Alexander Tsolkas | Friedrich Wimmer

Wirtschaftsspionage und Intelligence Gathering

Neue Trends der wirtschaftlichen Vorteilsbeschaffung

PRAXIS

Springer Vieweg

Wirtschaftsspionage und Intelligence Gathering

Alexander Tsolkas • Friedrich Wimmer

Wirtschaftsspionage und Intelligence Gathering

Neue Trends der wirtschaftlichen Vorteilsbeschaffung

Mit 20 Abbildungen

PRAXIS

Springer Vieweg

Alexander Tsolkas
Riedstadt, Deutschland

Friedrich Wimmer
Bad Feilnbach, Deutschland

ISBN 978-3-8348-1539-2
ISBN 978-3-8348-8640-8 (eBook)
DOI 10.1007/978-3-8348-8640-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Einbandentwurf: KünkelLopka GmbH, Heidelberg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.springer-vieweg.de

Dieses Buch widme ich meiner lieben Familie Olivia, Helen und Franziska Tsolkas.

– Alexander Tsolkas

Dieses Buch widme ich Christina, Samuel und der gesamten Familie Wimmer, sowie allen, die mich bei diesem Projekt unterstützt haben.

– Friedrich Wimmer

Vorwort

Friedrich Wimmer studierte Computer- und Mediensicherheit und anschließend Sichere Informationssysteme. Nach und nach formte sich bei Ihm die Idee, dass über vorrätig gehaltene Daten Wirtschaftsspionage betrieben werden kann. Vor allem zur Generierung von „Vorwissen“ (z.B.: Trends, Geschäftsentwicklungen, Profiling) als Auftakt für Entscheidungen sind diese Datenbanken prädestiniert. Bei eingehenderer Recherche wurde ihm klar, dass dies ein kaum bis gar nicht thematisiertes Gebiet der Wirtschaftsspionage ist. Es zeigte sich ebenfalls, dass diese Daten nicht nur für Geheimdienste, sondern auch für weitere Akteure von Interesse sind.

Ein Workshop mit Siemens-Mitarbeitern aus der Abteilung Corporate Security, zwei Mitarbeitern des Bayerischen Landesamtes für Verfassungsschutz aus der Abteilung Spionageabwehr/Wirtschaftsschutz und einem KPMG-Mitarbeiter aus Österreich zeigte die Brisanz dieses Themas.

Alexander Tsolkas beschäftigt sich seit 1993 mit Informationssicherheit, IT- und operationellem Risikomanagement, Datenschutz und Unternehmenssicherheit. In vielen seiner IT-Projekte ist er mit unterschiedlichsten Anforderungen und Sachverhalten bei der Absicherung anfragender Unternehmen und Organisationen konfrontiert worden.

Seit dem Jahr 2002 beschäftige er sich zusätzlich zu den oben genannten Themen mit e-Discovery. In diversen e-Discovery-Fällen, in denen er analytisch, empirisch und forensisch beratend involviert war, entdeckte Alexander Tsolkas von Mal zu Mal mehr den eindeutigen Sachverhalt der Wirtschaftsspionage.

In vielen e-Discovery-Fällen in den USA wurde im Anschluss an einige Urteile bzw. auch bei einem Vergleich Recht verzerrt, um ausländische Unternehmen vornehmlich in den USA finanziell oder in Ihrem Image zu schädigen. Andere, nichtamerikanische Unternehmen, wurden in den USA zu Recht verurteilt, wie z.B. auch verschiedene deutsche Unternehmen, die in Schmiergeldaffären verwickelt waren.

Ein Gespräch mit einem Sicherheitsexperten wurde als Interview in der Computerwoche im Security Expertenrat und später in SecTank[1] veröffentlicht. Der Arti-

1 SecTank ein bekanntes IT-Security Blog und ein auf Alexander Tsolkas eingetragenes Markenzeichen beim Deutschen Marken- und Patentamt.

kel heißt: „S.W.I.F.T[2]: Spioniere. Wirtschaftsdaten. International. Faktisch. Täglich“ und beschreibt, wie durch den Datentransfer der S.W.I.F.T-Daten von Europa in die USA, wesentliche wirtschaftliche Zusammenhänge diverser Art durch Datenanalyse der Amerikaner herausgelesen werden können.

Weitere Anstöße erhielt Alexander Tsolkas in der Zeit als CSO der Schenker AG in Essen, als die Amerikaner nach dem 11.9.2001 im Schlepptau von Safe Harbour und dem Terrorismus C-TPAT und vieles andere einführten, um die Daten von zu versendenden Transportgütern mindestens 24 Stunden vor Eintreffen der Fracht auf amerikanischem Boden zu erhalten.

Zwei Jahre später erhoben die Amerikaner die Flugpassagierdaten aller Fluggäste, und fingen in 2005 unangekündigt an, mobile Computergeräte bei der Einreise von Nicht-Amerikanern am Immigration Officer Desk zu beschlagnahmen. Hinter verschlossenen Türen wurde seitens der Amerikaner seit mehreren Jahren versucht das Anti-Counterfeiting Trade Agreement (ACTA-Abkommen, SOPA, PIPA) international durchzusetzen. Das alles machte Alexander Tsolkas sehr skeptisch, und er fing an, einen Zusammenhang in all den gesammelten Daten zu sehen. Für was musste man so viele Daten erheben? Alles nur dafür, um einen Terroristen und seine Gefolgsleute zu jagen? Es hatte genauso System, wie viele andere eingesetzte Methoden der Wirtschaftsspionage.

Das vorliegende Buch soll Unternehmen auf diese Bedrohung aufmerksam machen und verständlich darlegen, welche Problemfelder derartige Datenhalden eröffnen.

Die Autoren danken dem Verlag Springer Vieweg herzlich für die super Unterstützung bei der Erstellung dieses Buches. Unser Dank gilt auch allen anderen, die uns in jeglicher Form unterstützten. Danke!

Februar 2012 Alexander Tsolkas und Friedrich Wimmer

[2] SWIFT - Society for Worldwide Interbank Financial Telecommunication

Inhalt

1 Einleitung

1.1 Hintergrund

Die Wirtschaftsspionage hat seit dem Mauerfall zugenommen. Seit dem Zusammenbruch des ehemaligen Ostblocks und dem Ende des Kalten Krieges gab es einen Überfluss an amerikanischen und russischen Agenten. Die meisten russischen Agenten wurden arbeitslos oder (Militär-)Berater von unterentwickelten Drittländern, gingen entweder in die Politik (siehe Putin) oder betrieben Wirtschafts- oder Militärspionage im Auftrag Moskaus und im Auftrag von privaten Auftraggebern in aller Herren Länder.

Die amerikanischen Agenten hingegen wurden von Präsident Clinton zum größten Teil zu Wirtschaftsspionen gegen Deutschland und die Welt umorganisiert [109].

Die Visionen der Intelligence Services im Allgemeinen und der in Europa stationierten Three-Letter-Code Agencies, bzw. der amerikanischen NSA wurden neu definiert. Sollte kein militärischer Krieg mehr gewonnen werden können, so musste man die amerikanische Wirtschaft von dieser Zeit an auch auf anderen Gebieten mit Aufträgen versorgen und deren wirtschaftliche Vorteile sichern, nicht nur die der Rüstungsindustrie.

Nach einigen öffentlich gewordenen Fällen kochte das Thema Wirtschaftsspionage Ende der 90er Jahre hoch. Echelon wurde langsam „offiziell“ und einige (vor allem Luftfahrt-) Manager gingen dazu über, nicht mehr per Telefon, Fax oder E-Mail zu verhandeln [135]. Wie in diesem Buch unter anderem erläutert wird, wurde diese „Lücke“ des persönlichen Verhandelns als Schutz vor Wirtschaftsspionage nun durch das Sammeln von Bewegungsprofilen von den Geheimdiensten der USA als Problem erkannt und „geschlossen“.

Deutschland wird nicht alleine durch die USA ausspioniert. Mit an der Spitze der Deutschland ausspionierenden Länder sind England, Frankreich, Russland, China, Indien, Brasilien, Japan, Mexiko, und mittlerweile auch Taiwan und Korea. Vietnam reiht sich langsam in die obige Gruppe ein. Beim Intelligence Gathering gibt es jedoch einen ungeschlagenen Spitzenreiter - die USA [109].

Das klassische Ausspionieren funktioniert noch immer in der Art und Weise, wie vor tausend und mehr Jahren. Ein eingeschleuster oder bezahlter Auftragnehmer liefert die wichtigen Informationen, die ein Auftraggeber benötigt. Diese Art und Weise ist immer noch die häufigste Form der Spionage. Eine Brute Force Attacke, d.h. der Einbruch und Diebstahl von Informationen in Büros der Opfer hat stark nachgelassen. Es passiert noch, aber es ist langsam „out“.

A. Tsolkas, F. Wimmer, *Wirtschaftsspionage und Intelligence Gathering*,
DOI 10.1007/978-3-8348-8640-8_1 © Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden 2013

Dafür hat Cyber Warefare bzw. Information Warfare [119] – unter anderem ein gezieltes Tool zur Wirtschaftsspionage und einer infrastrukturellen Kriegsführung mit noch weit größerer Auswirkung auf eine Gesamtwirtschaft im Internet – stark zugenommen.

Die derzeit aktuellste und modernste Version der Wirtschaftsspionage übertrifft alles, was es bisher gab. Im ihrem Buch „Die Schock-Strategie“ [131] beschreibt Naomi Klein anhand von belegten Beispielen, wie man nationale Ereignisse schafft, anhand derer man globale Gesetze und Regeln für die Menschheit ändern kann. Was Frau Klein hier beschreibt, haben die Amerikaner seit „9/11“ mehrmals ausgenutzt. Unter dem Deckmantel des Auffindens von Terroristen lassen wir in gutem Glauben alle möglichen Informationen und Daten, die wir früher alleine schon aus dem Bauchgefühl heraus nie geliefert hätten, fließen. Schließlich sind die deutsche und europäische Wirtschaft auf den amerikanischen Markt angewiesen. Eine Nicht-Befolgung würde den amerikanischen Markt verschließen. Die Amerikaner machen das nicht nur mit Deutschland, sie machen es mit allen Ländern so. Nicht nur die USA haben derartige Regulierungen, auch andere Nationen haben solche, bzw. zum Teil noch viel extremere. Diese Länder sind von Ihrer Kultur und ihrem Empfinden für Demokratie und Freiheit aber auch noch meilenweit von den USA oder anderen westlichen Ländern entfernt.

Und so liefern wir ohne groß darüber nachzudenken Datensatz über Datensatz unserem NATO-Verbündeten nach Amerika. Mittlerweile geschieht dies schon aus Gewohnheit, unaufgefordert gehen wir unserem Trott und der neuen Gegebenheit nach. In unsere IT-Systeme haben wir diese Geschäftsprozesse schon längst eingebaut und den Vorgang bzw. die Transaktionen automatisiert. Wir denken nicht mehr darüber nach, was wir an Daten liefern. Wir wissen nicht genau was mit den Daten geschieht. Wir bekommen fast nie eine Rückmeldung, es sei denn etwas Schwerwiegendes ist falsch gelaufen.

SWIFT, C-TPAT und viele andere Verfahren, die Daten liefern – „so viele Daten, die kann doch niemand auswerten…“, hört man da oft.

Das ist leider völlig falsch. Diese „paar“ Hundertmillionen Datensätze können nach einer ersten groben Filterung in einfachster Weise in einigen wenigen Tagen von den Amerikanern ausgewertet werden. Und genau das passiert auch. Wenn der geneigte Leser sich die Tabelle der Computersysteme der NSA im Internet anschaut, dann gibt es sehr viele Systeme des Hochleistungscomputertyps namens CRAY. Als Verbund, und mit vorgeschalteten Vektorrechnern leisten diese Systeme Unvorstellbares.

Es ist das Groteskeste, was sich die deutsche Wirtschaft vorstellen kann. Wir liefern unseren Spionen die Daten, um uns auszuspionieren, um uns insgesamt wirtschaftlich zu schaden, um uns speziell finanziell zu schaden, um uns Marktanteile abzujagen, um uns Marktzugänge durch Patentstreitigkeiten verwehren zu lassen und um unserem Image zu schaden.

Seit einigen Jahren verstärkt sich der Trend massiv, zielgerecht spezielle Daten zu sammeln und auch teilweise der Öffentlichkeit zugänglich zu machen. Staatliche Stellen speichern enorme Mengen an Daten, aber auch privatwirtschaftliche Unternehmen speichern diese auf Anweisung des Staates oder aus eigenem Interesse (z.B. für statistische Zwecke).

Weltweit werden Datenbanken über viele Bereiche einer wirtschaftlichen Tätigkeit von Unternehmen angelegt, deren Daten nicht mehr der Kontrolle der betroffenen Betriebe unterliegen. Von staatlicher Seite hat dieser Trend seit den Ereignissen des 11. September 2001 an Fahrt aufgenommen.

Anstatt dafür zu kämpfen und teilweise sinnlose Datenerhebungen wieder rückgängig zu machen, erlegen uns unsere Verbündeten immer mehr neue Verfahren auf, an die wir uns halten sollen – immer im Namen des Kampfes gegen den Terror. Cecilia Malmström, die schwedische Europaabgeordnete, ist unter anderem dafür verantwortlich, die Anfragen zu bearbeiten. Aber sie kann sich offensichtlich nicht gegen die USA durchsetzen.

Sind gespeicherte Daten für interessierte Kreise von hohem Wert, so stellt sich weniger die Frage, OB als eher WANN diese Kreise Zugriff auf diese Daten erlangen. Trifft dies in gewissem Umfang auch auf die Privatwirtschaft zu, so ist es staatlichen Einrichtungen, wie Nachrichtendiensten, nochmals um vieles leichter, auf diese Daten zuzugreifen.

Dabei ist der Zugriff der Inlands-Dienste weniger bedenklich, als der Zugriff durch ausländische Nachrichtendienste oder ausländische Unternehmen. Dennoch können in den Inlandsdiensten Doppelspione oder einfach korrupte Personen sitzen, die für Geld die Informationen an die ausländischen Dienste weitergeben.

Können durch diese Zugriffe, sei es von staatlicher Seite oder von Seite der Privatwirtschaft, Erkenntnisse gewonnen werden, aus denen sich ein wirtschaftlicher Vorteil ergibt, so entsteht der ausgespähten Volkswirtschaft oder dem Unternehmen im Gegenzug mit hoher Wahrscheinlichkeit ein Schaden.

Nicht nur DAX-Unternehmen sind betroffen. Sehr oft sind es kleine Mittelständler, die ein stark gefragtes Gebrauchsprodukt bzw. ein High-Tech-Produkt herstellen. Prozentual ist die zweite Gruppe der Unternehmen am häufigsten betroffen. Der wirtschaftliche Schaden ist um ein Vielfaches höher als der durch Wirtschaftsspionage in den DAX-Unternehmen entstandener Schaden.

Eine Form der Spionage ist die Konkurrenzspionage bzw. Konkurrenzausspähung (es werden beide Ausdrücke verwendet). Sie ist die häufigste Form der Spionage und die lukrativste. Wurde hierzu vor 30 Jahren noch klassisch spioniert, man erinnere sich an die Minikameras in diversen „James Bond-Filmen“, so hat Intelligence Gathering diese Form stark verdrängt. Heute lässt sich der Spion von Welt die Daten liefern, binnen 24 Stunden, und dazu noch in dem Format, das er sich ausgedacht hat.

1.2 Zielsetzung

In diesem Buch soll durch theoretische Szenarien aufgezeigt werden, dass viele der Daten, die in Datensammlungen gespeichert sind, von Relevanz sind und zur Ausspähung genutzt werden können. Dazu werden stellvertretend für die gesamte Thematik vier Datenhalden ausgewählt und beschrieben. Auf diese aufbauend, werden Ausspähungsszenarien entwickelt, anhand derer untersucht wird, inwieweit die Daten der jeweiligen Datenbank zur Ausspähung genutzt werden können. Anschließend wird aufgezeigt, dass durch Verknüpfung der Datenbanken die Aussagekraft erhöht werden kann.

Zeigen die Szenarien, dass wirtschaftlich interessante Erkenntnisse gewonnen werden können, so ist es dringend erforderlich, dass Unternehmen beim Thema „Schutz vor Spionage“ nicht nur interne Daten berücksichtigen. Auch sollte Gegenstand der Betrachtung sein, welche Daten über das Unternehmen extern und ohne gewolltes Zutun gespeichert werden. Des Weiteren muss eine Abwägung stattfinden, welche dieser Daten für das Intelligence Gathering wie genutzt und somit gegen das Unternehmen Verwendung finden können. Ebenso ist zu betrachten, wer die Akteure des Intelligence Gathering aus Sicht des Unternehmens sein können. Die in diesem Buch beschriebenen Szenarien sollen dabei den Unternehmen als Leitfaden bei der Analyse behilflich sein. Die Aufarbeitung dieses noch kaum thematisierten Gebietes soll dazu beitragen, es auf die Tagesordnung der zuständigen Stellen in den Unternehmen zu bringen und den Schaden für Unternehmen zu verringern.

1.3 Abgrenzung

Es ist nicht Ziel dieses Buches, Szenarien zu entwerfen, die jeden möglichen Aspekt berücksichtigen. Es sollen aber sehr wohl die Möglichkeiten dargelegt werden, welche die ausgewählten und beschriebenen Datenhalden bieten. Auch soll nicht jeder nur erdenkliche Fall erörtert, sondern ein verständlicher Überblick geschaffen werden, der geeignet ist, dieses Gebiet zu thematisieren. Die Szenarien bei der Verknüpfung von Datenhalden (siehe Kapitel 7) sind mit Bedacht gewählt und beschränken sich darauf, erste Möglichkeiten der Verknüpfung aufzuzeigen. Es soll das Konzept der Verknüpfung und dessen Mehrwert skizziert werden.

Eine ausführliche Thematisierung, wer auf die ausgewählten Datenhalden schon heute oder auch in Zukunft Zugriff hat oder erlangen wird, soll nur in einem eingeschränkten Rahmen erfolgen. Es soll daraus hervorgehen, dass ein Zugriff prinzipiell denkbar ist bzw. schon stattfindet. In diesem Buch wird die Hypothese zu Grunde gelegt, dass es nur eine Frage der Zeit ist, bis interessierte Kreise Zugriff auf Daten erlangen (siehe Abschnitt 1.1), falls diese nur interessant genug sind. Diese Annahme wird in regelmäßigen Abständen durch diverse Berichte in Tageszeitungen gestützt, die über unrechtmäßigen Zugriff auf elektronische Informationen berichten.