WIS[sen]

SCHUTZ DURCH WISSEN

WIRTSCHAFTS- UND INDUSTRIESPIONAGE

DAS BULLETIN

AUSGABE 2/2014

IN DIESER AUSGABE

Der Faktor Zeit bei Geschäftsgeheimnissen

- Problematik der Definition
- Optimale Unternehmensstrukturen und –prozesse
- „best practice“ - Deutsche Telekom
- Informationen und Ausblick

BM.I

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES

Impressum:
Medieninhaber: Bundesministerium für Inneres, Generaldirektion für die öffentliche Sicherheit, 1014 Wien, Herrengasse 7, Telefon: +43 (0)1-53126-0, E-Mail: einlaufstelle@bmi.gv.at, www.bmi.gv.at
Inhaltlich verantwortlich: Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (.BVT), 1014 Wien, Postfach 100, Herrengasse 7, Telefon: +43 (0)1-53126-4100, E-Mail: WIS@bvt.gv.at
Gestaltung: Bundesministerium für Inneres, Abteilung I/8 - Protokoll und Veranstaltungsmanagement

WKO WIRTSCHAFTSKAMMER ÖSTERREICH

FH CAMPUS WIEN UNIVERSITY OF APPLIED SCIENCES

iv INDUSTRIELLEN VEREINIGUNG

WIRTSCHAFTS- UND INDUSTRIESPIONAGE

Sehr geehrte Damen und Herren,

bereits seit mehr als 100 Jahren stellen sich Expertinnen und Experten die Frage nach der Abgrenzung von Geschäfts- und Betriebsgeheimnissen gegenüber sonstigen Tatsachen eines Unternehmens. Im Rahmen der Strafverfolgung von Fällen der Wirtschafts- und Industriespionage kommt es bei dieser Diskussion zum Teil zu, für die betroffenen Unternehmen, nicht zufriedenstellenden Ergebnissen. Vielfach liegt ein unterschiedliches Verständnis darüber vor, inwiefern Tatsachen bzw. Informationen in einem Unternehmen tatsächlich geheim sind, dh. einem sehr begrenzten Personenkreis zugänglich sind, und ein Geheimhaltungsinteresse im Rechtssinn an dieser Tatsache besteht. Ein objektives Geheimhaltungsinteresse ist bei all jenen Tatsachen zu bejahen, durch deren Offenbarung dem Unternehmen ein materieller oder immaterieller Schaden und sohin eine Schlechterstellung im Wettbewerb drohen könnte. Die tatsächliche Kalkulation des potentiellen Schadens fällt jedoch sehr schwer, wodurch die Nachvollziehbarkeit der Schädigung des von Geheimnisverrat betroffenen Unternehmens wesentlich verringert wird.

Entsprechende rechtliche Rahmenbedingungen für den Schutz geistigen Eigentums sind für die Innovationstätigkeiten von Unternehmen jedoch von großer Bedeutung. Geschäfts- und Betriebsgeheimnisse schützen Wissen, aber an sie kann bzw. soll kein Exklusivrecht anknüpfbar sein, da dies zu Wettbewerbsbeschränkungen führen würde. Eben dieses Streben nach wettbewerbsfördernden bzw. innovationsfördernden Rahmenbedingen veranlasste die EU im Jahr 2013 zur Vorlage eines Richtlinienvorschlages[1] über den Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung. Neben einer EU-weiten einheitlichen Definition eines Geschäftsgeheimnisses sollen vor allem die Vorschriften zur Wahrung der Vertraulichkeit von Geschäftsgeheimnissen während und nach Gerichtsverfahren vereinheitlicht bzw. gestärkt werden. Denn der befürchtete Reputationsverlust stellt für ein geschädigtes Unternehmen das Hauptargument für die Nichtmeldung von Vorfällen des Diebstahls oder Ausspähens von Geschäftsgeheimnissen dar.

Im Regelfall stellt der Verlust von Geschäftsgeheimnissen eine langfristige Beeinträchtigung der Wettbewerbsfähigkeit des betroffenen Unternehmens dar. So entfallen insbesondere bei Innovationen die „First-Mover“ Renditen und es kommt durch den Nichtausgleich der Forschungs- und Entwicklungskosten (FuE Kosten) zu einer wesentlichen Schwächung des Gesamtunternehmens. Im Falle zeitlich begrenzter Geschäftsgeheimnisse, wie beispielsweise Angebotsspezifikationen im Zusammenhang mit Ausschreibungen, Höchstgebote bei Auktionen sowie Vertragsverhandlungen über Unternehmenskooperation, hat die rechtswidrige Offenlegung der geheimen Informationen ebenso einen Umsatzverlust zur Folge.

OPTIMALE UNTERNEHMENSSTRUKTUREN UND –PROZESSE

Optimaler Schutz heißt nicht nach 100% Schutz zu streben, sondern das Wissen darüber, was wie geschützt werden muss.

Entscheidend ist die richtige Einordnung von Informationen. Die Wahrnehmung von FuE Informationen sowie von Produktionsvorgängen als Geschäftsgeheimnisse ist grundsätzlich stärker ausgeprägt. Zudem werden Informationsschutzkonzepte und Risikomanagementmodelle zumeist für geheimes Know-how generell herangezogen.

Die Bewertung von Informationen in aktuellen Geschäftsvorgängen wird jedoch oftmals ausschließlich in Bezug auf technische Schutzmaßnahmen vorgenommen, ohne nicht-technische Schutzmaßnahmen – beispielsweise im Rahmen einer Information Security Policy – ebenfalls entsprechend umzusetzen.

Im Programm „TBS – Top Business Secrets“ der Deutschen Telekom bedeutet dies die Konzentration auf den Schutz der Geschäftsgeheimnisse mit besonders hohem Schadenspotential bei Vertraulichkeitsverlust, insbesondere im Zusammenhang mit aktuellen Geschäftsvorgängen. Im Falle der Deutschen Telekom wurde für die Einstufung als TBS ein Ansatz von mehreren Millionen Euro als potentielle Verlusthöhe gewählt. Die Bewertung und Kategorisierung von Informationen als TBS im Rahmen eines Geschäftsvorgangs obliegt dem sogenannten TBS Identifier. Weiters gibt es die Rolle des TBS-Owners, dies sind potentiell alle Mitglieder der Geschäftsführung und deren Direct-Reports, den Counter Espionage Officer / Spionageabwehrbauftragten welcher von der Geschäftsleitung mit Zustimmung des Sicherheits-Chefs benannt wird, sowie das Center of Excellence als jene Einheit, die den Gesamtprozess verantwortet.

Programm TBS—Verantwortlichkeiten

- TBS-Owner
- TBS-Identifier
- Counter Espionage Officer / Spionageabwehrbeauftragter
- Center of Excellence

Im Anschluss an die organisatorische Maßnahme der Benennung der Verantwortlichkeiten im TBS-Prozessmodell wird, entsprechend der Ergebnisse der durch den Spionageabwehrbeauftragten durchgeführten Risiko- und Bedrohungsanalyse, die Auswahl der technischen und / oder der nicht-technischen Schutzmaßnahmen aus der „Toolbox“ vorgenommen.

Diese „Toolbox“ beinhaltet beispielsweise speziell gehärtete bzw. verschlüsselte Hardware (Laptop, Crypto-Handy) im Bereich der technischen Maßnahmen, sowie spezielle Social Engineering Awareness-Programme, Informationsflyer für unterschiedliche interne Bedarfsträger, Labeling und spezielle physikalische und logische Zugangsbegrenzungen zu Projekträumen als besondere nicht-technische Maßnahmen.

Labeling – mittels digitaler Wasserzeichen in Dateien können diese bis zu ihrer Urheberin / ihrem Urheber rückverfolgt werden, und somit eine unberechtigte Weitergabe nachgewiesen werden.

Die Verantwortung der Identifizierung von Informationen, die als geheim einzustufen sind muss bei der / dem – für Bedrohungen durch Wirtschafts- und Industriespionage sensibilisierten – fachlich zuständigen Mitarbeiterin / Mitarbeiter liegen. Die Berücksichtigung der fachabteilungsübergreifenden Tätigkeit einer / eines Sicherheitsverantwortlichen – im TBS-Programm der / des Spionageabwehrbeauftragten – muss in den Unternehmensprozessen erfolgen, um die tatsächliche Entlastung einzelner Trägerinnen / Träger eines Geschäftsgeheimnisses zu erreichen. Denn wenngleich es logisch erscheint, im Rahmen eines entscheidenden Geschäftsprozesses mit technischen Schutzmaßnahmen wie Crypto-Handys und stand alone PCs zu arbeiten und zu kommunizieren, so werden die Annehmlichkeiten eines Smartphones sowie der verfügbaren Apps im Regelfall dennoch schmerzlich vermisst. Neben der Wertehaltung eines Unternehmens, sowie der Kommunikation dieser verbindlichen Werte, kann eine „Toolbox“ sowie die mit deren Befüllung verbundene Verantwortung einer Stelle bzw. Person zur tatsächlichen Entlastung und Akzeptanz, durch die Unternehmensangehörigen, ein wichtiges Element darstellen.

Durch Meldungen von Verdachtsmomenten bzw. kritischer Situationen in Bezug auf Wirtschafts- und Industriespionage im In– oder Ausland ist es dem .BVT als kompetentem und vertrauenswürdigem Ansprechpartner möglich, Risikoprofile zu erstellen und dadurch aktuelle Trends aufzuzeigen.

Entscheidend ist die Wahrnehmung von Sicherheit als Unternehmenswert. Im Falle der Deutschen Telekom bedeutet dies, dass das TBS-Schutz Konzept bzw. die Elemente der „Toolbox“ von den internen Kundinnen / Kunden gerne angenommen werden, da sofort anwendbare Lösungen bereitgestellt werden, und die Risiken des Verlust geheimer Informationen durch Wirtschafts- oder Industriespionage deutlich minimiert werden. „Die Methode wie diese Geheimnisse geschützt werden ist nichts Geheimes, nur die technischen Details. Hiervon sollen auch mittelständische Unternehmen profitieren können.“, meinte Thomas Königshofen, der Konzern-Sicherheitsbevollmächtigte der Deutschen Telekom, während seines Vortrags im Rahmen des Lehrgangs WIS-M im Jänner 2014 in Wien. Daher hat die Deutsche Telekom in einem Pilotprojekt das TBS-Konzept bereits auf ein deutsches Mittelstandsunternehmen erfolgreich umgelegt.

AUSBLICK

Der Umgang mit persönlichen Informationen und deren Verfügbarkeit in sozialen Medien bietet Akteuren des Social Engineerings eine Fülle an Angriffsmöglichkeiten. Die **Ausgabe 1/2015** enthält nützliche Informationen sowie Expertenmeinungen zu diesem Thema.

KONTAKT

Für weiterführende Informationen und im Anlassfall steht Ihnen das .BVT zur Verfügung:

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

E-Mail: wis@bvt.gv.at
Telefon: +43-(0)1-53126-4100

http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis

VERANSTALTUNGEN

- **D.A.CH Security 2014**
  16. und 17. September 2014 in Graz
  Übersicht über den aktuellen Stand der IT-Sicherheit

Freigabe der in diesem Bulletin enthaltenen Informationen zum TBS-Konzept der Deutschen Telekom durch Thomas Königshofen, Konzern-Sicherheitsbevollmächtigter der Deutschen Telekom.

[1] COM(2013) 813 final, vom 28.11.2013 – Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.