

Andreas Schnitzer, Michael Hochenrieder

Anatomie eines Industriespionage-Angriffs (I)

Sind die Angreifer wieder weg, dann sind auch wertvolle Daten aus der Entwicklungsabteilung verschwunden, die Öffentlichkeit kennt firmeninterne Details, die einen enormen Imageverlust bedeuten, und unter Umständen ist die Zukunft des Unternehmens gefährdet. Das Geschäft der Industriespione boomt, das Wissen um vertrauliche Informationen ist längst ein strategischer Wettbewerbsvorteil. Um sich vor solchen Attacken zu schützen, simulieren namhafte Unternehmen mit Hilfe externer Berater bei so genannten Security Assessments einschlägige Spionageangriffe.

Industriespionage¹ ist kein Phänomen der modernen Welt. Einer der ersten Fälle ist bereits im 6. Jahrhundert nach Christus aktenkundig geworden: Der römische Kaiser Justinian schickte Agenten nach China, um das Geheimnis der Seidenherstellung zu erfahren. Viele Jahrhunderte später wurde ein deutsches Unternehmen, das führend in der Technik für Windkraftanlagen war, offensichtlich Opfer der Spionage eines Konkurrenten aus den USA. Die Amerikaner konnten so schneller das Patent anmelden und verboten den Deutschen anschließend den Vertrieb ihrer eigenen Anlagen. Durch die Einführung der Computertechnik hat die Industriespionage in den vergangenen beiden Jahrzehnten einen zusätzlichen Auftrieb erhalten, da heute nahezu alle wichtigen Informationen digital gespeichert werden. Besonders spektakuläre Fälle werden auch in den Medien gern aufgegriffen. Die potenziellen Opfer dagegen scheint dies oft wenig zu kümmern: Unternehmen, die durch Industriespionage bis dato keine offensichtlichen Verluste erlitten haben, argumentieren häufig, ihre internen Informationen seien für die Konkurrenz ohnehin nicht interessant. Wer allerdings schon angegriffen wurde und Verluste erlitten hat, denkt ganz anders darüber.

An diesem Punkt setzen Beratungsunternehmen wie HvS-Consulting aus München an. Die Security-Spezialisten stellen immer wieder fest, dass die meisten Unternehmen, mit denen sie in Kontakt kommen, die Gefahren von Industriespionage vollkommen unterschätzen oder gar nicht kennen. Um diese aufzuzeigen, starten sie Projekte zur Information Security daher oft mit einem simulierten Industriespionage-Angriff im Rahmen eines Security Assessment. Die Berater verhalten sich dabei wie echte Spione: Sie verschaffen sich gezielt Informationen, versuchen, das Vertrauen Ihrer Opfer zu gewinnen, dringen illegal in Gebäude ein und hacken sich in IT-Systeme, um schließlich an die gewünschten Informationen zu gelangen.

Ziel der Angriffe ist dabei in der Regel der Mensch als schwächstes Glied in der Sicherheitskette. Mit gutem Grund: Zwar haben viele Unternehmen in den letzten Jahren in Sachen Sicherheitstechnik kräftig nachgerüstet. Doch

Die meisten Unternehmen kennen die Gefahren der Industriespionage entweder gar nicht oder unterschätzen sie erheblich

^[1] Als Industriespionage definiert das Bundesamt für Verfassungsschutz die Ausforschung eines Unternehmens durch einen direkten Konkurrenten. Im Gegensatz dazu bezeichnet der Terminus Wirtschaftsspionage die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. Die Unterscheidung mutet indes etwas akademisch an: Denn da auch die staatliche Wirtschaftsspionage meist zum Vorteil „landeseigener“ Unternehmen betrieben wird, ist das Ergebnis für die betroffenen Unternehmen letztlich das gleiche.

Industriespione nutzen i. d. R. sog. Social-Engineering-Techniken, attackieren also den Menschen als schwächstes Glied der Sicherheitskette

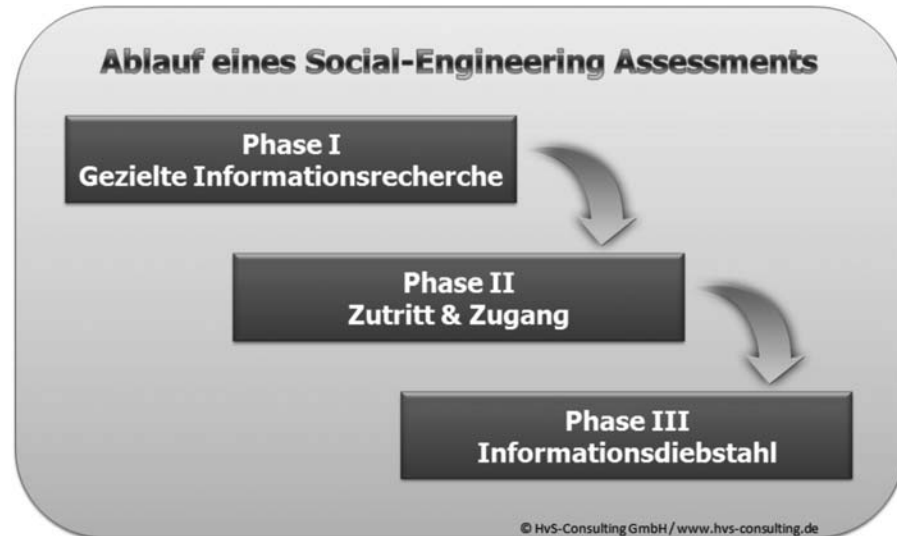
Zutrittskontrollen, Firewalls und Virens Scanner versagen zwangsläufig, wenn ein Mitarbeiter abends in der Kneipe gesprächig wird oder auf Community-Plattformen im Internet private und arbeitsrelevante Informationen offen darlegt. Genau durch solche sozialen Kontakte jedoch gelangen Spione an vertrauliche Informationen. Die Methode ist unter dem Namen *Social Engineering* bekannt. Kevin Mitnick, einst meistgesuchter Hacker der USA und heute Sicherheitsberater, hat sie in seinem Buch „Die Kunst der Täuschung“ eindrucksvoll beschrieben. Die Grundzüge des *Social Engineering* basieren auf einer Manipulation des Opfers durch psychologische Tricks, ohne dass dieses etwas ahnt oder gar weiß, und kommen immer ohne den Einsatz von Gewalt (wie z. B. Erpressung) aus.

Experten unterscheiden zwischen Human-Based und Tool-Based Social Engineering; jeder Angriff erfolgt in drei Phasen

Grundsätzlich unterscheidet man zwischen *Human-Based* und *Tool-Based Social Engineering*. Der erste Begriff bezeichnet die Informationsbeschaffung ohne Einsatz technischer Hilfsmittel: Der Angreifer appelliert z. B. an die Hilfsbereitschaft der vermeintlichen Kollegen und erzeugt so sanften Druck oder Schuldgefühle oder er gibt sich als Mitarbeiter der IT-Abteilung aus und wickelt sein Opfer mit einem Gemisch aus Fachchinesisch und vorge-täuschter Autorität ein. Das kann sowohl in persönlichen Gesprächen als auch am Telefon geschehen. Beim *Tool-Based Social Engineering* werden dagegen Hilfsmittel wie versteckte Kameras, Keylogger oder Trojaner eingesetzt.

Psychologisches Know-how, das Wissen um die richtigen Tools, gute kommunikative Fähigkeiten, schauspielerisches Talent und nicht zuletzt und eine gehörige Portion Chuzpe sind also die Zutaten eines guten *Social Engineers*, wenn er einen Angriff simuliert. Dies erfolgt typischerweise in drei Phasen:

- Phase I: gezielte Informationsrecherche;
- Phase II: Zutritt & Zugang;
- Phase III: Informationsdiebstahl.



Phase I: Gezielte Informationsrecherche

In der ersten Phase macht sich der Industriespion mit dem Unternehmen vertraut und ermittelt die lohnendsten Zielpersonen

Wie „funktioniert“ das ausspionierte Unternehmen? Wer sind die lohnendsten Zielpersonen? Wie kann ich mit ihnen Kontakt aufnehmen und vertraut werden? In der ersten Phase seines Angriffs sucht der Spion gezielt Antworten auf diese Fragen und bringt so in Erfahrung, wie er am besten an die benötigten Informationen gelangen kann.

Die erste und beste Informationsquelle ist hier das Internet: Schon die Website eines Unternehmens gibt – oft ungewollt – wichtige Informationen preis. Über Stellenausschreibungen und Online-Jobbörsen lässt sich beispielsweise in Erfahrung bringen, welche Mitarbeiter ein Unternehmen sucht und ob man auf diesem Weg gegebenenfalls einen Spion einschleusen kann. Interessant ist auch, auf welchen anderen Websites das Opfer auftaucht, ob es Mitglied in einem Verband ist und ob seine Mitarbeiter Beiträge für News-groups verfassen.

Sobald man das „Gebilde“ Unternehmen verstanden hat, kann man sich daran machen, Zielpersonen auffindig zu machen, diese zu kontaktieren und ihr Vertrauen zu gewinnen. Auch hier hilft entscheidend das Internet mit Personensuchmaschinen wie z. B. YASNI. Die vorgebliche Intimität so genannter *Social Networks* wie Xing oder LinkedIn, die dem Knüpfen persönlicher Kontakte dienen sollen, verführt manche ihrer Mitglieder dazu, bereitwillig vertrauliche „dienstliche“ Informationen preiszugeben. So zeigt eine aktuelle Studie von McAfee, dass Namen und Daten, die auch auf den Onlineplattformen hinterlegt sind, häufig als Passwörter für Firmennetze benutzt werden. Spione schleichen sich in diese Netzwerke ein, um ein Vertrauensverhältnis zu einzelnen Mitgliedern aufzubauen mit dem Ziel, an wichtige Firmendaten heranzukommen.



Phase II: Zutritt und Zugang

Mit den aus Phase I gewonnenen Informationen versucht der Spion nun, in das Unternehmen einzudringen, d. h. sich physisch Zutritt zu verschaffen. Das kann z. B. bei einem Tag der offenen Tür für Ortsansässige geschehen, der eine erste Gelegenheit bietet, einen Betrieb von innen kennenzulernen. Mit dem nötigen Hintergrundwissen ist es für den geübten Spion auch kein Problem, als potenzieller Kunde aufzutreten oder als Servicetechniker Zutritt zu den Geschäftsräumen zu erhalten. Einen etwas anderen Weg wählten im Frühjahr dieses Jahres Datenräuber aus China, als sie ein Hamburger Technologieunternehmen ausspionierten: Sie schleusten chinesische Studenten als Praktikanten in die Firma ein. Diese kopierten vor Ort alle Daten, die Ihnen in die Hände fielen – aufgrund fehlender Deutschkenntnisse konnten sie einfach nicht einschätzen, welche Informationen wichtig waren und welche nicht.

In der zweiten Phase verschafft er sich physischen Zutritt zum Unternehmen und damit zu den Büros und dem Rechnernetz

Spione nehmen aber auch gerne den direkten Weg: In diesem Fall sieht man, wie sie untermals höflich lächelnd am Empfang vorbeigehen oder abends wild gestikulierend im schwarzen Anzug mit Krawatte die Putzkraft um Einlass bitten, begleitet von den Worten: „Alle Server sind abgestürzt, ich musste gerade diese Abendveranstaltung verlassen und jetzt funktioniert auch noch mein Firmenausweis nicht.“ Schon sind sie drin. Und sind sie erst mal drin, beginnt Phase III, der Diebstahl von Informationen.

Phase III: Informationsdiebstahl

Die klassische Methode des Informationsdiebstahls besteht in der Entwendung von materiellen und immateriellen Gegenständen: Der Spion betritt unverschlossene Büros oder Archivräume und durchforstet Schreibtische, Ablagen und Schränke. Er wühlt in Papierkörben neben Kopierern und Druk-

kern nach Fehlkopien von vertraulichen Informationen und durchsucht Abfalltonnen nach brauchbarem Material – in der Fachsprache nennt sich dieses Vorgehen „Dumpster Diving“. Sollte der Spion die benötigten Informationen hier nicht finden, entwendet er die Geräte, auf denen sie gespeichert sein könnten – Laptops, PDAs, externe Festplatten, Smartphones oder, in Fällen besonderer Dreistigkeit, auch einmal komplette stationäre Rechner. Diese Geräte durchsucht er nach den Daten oder benutzt sie, um auf größere zentrale Speichersysteme (Netzlaufwerke) Zugriff zu erhalten. Im günstigsten Fall gelingt es dem Spion, das betreffende Gerät nach Nutzung an seinen ursprünglichen Platz zurückzubringen, ohne dass der Besitzer vom Missbrauch Kenntnis erlangt.



Die dritte Phase bildet der eigentliche Informationsdiebstahl, d. h. das Entwenden von Fehlkopien und/oder Hardware sowie das Abschöpfen von Passwörtern bzw. Zugangscodes im telefonischen oder persönlichen Gespräch

In größeren Unternehmen bieten sich öffentliche Orte wie Kantinen an, um Kontakt zu Mitarbeitern aufzunehmen und sie in vorgeblich harmlose Gespräche zu verwickeln. Das persönliche Gespräch steht auch bei der „Königsdziplin“ des *Social Engineering* im Mittelpunkt – der Erlangung vertraulicher Informationen am Telefon. Dazu kontaktiert der Spion von einem internen Telefonapparat aus die Zielperson und gibt sich z. B. als Mitarbeiter der IT aus. Mit viel Fachchinesisch verwirrt er sodann sein Opfer: „Hallo, hier ist Meier vom IT-HelpDesk. Wir haben Ihretwegen 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 weitergeht, wird unser zentraler Core-Backbone-Router aufgrund der Denial-of-Service-Attacke automatisch rebooten, und kein Kollege wird mehr arbeiten können.“ Im Anschluss an dieses Bombardement bittet er höflich um Mithilfe bei der Lösung des Problems. Nach mehreren vorgetäuschten Fehlversuchen wird der User schließlich gebeten, dem vermeintlichen IT-Mitarbeiter sein Passwort mitzuteilen – und in 80 Prozent der Fälle erhält der Spion es auch.



Mit den so gewonnenen Informationen beginnt der Angreifer dann, richtigen Schaden anzurichten

Verlief ein solcher direkter Angriff auf einen Mitarbeiter erfolgreich, ergibt sich daraus meist die Möglichkeit, vor Ort mit den Mitteln des *Tool-Based Social Engineering* weiteren Schaden anzurichten. Industriespione können vertrauliche Informationen auf USB-Sticks kopieren, Keylogger an PCs anbringen oder Trojaner einschleusen.



Bis zu diesem Punkt bilden Security Assessments potenzielle Angriffsszenarien möglichst naturgetreu nach. Was sich daraus lernen lässt und wie Unternehmen die Erfahrungen in geeignete Maßnahmen und eine schlüssige Sicherheitsstrategie überführen können, ist Gegenstand der zweiten Folge unseres Beitrags in einem der nächsten Hefte.

Zu den Autoren: Andreas Schnitzer und Michael Hochenrieder sind Consultants beim auf Business Security und Business Development spezialisierten Beratungsunternehmen HvS-Consulting in München. E-Mail-Kontakt: schnitzer@hvs-consulting.de, hochenrieder@hvs-consulting.de.

Andreas Schnitzer, Michael Hochenrieder

Anatomie eines Industriespionage-Angriffs (II)

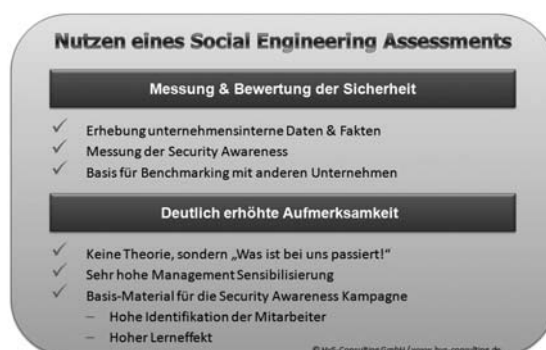
Im letzten Heft hatten wir die vielfältigen Angriffsmöglichkeiten aufgezeigt, die Industriespione heute nutzen können, und dabei insbesondere Techniken des so genannten Social Engineering herausgestellt. Diesmal wollen wir erklären, wie sich Unternehmen gegen solche Angriffe wappnen können.

Der erste Schritt sollte darin bestehen, ein Security Assessment mit Social-Engineering-Komponente vorzunehmen, um so Schwachstellen in der IT-Sicherheit aufzudecken. Die Ergebnisse dieser Prüfung sind in einer Dokumentation festzuhalten, die als Basis für den Auf- und Ausbau eines *Information Security Management* dient.

Zweck und Nutzen eines Security Assessment

Von der Prüfung wie von der Dokumentation nach einem Security Assessment profitieren Anwender gleich doppelt: Zum einen erhalten sie ein realistisches Bild davon, wie es in ihrem Unternehmen um die Sicherheit bestellt – hinsichtlich der Security Awareness der Mitarbeiter, aber auch hinsichtlich der physikalischen Sicherheit, etwa der Wirksamkeit von Zugangskontrollen. Ganz objektiv werden im Assessment unternehmensinterne Daten und Fakten zur Sicherheit erhoben, die auch zum Benchmarking mit anderen Unternehmen genutzt werden können.

Zum anderen bewirkt ein Security Assessment eine deutliche erhöhte Aufmerksamkeit gerade beim Management. Hat sich ein Sicherheitsverantwortlicher davor unter Umständen schwer getan, Sicherheitsthemen beim Management zu platzieren („bei uns kann so etwas nicht passieren“), sind die Ergebnisse eines Assessment nicht mehr Theorie, sondern Realität. An dieser Stelle sei darauf hingewiesen, wie wichtig es ist, ein Security Assessment von externen Beratern und nicht von eigenen Mitarbeitern vornehmen zu lassen: Die Ergebnisse eines solchen internen Assessment werden meist gerade deshalb in Zweifel gezogen, weil die Beschäftigten über einen hohen Kenntnisstand bezüglich Interna wie Sicherheitsvorkehrungen und -prozessen verfügen.



Zum anderen wird für Management und Mitarbeiter erkennbar, wo die konkreten Risiken liegen – das Thema wird fassbar und weniger abstrakt, wodurch die Sensibilität wächst und die Bereitschaft steigt, den Schutz von Informationen als wichtige Aufgabe der Unternehmensleitung zu sehen (s. nebenstehende Grafik).

Schutz vor Social Engineering

Natürlich wäre es von Vorteil, wenn es Patentrezepte zur Abwehr von Industriespionen und damit Social-Engineering-Attacken gäbe. Aber leider ist dies nicht der Fall. Im Gegenteil: Schon das Erkennen eines derartigen Angriffs bereitet oft nicht geringe Schwierigkeiten. Das liegt vor allem daran, dass jedes Unternehmen seine Eigenarten und Besonderheiten hat, auf die sich ein geschickter Spion binnen kurzer Zeit einstellt. Entsprechend individuell müssen potenzielle Opfer auch ihre Abwehrmaßnahmen gestalten.

Dabei ist vor allem ein Grundsatz zu beachten: Technik allein hilft nicht! Funktionierende physikalische und technische Sicherheitsmaßnahmen (z. B. Einlasskontrollen, der Einsatz von Firewalls oder abgestufte Berechtigungskonzepte für den Datenzugriff) sind zwar Voraussetzung für eine erfolgreiche Abwehr, können aber auch das Gegenteil bewirken: Verlassen sich die Mitarbeiter auf die Technik, hat es ein Spion oft besonders leicht. Denn in einer solchen Umgebung rechnet meist niemand mit den – wie gezeigt – oft verblüffend einfachen Social-Engineering-Attacken.

An erster Stelle steht daher die Sensibilisierung der Mitarbeiter. Da der Angreifer beim Social Engineering 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.

Diese Sensibilisierung der Mitarbeiter muss in die Einführung unternehmensweiter Sicherheitsmaßnahmen eingebettet sein. Dazu zählen u. a. die Einführung von Sicherheitsrichtlinien, die Optimierung aller sicherheitsrelevanten Prozesse sowie deren Dokumentation, regelmäßige Security-Audits (ebenfalls mit Dokumentation), die Optimierung der physikalischen Sicherheit, Regelungen für den Katastrophenfall und weitere individuell auf das jeweilige Unternehmen abgestimmte Maßnahmen. Verantwortlich für diese Maßnahmen ist der (gegebenenfalls noch zu bestimmende) Sicherheitsbeauftragte, der auch ihre Einhaltung überwacht.

Die Sicherheitsrichtlinien des Information Security Managements sind inhaltlich Grundlage einer Security-Awareness-Kampagne, die sich an alle Mitarbeiter und diese für die Richtlinien, die eingeführten Maßnahmen und insbesondere auch für Social Engineering sensibilisiert. 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. Dabei wird zuerst das Interesse für das Thema Informationssicherheit geweckt, z.B. mit Postern oder Ausstellern. Den Schwerpunkt bildet Phase 2, in der die Mitarbeiter in Präsenztrainings geschult werden. Ist dies nicht möglich – etwa aufgrund besonderer Dringlichkeit, einer extrem großen Zahl von Teilnehmern oder damit verbundener Zusatzkosten – kann man auch auf Onlinetrainings zurückgreifen. Große Bedeutung bei den Trainings hat die direkte und nachvollziehbare Darstellung der Gefahren durch Live-Demonstrationen (z. B. Spam verschicken, Wirkung eines Trojaners demonstrieren) oder durch den Einsatz multimedialer Elemente wie Videos. Gesehenes wird oft besser erinnert als nur Gehörtes.

Gerade die Social-Engineering-Angriffsmethoden eines Industriespions können in nachgestellten Szenen effektiv verbildlicht werden. Beispielsweise lässt sich so veranschaulichen, wie die guten menschlichen Eigenschaften Hilfsbereitschaft oder Freundlichkeit durch einen Angreifer gezielt ausgenutzt werden. Kennen die Mitarbeiter die Vorgehensweise eines Industriespions, sind sie später in der Lage, den Unterschied zwischen reiner Freund-

lichkeit und einem Angriffsversuch, zwischen Smalltalk und Aushören zu erkennen. Phase 3 einer Kampagne dient der Nachhaltigkeit, damit Sicherheit nach den Trainings nicht nur verstanden, sondern auch gelebt wird. Hier können Elemente wie Security-Bildschirmschoner oder Give-Aways eingesetzt werden. Da einmal Gelerntes leider in Vergessenheit gerät, sind die Maßnahmen einer Kampagne durch alle Phasen hindurch stetig zu wiederholen, um die Einstellung der Mitarbeiter zeitstabil nachhaltig zu verändern. Um die Effizienz der Maßnahmen zu steigern, sollten Unternehmen – ebenso wie für das Security Assessment im Vorfeld – einen externen Dienstleister ins Boot holen. Dieser muss, wie jeder andere Dienstleister auch, in Hinsicht auf Vertrauenswürdigkeit und Referenzen überprüft werden. Der externe Dienstleister verfügt nicht nur über das größere Know-how, sondern in aller 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.

Zusammenfassung

Industriespionage stellt für viele Unternehmen ein reales Gefahrenpotenzial dar, das die meisten Betriebe und deren Management 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. Vorsorgemaßnahmen zur Abwehr von Industriespionage-Angriffen stellen zumeist eine Art Versicherung dar, die oft als „unnütze“ Ausgabe angesehen wird, solange es zu keinem Schaden kommt. Aber muss man wirklich warten, bis das Kind in den Brunnen gefallen ist? Die Antwort auf diese Frage kann nur „Nein“ lauten. Unternehmen sollten stattdessen wachsam bleiben und eine Reihe von Vorkehrungen treffen, um Angriffe rechtzeitig zu erkennen und abzuwehren (vgl. unsere abschließende Checkliste).

Ihre Checkliste gegen Industriespionage
Unternehmensweite Sicherheit ist eine Aufgabe der Geschäftsleitung. Beauftragen Sie einen Sicherheitsverantwortlichen (z.B. Chief Security Officer) in entsprechender Stellung.
Führen Sie allgemein gültige unternehmensweite Sicherheitsrichtlinien ein.
Definieren Sie die relevanten Prozesse und dokumentieren Sie diese. Orientieren Sie sich dabei an allgemeingültigen Sicherheitsstandards wie z.B. ISO 27001.
Überprüfen Sie regelmäßig die Einhaltung der Richtlinien und Prozesse (Audits).
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 stetige Sensibilisierung notwendig.
Eine funktionierende IT- und physische Sicherheit sind Voraussetzung zur Abwehr von Industriespionage – aber denken Sie daran: Je ausgereifter die technische Sicherheit, desto einfacher ist Social Engineering!
Nutzen Sie das spezielle Know-how von Externen (gegen Betriebsblindheit).
Sicherheit ist kein einmaliger Prozess – Sicherheit ist ein laufender Prozess. Heute so wichtig wie morgen.

Zu den Autoren: Andreas Schnitzer und Michael Hochenrieder sind Consultants beim auf Business Security und Business Development spezialisierten Beratungsunternehmen HvS-Consulting in München. E-Mail-Kontakt: schnitzer@hvs-consulting.de, hochenrieder@hvs-consulting.de.