Technologie aufgerüstet. Doch jede Firewall, jeder Virens Scanner und jede noch so gute physische Sicherheit versagen, wenn ein Mitarbeiter abends in der Kneipe gesprächig wird oder auf Community-Plattformen im Internet private und arbeitsrelevante Informationen offen darlegt.

Mittels solcher sozialen Kontakte, Social Engineering genannt, gelangen Spione an vertrauliche Informationen. Kevin Mitnick, ehemaliger verurteilter Hacker und heute Sicherheitsberater, hat in seinem Buch „Die Kunst der Täuschung“ die Methoden des Social Engineering eindrucksvoll beschrieben. Es basiert auf der Manipulation des Opfers (ohne dessen Wissen) durch Anwendung psychologischer Tricks, aber immer ohne den Einsatz von Gewalt (wie zum Beispiel Erpressung).

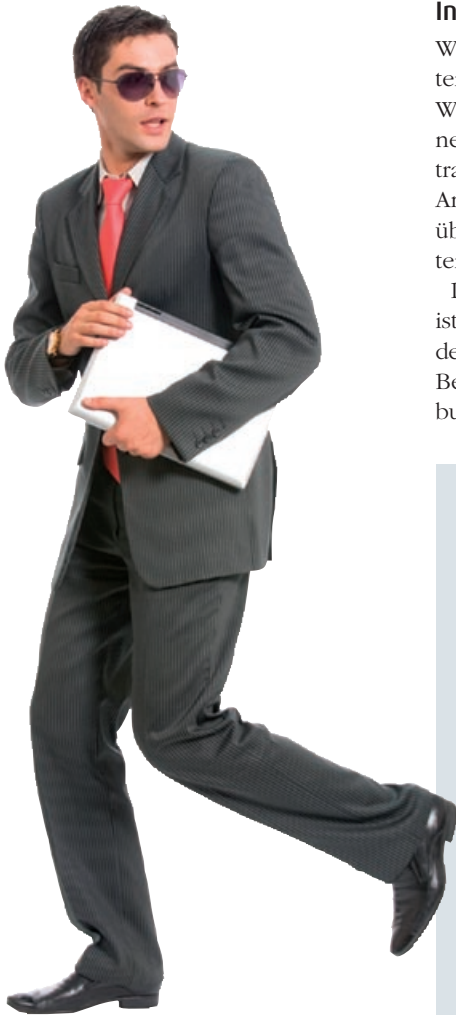
Bei der Art des Angriffs unterscheidet man zwischen Human-Based und Tool-Based Social Engineering:

➤ Human-Based Social Engineering ist die Informationsbeschaffung ohne Einsatz von Hilfsmitteln. Der Social Engineer wendet hier vor allem psychologische Methoden wie Schuldgefühle erzeugen, Fachchinesisch, Lockmittel, Hilfsbedürftigkeit oder Autorität/Druck an. Das kann in persönlichen Gesprächen oder am Telefon geschehen.

➤ Bei der Variante Tool-Based Social Engineering werden Hilfsmittel wie Trojaner, versteckte Kameras oder Keylog-

Wirtschaftsspionage vs. Industriespionage

Wirtschaftsspionage ist staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. Industriespionage ist die Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt (Definition des Bundesamtes für Verfassungsschutz). Da auch Wirtschaftsspionage durch Staaten meist zum Vorteil von „landeseigenen“ Unternehmen durchgeführt wird, ist das Ergebnis für das angegriffene Unternehmen in beiden Fällen vergleichbar.



ger zum Aufzeichnen von Tastatureingaben eingesetzt.

Psychologisches Know-how, das Wissen um die richtigen Tools, gute kommunikative Fähigkeiten, schauspielerisches Talent und nicht zuletzt eine gehörige Portion Chuzpe sind die Zutaten eines guten Social Engineers, wenn er einen simulierten Angriff startet.

Ein Angriff erfolgt typischerweise in drei Phasen:

- > Phase 1: gezielte Informationsrecherche
- > Phase 2: Zutritt und Zugang
- > Phase 3: Informationsdiebstahl

Phase 1: Gezielte Informationsrecherche

Wie „funktioniert“ das ausspionierte Unternehmen? Wer sind die Zielpersonen? Wie kann ich mit diesen Kontakt aufnehmen? Wie kann ich mit diesen vertraut werden? In der ersten Phase des Angriffs informiert sich der Spion gezielt über sein Ziel und wie er an die benötigten Informationen gelangen kann.

Die beste und erste Informationsquelle ist das Internet. Was steht auf den Seiten des Unternehmens selbst? Kann man zum Beispiel anhand von Stellenausschreibungen nähere Informationen erhalten?

Sucht das Unternehmen vielleicht gerade einen Mitarbeiter, den man einschleusen könnte? Auf welchen anderen Websites taucht das Unternehmen noch auf? Ist es Mitglied in einem Verband? Schreiben Mitarbeiter des Unternehmens Beiträge in Newsgroups oder Blogs?

Sobald man das „Gebilde“ Unternehmen verstanden hat, geht es darum, Zielpersonen ausfindig zu machen, diese zu kontaktieren und ihr Vertrauen zu gewinnen. Auch hier hilft entscheidend das Internet. Auf Business Networks wie *Xing* oder *LinkedIn*, die sich dem Knüpfen und der Pflege sozialer Kontakte verschrieben haben, geben die Mitglieder bereitwillig teilweise auch vertrauliche Informationen preis. So zeigt eine Studie des Security-Anbieters McAfee, dass für Passwörter häufig Namen oder Daten verwendet werden, die auch auf den Online-Plattformen hinterlegt sind. Spione nutzen dieses Wissen, um mit Social Networking das nötige Vertrauen zu schaffen, um an wichtige Firmendaten heranzukommen.

Phase 2: Zutritt und Zugang

Mit den aus Phase 1 gewonnenen Informationen versucht der Spion nun, in das Unternehmen einzudringen. Viele Unternehmen bieten zum Beispiel Be-

Checkliste gegen Industriespionage

- Unternehmensweite Sicherheit ist eine Aufgabe der Geschäftsleitung. Beauftragen Sie einen Sicherheitsverantwortlichen in entsprechender Stellung.
- Führen sie allgemeingültige unternehmensweite Sicherheitsrichtlinien ein.
- Definieren Sie die relevanten Prozesse und dokumentieren Sie diese. Orientieren Sie sich dabei an allgemein gültigen Sicherheitsstandards wie ISO 27001.
- Überprüfen Sie regelmäßig die Einhaltung der Richtlinien und Prozesse.
- Dokumentieren Sie die gefundenen Schwachstellen und leiten Sie Handlungen daraus ab.
- Sensibilisieren und motivieren Sie Ihre Mitarbeiter für das Thema Sicherheit – und das fortlaufend. Menschen „vergessen“ Erlerntes. Um ein sicherheitsbewusstes Verhalten zu garantieren, ist eine stetige Sensibilisierung notwendig.
- Eine funktionierende IT- und physische Sicherheit ist Voraussetzung für die Abwehr von Industriespionage. Aber denken Sie daran: Je ausgereifter die technische Sicherheit, desto einfacher kann Social Engineering sein.
- Nutzen Sie gegebenenfalls das spezielle Know-how externer Experten (gegen Betriebsblindheit).
- Sicherheit ist kein einmaliger, sondern ein laufender Prozess – und heute so wichtig wie morgen.

suchstage für Ortsansässige an: eine erste Gelegenheit, um das Unternehmen auch von innen kennenzulernen. Mit dem nötigen Background tritt der Spion als potenzieller Kunde auf oder versucht, als Techniker für Drucker und Kopiergeräte Zutritt zu den Geschäftsräumen zu erhalten.

Einen anderen Weg ging vor kurzem China, um ein Technologie-Unternehmen in Hamburg auszuspionieren: Als Praktikanten in die Firma eingeschleuste chinesische Studenten kopierten vor Ort alle Daten, die ihnen in die Hände fielen; wegen ihrer fehlenden Deutschkenntnisse konnten sie allerdings nicht einschätzen, welche Informationen wirklich wichtig waren.

Spione nehmen auch gern den einfachen Weg. Am Tage höflich lächelnd am Empfang vorbei oder abends wild gestikulierend im schwarzen Anzug mit Krawatte bitten sie die Putzkraft um Einlass: „Alle Server sind abgestürzt, ich musste gerade diese Abendveranstaltung verlassen und jetzt funktioniert auch noch mein Firmenausweis nicht.“ Schon ist man drin.

Phase 3: Informationsdiebstahl

Ist der Spion erst einmal im Firmengebäude, beginnt Phase 3, der eigentliche

Diebstahl von Informationen. Das geschieht meist durch das Entwenden materieller und immaterieller Gegenstände. Der Spion betritt unverschlossene Büros oder Archivräume und durchforstet Schreibtische, Ablagen und Schränke. Er wühlt in Papierkörben neben Kopierern und Druckern nach „Fehlkopien“ vertraulicher Informationen und durchsucht Abfalltonnen nach brauchbarem Material – „Dumpster Diving“ heißt das in der Fachsprache des Social Engineers.

Findet der Spion die benötigten Informationen nicht, entwendet er Geräte, auf denen Informationen gespeichert sein könnten wie Laptops, BlackBerrys und PDAs. Diese Geräte durchsucht er nach Daten oder benutzt sie, um auf größere zentrale Speichersysteme (Netzlaufwerke) Zugriff zu erhalten. Im günstigsten Fall gelingt es dem Spion nach Nutzung des Gerätes, dies an seinen ursprünglichen Platz zurückzubringen, ohne dass der Besitzer vom Missbrauch erfährt.

Vorsicht, Kantine!

In größeren Unternehmen bieten sich öffentliche Orte wie Kantinen an, um Kontakt zu Mitarbeitern aufzunehmen und sie in „harmlose“ Gespräche zu verwickeln. Das persönliche Gespräch



Die physische (Gebäude-)Sicherheit ist eine wichtige Komponente zum Schutz vor Industriespionen. Doch die beste Technik hilft nichts, wenn es am Sicherheitsbewusstsein der einzelnen Mitarbeiter mangelt.

Security-Awareness-Kampagne

Eine Security-Awareness-Kampagne umfasst in der Regel mehrere Phasen, die der Information, Emotionalisierung und Motivation dienen, um so das Verhalten der Mitarbeiter bezüglich Sicherheit zu verändern. Zuerst wird das Interesse der Mitarbeiter für das Thema Informationssicherheit geweckt, zum Beispiel mit Postern oder Ausstellern.

Den Schwerpunkt bildet Phase 2, in der den Mitarbeitern in Präsenz- oder alternativ in Online-Schulungen das Wissen zur Informationssicherheit vermittelt wird. Große Bedeutung bei den Trainings hat die direkte und nachvollziehbare Darstellung der Gefahren durch Live-Demonstrationen (zum Beispiel Spam verschicken, Wirkung eines Trojaners zeigen) oder durch den Einsatz multimedialer Elemente wie Videos. Gesehenes wird oft besser erinnert als nur Gehörtes.

Gerade die Social-Engineering-Methoden eines Industriespions können in nachgestellten Szenen effektiv verbildlicht werden. Beispielsweise wird so veranschaulicht, wie die guten menschlichen Eigenschaften Hilfsbereitschaft und Freundlichkeit durch einen Angreifer gezielt ausgenutzt werden. Kennen die Mitarbeiter die Vorgehensweise eines Industriespions, sind sie später in der Lage, den Unterschied zwischen reiner Freundlichkeit und einem Angriffsversuch zu erkennen.

Phase 3 einer Kampagne dient der Nachhaltigkeit, damit Sicherheit nicht nur nach den Trainings verstanden, sondern anschließend auch gelebt wird. Hier können Elemente wie Security-Bildschirmschoner oder Give-Aways eingesetzt werden. Da einmal Gelerntes leider auch wieder vergessen wird, sollten die Maßnahmen einer Kampagne durch alle Phasen hindurch stetig wiederholt werden, um die Einstellung der Mitarbeiter zeitstabil nachhaltig zu verändern.



Klassische Angriffsmethoden ergänzen sich mit modernster Technik.



So rabiät gehen Industriespione nur höchst selten vor. Das haben sie auch gar nicht nötig, denn Social Engineering ist nicht nur diffiziler, sondern verspricht meist auch mehr Erfolg.

steht auch bei der Königsdisziplin des Social Engineerings im Mittelpunkt: dem Abgreifen vertraulicher Informationen am Telefon. Von einem internen Telefonapparat aus kontaktiert der Spion die Zielperson und gibt sich zum Beispiel als Mitarbeiter der IT aus.

Mit viel Fachchinesisch wird der Angerufene verwirrt: „Hallo, hier ist Herr Meier vom IT-HelpDesk. Wir haben wegen Ihnen ein großes Problem in unserem Netzwerk. Ihr Rechner sendet permanent SYN-Pakete ohne ACK-Bit an unser Default-Gateway. Wenn das noch zehn Minuten so weiter geht, wird unser zentraler Core-Backbone-Router aufgrund der Denial-of-Service-Attacke automatisch rebooten und kein Mitarbeiter wird mehr arbeiten können.“

Dann bittet der Spion die Zielperson um Mithilfe bei der Lösung des Problems. Nachdem mehrere Versuche nicht funktioniert haben, wird der User aufgefordert, sein Passwort dem vermeintlichen IT-Mitarbeiter mitzuteilen, und in 80 Prozent der Fälle erhält der Spion es auch.

Ist der geschilderte Fall, ein reines Human-Based Social Engineering, erfolgreich, ergibt sich auch vor Ort die Möglichkeit des Tool-Based-Vorgehens. Man kann zum Beispiel Keylogger an PCs anbringen, um Daten abzugreifen, oder mit Hilfe von USB-Sticks Trojaner einschleusen und in der Folge die IT-Systeme kontrollieren.

Die Möglichkeiten eines Industriespions sind vielfältig; deshalb ist es für betroffene Unternehmen schwierig, sich dagegen zu wappnen. Ein Security Assessment mit Social-Engineering-Komponente kann ein erster wichtiger Schritt

sein, Schwachstellen in der Unternehmenssicherheit aufzudecken. Die anschließende Dokumentation ist Basis für den Auf- und Ausbau eines Information Security Managements.

Schutzmaßnahmen

Leider gibt es für die Erkennung von Angriffsversuchen speziell im Bereich des Social Engineering kein Patentrezept. Jedes Unternehmen hat seine Eigenarten und Besonderheiten. Genauso, wie ein Social Engineer sich darauf einstellen muss, müssen auch die Schutzmaßnahmen eines Unternehmens individuell gestaltet werden.

Wichtig: Technik allein hilft nicht! Eine funktionierende IT- und physische Sicherheit sind Voraussetzung für eine Abwehr, können aber auch das Gegenteil bewirken. Verlassen sich die Mitarbeiter auf die Technik, hat es ein Spion, der Social-Engineering-Methoden einsetzt, meist noch einfacher: „Da wird doch viel Geld für Technik ausgegeben – die sollte doch funktionieren. Ich bin ja nur ein kleiner Anwender.“

An erster Stelle steht daher die Sensibilisierung der Mitarbeiter. Da der Social Engineer technische Schutzeinrichtungen geschickt umgeht und sich auf das schwächste Glied in der Sicherheitskette – den Menschen – konzentriert, kann man sich primär nur durch das Schaffen eines Sicherheitsbewusstseins vor Angriffen schützen.

Viele Menschen sind hilfsbereit und freundlich – und genau das ist das Problem. Ziel muss es sein, den Mitarbeitern das Problem vorzustellen und die Vorgehensweisen zu erklären. Nur so ist es möglich, dass Mitarbeiter den Unter-



Industriespionage wird es oft sehr leicht gemacht, Firmendaten zu stehlen. <

schied zwischen reiner Freundlichkeit und einem Angriffsversuch oder zwischen Smalltalk und Aushorchen erkennen können.

Um das angesprochene Sicherheitsbewusstsein bei den Mitarbeitern zu etablieren, kann eine Security-Awareness-Kampagne hilfreich sein. Sie enthält verschiedene Elemente zur Information, Sensibilisierung und Motivation der Mitarbeiter für dieses Thema. Im Mittelpunkt stehen dabei Schulungsmaßnahmen – soweit möglich sollte das in Präsenztrainings geschehen (anderenfalls auch zum Beispiel mit Online-Trainings). Die Maßnahmen der Kampagne müssen stetig wiederholt werden, um die Einstellung der Mitarbeiter nachhaltig zu verändern.

Security Assessment

Die Sensibilisierung der Mitarbeiter ist eingebettet in die Einführung von unternehmensweiten Sicherheitsmaßnahmen. Dazu zählen die Einführung von Sicherheitsrichtlinien, die Optimierung aller sicherheitsrelevanten Prozesse, die Dokumentation der Prozesse, die regelmäßige Durchführung und Dokumentation von Security Audits, die Optimierung der physischen Sicherheit, Regelungen für den Katastrophenfall und weitere auf das jeweilige Unternehmen individuell abgestimmte Maßnahmen. Verantwortlich für diese Maßnahmen ist der Sicherheitsbeauftragte. Er überwacht auch deren Einhaltung.

Um die Effizienz der Maßnahmen zu steigern, können Unternehmen einen externen Dienstleister ins Boot holen. Dieser muss – wie jeder andere Dienstleister auch – im Hinblick auf Vertrauens-

würdigkeit und Referenzen überprüft werden. Der externe Dienstleister verfügt oft nicht nur über das größere Know-how, sondern in der Regel auch über Erfahrungen aus anderen Projekten, was einerseits einer möglichen Betriebsblindheit entgegenwirkt und andererseits Vergleichs- oder sogar Benchmarking-Möglichkeiten schafft, die wiederum der Qualität der einzelnen Maßnahmen ebenso wie der Gesamtarchitektur zugute kommen. Sicherheitsbewusste Unternehmen schaffen sich so einen deutlichen Wettbewerbsvorteil.

Fazit

Industriespionage stellt für viele Unternehmen ein reales Gefahrenpotenzial dar, das die meisten Betriebe und deren Management aber noch immer unterschätzen. Viele Manager sind sich der Bedeutung des eigenen Unternehmens und der unternehmensinternen Informationen nicht bewusst. Aber nicht nur große multinationale Konzerne, auch Mittelständler sind heute oft „Global Player“ und innovative Marktführer und wecken so das Interesse der Konkurrenz. Es lohnt sich also, über Sicherheit nachzudenken.

Vorsorgemaßnahmen zur Abwehr von Industriespionage-Angriffen stellen zu meist eine Art Versicherung dar, die oft als „unnütze“ Ausgabe angesehen wird, solange es zu keinem Schaden kommt. Doch Unternehmen dürfen nicht warten, bis es zum Schadensfall kommt. Vielmehr sollten sie wachsam bleiben, die richtigen Vorkehrungen treffen und ihre Mitarbeiter sensibilisieren, um Angriffe rechtzeitig zu erkennen und abzuwehren.

[rm]

Die Autoren dieses Beitrags, Andreas Schnitzer und Michael Hochenrieder, sind Consultants beim auf Business Security und Business Development spezialisierten Beratungsunternehmen HvS-Consulting in München. <