Eine Bestandsaufnahme

Wirtschaftskriminalität & Industriespionage 2.0

Von Hans Joachim Giegerich, Christian Schülke, Michael Wiesner und Christian Flory

Ein modernes Unternehmen öffnet sich der Welt, denn in der Globalisierung ist es für eine exportorientierte Industrie wie die deutsche unerlässlich, auch extrovertiert zu kommunizieren, um neue Märkte zu erschließen und vorhandene Marktstellungen zu behaupten.

Hans Joachim Giegerich, Geschäftsführer Giegerich & Partner GmbH

Christian Schülke ist Geschäftsführer der schuelke.net internet. security.consulting

Michael Wiesner ist Geschäftsführer der Secutrends GmbH

Christian Flory, Projektleiter Hessen-IT, HA Hessen Agentur GmbH

Das wissen auch Wirtschaftskriminelle und Industriespione und machen sich diesen Umstand zunutze, um wahlweise an das Geld oder die Innovationen anderer zu gelangen. Die wichtigsten Methoden und deren Abhilfe soll dieser Beitrag analysieren.

Stellen Sie sich vor: Hannover Messe Industrie, die Welt zeigt die neuesten Innovationen, und Sie sind dabei. Der eigene Messestand steht, und Sie nehmen sich die Zeit, durch die Hallen zu schlendern und einen Blick auf die Mitbewerber zu werfen. Da sehen Sie – Ihre Maschine an einem anderen Stand! Ihre Maschine, deren erste Muster Sie ausgewählten Kunden an den nächsten Messetagen zeigen wollen. Die Maschine, von der Sie sich versprechen, den Markt aufrollen zu können. Die Maschine, die die Zukunft Ihres Unternehmens für die nächsten Jahre sichern soll.

Eine utopische Vorstellung? Leider nein, denn immer öfter werden hierzulande innovative Unternehmen Opfer von Industriespionage. Das dokumentieren verschiedene Studien zur Wirtschaftsspionage sehr deutlich, zuletzt die Untersuchung der Sicherheitsfirma Corporate Trust in Kooperation mit dem TÜV Süd und der Internetsicherheitsfirma Brainloop. Demnach haben 20 Prozent aller Unternehmer schon einmal Spionageangriffe der Konkurrenz erlebt. Weitere 33 Prozent verzeichnen einen Informationsabfluss aus ihrem Unternehmen, ohne die Spionage belegen zu können. Immer öfter werden Betriebe Opfer von Wirtschaftskriminellen, die sich an ihnen bereichern wollen.

Intellectual Property

Wissen und Innovationen, neudeutsch Intellectual Property genannt, sind der wichtigste Rohstoff der Exportnation Deutschland. Dadurch sind unsere Produkte und Dienstleistungen weltweit sehr gefragt. Manche Unternehmer aus anderen Staaten verfolgen jedoch böse Absichten: Sie wollen keine Produkte und Dienstleistungen der Anbieter, sondern deren Know-how erwerben – durch Diebstahl und verschiedentlich sogar mit

der Unterstützung der Geheimdienste ihres Landes. Zielten die Aktivitäten mancher Geheimdienste in der Vergangenheit lediglich auf militärische Objekte ab, so sind inzwischen kommerzielle Innovationen in den Fokus der Täter gerückt (vergleiche Verfassungsschutzbericht 2010, BKA Bundeslagebild Cybercrime 2010). Dafür bedienen sich die Angreifer einer breiten Palette an Möglichkeiten der Informationsbeschaffung. Die wichtigsten diskutieren wir hier.

Data Leakage

Spionageinstrument Aktentasche

Es muss nicht immer ein Angriff durch elektronische Spionagewerkzeuge sein. Selbst im Zeitalter der Online-Datenverarbeitung werden sensitive Informationen noch gerne auf Papier gespeichert und transportiert. Geht es nur um einzelne Dokumente, so lassen sich diese bequem in einer Aktentasche außer Haus tragen. Welcher Mittelständler kontrolliert schon die Taschen seiner Mitarbeiter? Wenn einem Täter Taschen nicht genügend „Tragekomfort" bieten, benutzt er eine Digitalkamera oder ein Smartphone. Die Qualität der dort integrierten Kameras reicht inzwischen für viele Spionageaufgaben vollkommen aus. Für den Profi gibt es in einschlägigen Internetshops auch die Uhr mit eingebauter HD-Kamera – James Bond lässt grüßen. Im Zeitalter von BYOD (Bring Your Own Device) haben viele Mitarbeiter die Möglichkeit, auf diesem Weg brisante Informationen außer Haus zu schaffen. Diesem Risiko lässt sich nur durch Reglementierung des physischen Zutritts und des Zugriffs begegnen.

Nicht alle Unterlagen eignen sich für diese Methode. So ist der Datendieb oft an digitalen Originalunterlagen interessiert. Gleich einem Fuchsbau, haben digitale Rechnersysteme eine ganze Menge an Ausgängen. Hierzu zählen:

- E-Mails,
- Uploads über Webseiten oder Cloud-Festplatten wie Dropbox & Co.,
- soziale Netzwerke,
- Peer-2-Peer Filesharing,
- Instant Messaging,
- lokale Schnittstellen (USB, DVD-Brenner, Firewire, Smartcard-Reader etc.).

Um den Spionagefuchs zu stellen und ihn am Verlassen des Baus zu hindern, sollten Unternehmen alle diese Ausgänge überwachen. Hierzu ist ein ganzes Bündel an Maßnahmen erforderlich:

- Beschränkung des Zugriffs auf den jeweils notwendigen Personenkreis (Need to Know/Need To Have-Prinzip),

- Beschränkung der Internet- und E-Mail-Nutzung im Unternehmen auf geschäftliche Zwecke,
- Prüfung des aus- und eingehenden Datenverkehrs auf fragwürdige Aktivitäten,
- Richtlinien zum Gebrauch sozialer Netzwerke sowie ein Monitoring der dortigen Aktivitäten,
- Implementierung von Endpoint Security zur Überwachung und Sperrung lokaler Schnittstellen.

Social Engineering

Schwachstelle Mitarbeiter

Angenommen, die obigen Maßnahmen sind in Ihrem Unternehmen bereits implementiert und werden entsprechend gelebt, dann wäre die Palette der Möglichkeiten für potentielle Angreifer noch lange nicht ausgeschöpft. Sie greifen zu Methoden, die im Spionageumfeld zum absoluten Handwerkszeug gehören und unter dem Begriff Social Engineering zusammengefasst sind. Nur wenige Mitarbeiter besitzen das notwendige Gefahrenbewusstsein für den Fall, dass ein freundlicher Anrufer scheinbar unwesentliche Informationen erfragt oder Tätigkeiten forciert, die dazu dienen, einen Angriff vorzubereiten. Diese Methoden sind deutlich älter als die moderne Datenverarbeitung, aber auch im Internetzeitalter erfolgreich.

Kennen Täter die Schwächen und Vorlieben von Mitarbeitern in einem Unternehmen, die an zentraler Position tätig sind, so lassen sich einzelne Personen am Ende für die eigenen Ziele manipulieren. Mancher Angreifer gelangt unter einem seriösen Vorwand oder bei einem zur Tarnung vereinbarten Termin ins Firmengebäude oder auf das Werksgelände, um beispielsweise ein paar USB-Sticks unauffällig zu verteilen. Jene Sticks sind vielleicht mit einem ansprechenden Aufkleber mit dem Aufdruck „Privat“ oder „xxx“ versehen, was insbesondere das Interesse der männlichen Belegschaft wecken soll. Fällt ein Mitarbeiter darauf herein und öffnet den Inhalt der USB-Sticks, so beginnt ein Trojaner seine perfide Arbeit im Hintergrund und teilt Informationen wie Zugangsdaten, Surfverhalten und Ähnliches seinem spionierenden Herrn und Meister mit.

Möchte ein Angreifer das Risiko, entdeckt zu werden, so gering wie möglich halten, greift er in die IT-technische Büchse der Pandora. Reisekosten und Risiken der Ergreifung sinken, wenn statt eines Menschen direkt ein vom Mensch gesteuerter digitaler Sprengsatz mit Hilfe eines Computervirus oder eines Trojaners ins Zielunternehmen eindringt.

Eine E-Mail mit dem Betreff „Gratis im 911er über die Nordschleife“ wird ein motorsportbegeisterter Mitarbeiter – und diese Information erhält er

problemlos durch soziale Netzwerke wie Facebook oder XING – mit großer Sicherheit öffnen, selbst dann, wenn sie von einem unbekannten Absender stammt. Ist die E-Mail mit einem digitalen Schädling gespickt, stehen dem Angreifer Tür und Tor offen. Virenschutzprogramme sind hier oft wirkungslos, da es sich in den meisten Fällen um speziell angepasste Schadprogramme handelt, sogenannte Custom Malware, die nicht erkannt wird. Bei Drive by Downloads werden ähnliche Techniken eingesetzt – mit dem Unterschied, dass dabei Webseiten, die auf den ersten Blick sicher und seriös wirken, manipuliert werden, um Besuchern der Webseite die verborgene Nutzlast beim Vorbeisurfen einzuschleusen.

Sabotage

Spionagelücken können in die Insolvenz führen

Der Angreifer setzt bei solchen Methoden die Ideen des Social Engineerings und des Angriffs durch Schadsoftware kombiniert ein und kann so oft dauerhaft auf die internen Unternehmensressourcen zugreifen. Jüngstes und gleichwohl ältestes Beispiel dieser als Advanced Persistent Threads (APT) bezeichneten Angriffe ist der ehemalige TK- und Netzwerkausrüster Nortel Networks. Hier hatten Angreifer über zehn Jahre lang ungehinderten und unerkannten Zugriff auf sämtliche brisanten Informationen des Unternehmens. Die Insolvenz des Unternehmens im Jahr 2009 lässt genügend Raum zur Spekulation darüber, ob hier ein direkter Zusammenhang besteht.

Neben der reinen Informationsgewinnung ist auch die gezielte Sabotage ein verbreiteter Zweck solcher Angriffe. Nach wie vor gilt dabei Stuxnet als Paradebeispiel dafür, wie Social Engineering mit digitalen Sprengsätzen in Trojanern gepaart werden kann, um hochsensible und hochkritische Infrastrukturen zu schädigen. Im genannten Fall haben Experten drei Versionen des Wurms identifiziert, die gezielt an wenigstens fünf Unternehmen verteilt wurden, die für die iranische Urananreicherungsanlage in Natanz arbeiteten. Vermutlich haben deren Mitarbeiter den Trojaner unwissentlich in die Anlage eingeschleppt, der die Steuerungssysteme manipulierte und die Urananreicherung blockierte. Stuxnet wurde wohl von staatlichen Stellen initiiert und ist eine Demonstration der Wirkung und der Ziele von APT.

Digitale Erpressung

Wird eine Sabotage angedroht, geht es den Angreifern meist um eine direkte monetäre Bereicherung. Sie attackieren kritische Infrastrukturen von Unternehmen, ohne sie direkt zu zerstören. Die Androhung des Verlusts ganzer Produktionschargen im Industriesektor oder der Störung des Webauftritts eines Online-Wettanbieters kurz vor der heißen Phase sind

die digitale Version der Schutzgelderpressung. In der Regel demonstriert der Angreifer seine Macht entsprechend wirkungsvoll, so dass den Opfern kaum etwas Anderes übrig bleibt, als den Forderungen nachzukommen.

DDoS-Attacken (Distributed Denial of Service), bei denen IT-Dienste über massenweise versendete Anfragen außer Gefecht gesetzt werden, sind hierbei das beliebteste Mittel. Doch nicht nur Unternehmen sind Ziele solcher Angriffe. Speziell für diesen Zweck entwickelte Trojaner, sogenannte Ransomware, sperren den heimischen PC und fordern eine Lösegeldzahlung, damit der Benutzer wieder an seine Daten kommt. BKA- und GEMA-Trojaner sind die bekanntesten Vertreter dieser Art.

Hacktivisten

Spaß an der Zerstörung

Bedrohlich kann es für Ihr Unternehmen auch werden, wenn Sie ins Fadenkreuz sogenannter Hacktivisten geraten. Im Sammelbecken dieser Spezies von IT-Experten finden sich Menschen, denen es schlicht Spaß bereitet, an sensitive Informationen zu gelangen oder IT-Infrastrukturen zu stören. Zu den Hacktivisten gehören auch Hacker mit unterschiedlichsten politischen Zielen und solche Hacker, die mit ihrem Wissen und ihren Fähigkeiten – oft durch zerstörerische Tätigkeit – selbst die kleinste Sicherheitslücke nachweisen wollen. Der Kollateralschaden, den diese Gruppen erzeugen, reicht bis zur Liquidierung von Unternehmen, indem sie deren Sicherheit öffentlichkeitswirksam aushebeln. Sicherheitsdienstleister wie RSA oder Digi-Notar zählen bereits zu den Opfern solcher Gruppierungen. Sollte Ihr Unternehmen in eine der Risikogruppen fallen, zu denen Sicherheitsdienstleister, Sicherheitsbehörden, Finanzwirtschaft etc. gehören, sind zusätzliche Maßnahmen erforderlich, um die Angriffsfläche für Gruppierungen wie Anonymous und ähnliche möglichst gering zu halten.

Sicherheitsmaßnahmen

Gemäß dem bekannten Satz, dass Sicherheit niemals hundertprozentig sein kann, empfiehlt es sich, nicht in Panik zu verfallen oder den Kopf in den Sand zu stecken. Wichtig ist vielmehr, sich der Bedrohungen bewusst zu werden und geeignete Sicherheitsmaßnahmen zu etablieren. Oft wird der Fehler gemacht, sich allein auf technische Maßnahmen zu verlassen. Die wirken aber nie umfassend, sondern nur punktuell. Eine Grundinfrastruktur wie Virenscanner, Content-Filter, Firewalls oder Intrusion-Präventionssysteme sollte natürlich vorhanden sein, um wenigstens die nicht gezielten Angriffe abwehren zu können.

Zudem sollten Unternehmen Angreifern ihr Handwerk durch den Einsatz zusätzlicher Sicherheitsmechanismen wie Verschlüsselungen und

Authentifizierungen zusätzlich erschweren. Noch effektiver sind organisatorische Maßnahmen zur Verbesserung der IT-Sicherheit. Dies sind insbesondere Sensibilisierungs- und Weiterbildungsmaßnahmen, da der Mensch in vielen Fällen das schwächste Glied in der Kette ist. Prüfen Sie vor jeder Implementierung, welche Bereiche Ihres Unternehmens wie viel Sicherheit brauchen bzw. welche Sicherheitsmaßnahmen noch in Relation zum erwarteten Sicherheitsgewinn stehen.

Datensparsamkeit

Das Volumen an veröffentlichten Informationen wächst ständig

Das Bundesverfassungsgericht bestätigte erst jüngst dem Einzelnen ein sehr weitgehendes Grundrecht auf informationelle Selbstbestimmung. Aber auch Unternehmen haben vielfach ein vitales Interesse daran, aus rein unternehmerischen Gründen den Informationsfluss nach außen zu beschränken. Demgegenüber steht oftmals der Staat mit immer zahlreicher werdenden Informations- und Veröffentlichungspflichten. Der vordergründige Bürokratieabbau darf nicht darüber hinwegtäuschen, dass per Saldo mehr Informationen über Unternehmen öffentlich verfügbar sind denn je. Zusammen mit den Informationen, die Unternehmen aus Marketing- und Werbezwecken selbst veröffentlichen, bilden diese eine gute Basis für erfolgreiche Angriffe.

Hinzu kommen die Informationen, die Mitarbeiter über das Unternehmen veröffentlichen, beispielsweise in sozialen Netzwerken. Diese Informationsquellen sind der Nährboden für Open Source Intelligence. Dieser Begriff ist nicht mit Open-Source-Software zu verwechseln, denn er bezeichnet das Sammeln von (nachrichtendienstlichen) Informationen aus öffentlich zugänglichen Quellen.

Daher sollte ein Bewusstsein dafür entwickelt werden, welche Informationen sich für die Vorbereitung von Angriffen nutzen lassen und wie sich solche Angriffe einschränken oder verhindern lassen. Neben der durchgängigen Klassifizierung von Informationen ist eine unmissverständliche Kommunikationsrichtlinie ein wichtiger Baustein im Kampf gegen den ungewollten Informationsabfluss.

Exkurs: Staatstrojaner

Noch wichtiger wird die Bewusstseinserfordernis, wenn Ermittlungsbehörden oder Geheimdienste selbst, beispielsweise mit Hilfe von Staatstrojanern, Hintertüren auf Rechnern installieren, die im Zweifelsfall den direkten Zugriff auf Unternehmensdaten ermöglichen. Diese Hintertüren können gegebenenfalls auch Kriminelle für die eigenen Machenschaften ausnutzen.

GRC

Sicherheitsmaßnahmen dürfen nicht vom Kerngeschäft ablenken

Nun wird kein klar denkender Mensch erwarten, dass all diese Herausforderungen mal eben so neben allen anderen unternehmerischen Herausforderungen zu bewältigen sind. Welche Richtschnur, welchen Rahmen kann ich als Unternehmer wählen, um zum Ziel möglichst großer Sicherheit zu gelangen?

Für den universellsten Ansatz als Antwort steht die Abkürzung GRC – Governance, Risk Management, Compliance. Sie fasst die drei wichtigsten Handlungsebenen eines Unternehmens zusammen:

- Governance, d. h. die Unternehmensführung durch vordefinierte Richtlinien,
- Risikomanagement,
- Compliance, d. h. das Einhalten interner wie externer Normen.

GRC definiert Richtlinien für die erfolgreiche Unternehmensführung. Dabei darf keinesfalls vergessen werden, dass in einem höchst dynamischen und von starken Veränderungen geprägten Zeitalter der Weg zwar nicht das Ziel sein darf, aber im Detail sehr häufig der Stein des Sisyphos wieder den Berg hinunterzurollen droht.

Risikomanagement

Insbesondere das IT-Risikomanagement sollte integraler Bestandteil der Unternehmensführung sein. Das ist für bestimmte Unternehmen sogar gesetzlich verankert (vgl. z. B. §91 AktG). Wie bei jedem Managementprozess handelt es sich dabei um einen Kreislauf, der dem PDCA-Prinzip folgt (Plan – Do – Check – Act). In diesem fortlaufenden Prozess lassen sich die Unternehmensziele kontinuierlich mit den Risiken abgleichen. Auch kann für eine zweckmäßige Behandlung dieser Risiken gesorgt werden.

Seien Sie sich stets bewusst, dass Menschen außerhalb Ihres Unternehmens ein Interesse an Ihren Informationen haben! Seien Sie sich bewusst, dass andere Unternehmen Ihnen Ihre Produkte und Erfolge neiden und abjagen wollen! Immer mehr Angreifer im Sinne der oben getroffenen Definition „advanced“ und „persistent“ stellen eine echte Bedrohung (threat) für Ihr Unternehmen dar. Fangen Sie an, in diesem Bewusstsein zu handeln!

Die Aktionslinie Hessen-IT des Hessischen Wirtschaftsministeriums informiert Unternehmen über alle wichtigen Fragen des Einsatzes von Informations- und Kommunikationstechnologien und natürlich auch über

Risikomanagementstandards, Frameworks und Best Practices

- BSI-Standard 100-3
  www.bsi.bund.de
- ISO/IEC 27005
  www.iso.org
- COBIT 5 (ISACA)
  www.isaca.org
- Risk IT Framework (ISACA)
  www.isaca.org
- Risk Management Framework (NIST)
  www.nist.gov

IT-Sicherheitsaspekte. Die in die HA Hessen Agentur GmbH eingegliederte Aktionslinie hat verschiedene Informationsmaterialien herausgebracht, die sich mit dem Thema IT-Sicherheit beschäftigen. Darüber hinaus existiert in Hessen mit Institutionen wie dem Fraunhofer-Institut für Sichere Informationstechnologie (SIT) und dem Center for Advanced Security Research Darmstadt (CASED) eine vielseitige Forschungslandschaft mit IT-Sicherheitsschwerpunkten.

Neuer Leuchtturm in der IT-Sicherheit

Im Mai 2012 wurde das Intel Collaborative Research Institute for Secure Computing (CRI-SC) an der Technischen Universität Darmstadt eröffnet. Es stellt als erstes Intel-Institut außerhalb der USA einen neuen, weit über die Grenzen Hessens hinaus sichtbaren Leuchtturm dar. Im Rahmen der Aktivitäten von Hessen-IT ist zudem eine Expertengruppe hessischer IT-Sicherheitsanbieter sehr aktiv, aus deren Arbeit dieser Artikel entstanden ist. ■