Vol. 21 – Juli 19

ip Competence

Themenjournal für geistiges Eigentum

Geschäftsgeheimnisse – ein zentrales Compliance-Thema

Christoph Haid/Michael Lindtner

Geschäftsgeheimnisse – ein zentrales Compliance-Thema

Christoph Haid und Michael Lindtner

Geschäftsgeheimnisse sind für die Wettbewerbsfähigkeit von Unternehmen oft von zentraler Bedeutung. Wie sollen diese aber wirksam geschützt werden? Was tun, wenn der Verdacht besteht, dass Geheimnisse weitergegeben worden sind? Der vorliegende Beitrag zeigt auf, welche Aspekte hier im Rahmen von Compliance-Maßnahmen zu beachten sind.

I. Einleitung

Die Wichtigkeit von Geschäftsgeheimnissen ist unbestritten. Unternehmen suchen laufend nach Möglichkeiten, ihre Position am Markt durch Innovation zu verbessern. Bahnbrechende Ideen, Entwicklungen, Rezepturen und Formeln, Softwarelösungen und Algorithmen entscheiden über wirtschaftlichen Erfolg oder Misserfolg. Ihre ungewollte Veröffentlichung oder Weitergabe ist daher für das betroffene Unternehmen oft existenzgefährdend.

Auch der europäische Gesetzgeber hat dies erkannt und mit der „GeschäftsgeheimnisRL“[1] Vorschriften zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb, rechtswidriger Nutzung und rechtswidriger Offenlegung erlassen. Unternehmen müssen allerdings „angemessene Geheimhaltungsmaßnahmen“ treffen, um in den Genuss des Geheimnisschutzes zu kommen.

Der Schutz von Geschäftsgeheimnissen ist daher eine zentrale Compliance-Aufgabe jedes Unternehmens. Sowohl die GeschäftsgeheimnisRL als auch ihre Umsetzung in Österreich lassen aber offen, was unter „angemessenen Maßnahmen“ zu verstehen ist. Nachfolgend sollen daher die wesentlichen Eckpfeiler eines effektiven Geschäftsgeheimnisschutzes dargestellt werden.

II. Eckpfeiler eines wirksamen Geheimnisschutzes

Zwei wesentliche Missverständnisse gleich vorweg:

Erstens, effektiver Geheimnisschutz ist mehr als reines Schutzrechtsmanagement. Kommerzielle und technische Geschäftsgeheimnisse sind einem Schutzrecht nämlich oft nicht zugänglich. Zudem dauert die Erteilung eines Schutzrechts teilweise zu lange bzw ist der gewährte Schutz oft auch geographisch nicht weitreichend genug.

Zweitens, effektiver Geheimnisschutz ist mehr als nur die Abwehr externer Zugriffsversuche. Die Mehrheit der unfreiwilligen Know-how-Verluste geht nämlich nach mehreren Studien auf die eigenen Mitarbeiter zurück.

„EFFEKTIVER GEHEIMNISSCHUTZ IST MEHR ALS NUR DIE ABWEHR EXTERNER ZUGRIFFSVERSUCHE. DIE MEHRHEIT DER UNFREIWILLIGEN KNOW-HOW-VERLUSTE GEHT AUF DIE EIGENEN MITARBEITER ZURÜCK."

Angesichts dessen erfordert wirksamer Schutz von Geschäftsgeheimnissen einen Mix aus juristischen, organisatorischen und technischen Maßnahmen. Der Schutz von Geschäftsgeheimnissen als „Kronjuwelen“ eines Unternehmens muss für alle Mitarbeiter zur Selbstverständlichkeit werden. Das sicherste IT-System hilft nichts, wenn Mitarbeiter in der Öffentlichkeit für Dritte wahrnehmbar über die jüngsten Forschungs- & Entwicklungsarbeiten diskutieren oder wenn Geschäftspartner bei Werksbesichtigungen Prototypen oder neue Entwicklungen unbeaufsichtigt begutachten können. Strenge interne Vorschriften sind nutzlos, wenn Dritte an strategischen Projekten mitarbeiten und die Zusammenarbeit nicht vertraglich geregelt ist oder die Verträge keine wirksamen Vertraulichkeitsvereinbarungen enthalten.

Unabhängig von ihrer Größe sind Unternehmen daher gut beraten, die folgenden Maßnahmen ergreifen, um ihre Geschäftsgeheimnisse zu schützen.

1 RL (EU) 2016/943 des Europäischen Parlaments und des Rates vom 08.06.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl L 157/1.

INTERNE INFORMATION

A. Klassifizierung und Identifizierung von Geschäftsgeheimnissen

Alle Unterlagen und Informationen im Unternehmen sollten in „Öffentlich“, „Vertraulich“ oder „Geheim“ eingestuft werden:

- „Öffentlich“ sind jene Informationen, die bereits öffentlich zugänglich sind oder deren Veröffentlichung gesetzlich erforderlich ist oder die Position des Unternehmens stärken können.

- „Vertraulich“ sind jene Informationen, die sich entweder nur an einen bestimmten Personenkreis richten oder die gesetzlich geschützt sind. Ihre Weiterleitung ist entweder gesetzlich verboten oder schädigt das Unternehmen. Eine Weitergabe erfolgt nur auf „Need to Know“-Basis, also nur, wenn der Empfänger die Informationen kennen muss oder soll.

„UNTERNEHMEN SOLLTEN KLARE INTERNE REGELN SCHAFFEN, WIE MIT GESCHÄFTS-GEHEIMNISSEN UMZUGEHEN IST UND WELCHE PERSONEN UNTER WELCHEN UMSTÄNDEN ZUGRIFF DARAUF HABEN."

- „Geheim“ sind jene vertraulichen Informationen, bei denen der Empfänger nicht einmal nach dem „Need to Know“-Prinzip entscheiden kann, an wen er diese weiterleitet, sondern die von vornherein nur einem klar definierten, eingeschränkten Personenkreis bekannt sein dürfen.

Im zweiten Schritt sind die Geschäftsgeheimnisse zu identifizieren und katalogisieren.

B. Regeln für den Umgang mit Geschäftsgeheimnissen

Der ordnungsgemäße Umgang mit Geschäftsgeheimnissen umfasst die folgenden Aspekte:

- Es muss definiert werden, wer über die Einstufung von Informationen entscheidet und den Empfängerkreis geheimer Informationen festlegt; insb in kleineren Unternehmen ist das regelmäßig ein Mitglied der Geschäftsführung.

- Geheimnisträger müssen bestimmt und der Umgang mit Geschäftsgeheimnissen klar geregelt werden. Das beinhaltet ein stringentes Konzept insb für Zugriff, Offenlegung, Druck, Kopieren und Versenden von vertraulichen und geheimen Informationen.

- Werden Geschäftsgeheimnisse in Papierform extern versendet, sollte dies per Kurier erfolgen. Das Versenden innerhalb des Unternehmens hat in entsprechend gekennzeichneten Umschlägen zu erfolgen. Alle vertraulichen und geheimen Unterlagen sind bei Verlassen des Arbeitsplatzes zu versperren. Auch beim Entsorgen von Unterlagen ist mit entsprechender Sorgfalt vorzugehen.

- Werden Geschäftsgeheimnisse per E-Mail versendet, sollte die E-Mail verschlüsselt werden. Beim Speichern elektronischer Unterlagen sind Zugriffsbeschränkungen einzuführen und Dateien mit einem Passwort zu schützen.

C. IT-Sicherheit

Das IT-System eines Unternehmen muss ausreichend vor unerlaubten Zugriffen und Datenverlusten schützen. Effektive IT-Sicherheit beinhaltet folgende Features:

- Eine Datensicherungsstrategie, die entsprechende Sicherungstechnologie, die Definition von Zeitpunkt und Intervallen von Sicherungen, die Festlegung der Anzahl und Aufbewahrungsorte der Backup-Datenträger sowie Überprüfungen und Wiederherstellungstests.

- Technische Früherkennungssysteme, um das Kopieren großer Datenmengen oder den Einsatz bestimmter Software zu erkennen.

- Virenscanner und Firewalls auf allen Geräten, um Schadsoftware abzuwehren.

- Verschlüsselte bzw vollständig verschlüsselte Verbindungen für das Surfen im Internet, sowohl im Local Area Network als auch in drahtlosen Netzwerken.

- Festlegen von Sicherheitsstandards für die Nutzung betriebseigener und betriebsfremder mobiler Endgeräte (Laptops, Tablets, Smartphones) und Regeln für das Speichern von Unternehmensdaten auf unternehmensfremden Geräten.

- Verhaltensregeln für Mitarbeiter und der Einsatz von Sicherheitsprogrammen.

- Regelmäßige Mitarbeiterinformation über neue Gefahrenquellen, um zu verhindern, dass Dritte mit Spam- oder Phishing-Mails, mit Schadsoftware verseuchten Nachrichten oder mittels Social Engineering („Human Hacking“) an Passwörter, persönliche Daten oder vertrauliche Informationen gelangen.

- Laufendes Einspielen von Softwareupdates und Überprüfen des IT-Systems auf Aktualität, Angemessenheit und Effektivität. Dabei empfiehlt es sich, sich an vorhandenen Standards zu orientieren: Eine der bekanntesten Normen ist der Standard 27001 der International Standard Organisation („ISO“), der auch im Österreichischen Informationssicherheitshandbuch[2] abgebildet ist.

D. Sicherheitskonzept und Werkschutz

Geheimnisschutz setzt auch den Schutz der Unternehmensräumlichkeiten vor unbefugtem Zutritt voraus. Gäste mit Zugang zu sensiblen Bereichen müssen daher überprüft und kritische Unternehmensbereiche (zB die F&E-Abteilung) laufend überwacht werden.

Für Werksbesichtigungen sind Regeln für den Empfang und das Begleiten der Besucher zu erstellen und einzuhalten, um das Offenbaren von Geschäftsgeheimnissen oder Einblicke in geheime Unterlagen oder Projekte zu verhindern.

E. Geheimnisschutz in Verträgen

Bei der Zusammenarbeit mit Geschäftspartnern sind vorbeugende Schutzrechtsanmeldungen, strenge Vertraulichkeitsvereinbarungen und das Offenlegen geheimer Informationen nur auf „Need to Know“-Basis ratsam, um den Abfluss von Geschäftsgeheimnissen zu verhindern. Bei der Auswahl von Kooperationspartnern ist, neben den zu erwartenden Kosten, auch deren generelle Vertrauenswürdigkeit zu berücksichtigen. Die zentralen Informationen, die im Unternehmen bleiben müssen, sind vorab zu identifizieren und zu schützen. Auch empfiehlt es sich, bei Forschungs- & Entwicklungskooperationen die gemeinsamen Arbeitsstätten von der eigenen F&E-Abteilung zu trennen.

Auch wenn arbeitsrechtlich nicht zwingend, sind Vertraulichkeitsvereinbarungen mit den Mitarbeitern sinnvoll. Vertraulichkeitsvereinbarungen flankieren die sonstigen Schulungsmaßnahmen. Gleichzeitig instruieren sie Mitarbeiter nochmals, den Geheimnisschutz ernst zu nehmen und können auch die Grundlage für rechtliche Schritte im Fall des Geheimnisverrats darstellen. Wenn Mitarbeiter befördert werden, sollten Unternehmen zudem prüfen, ob die bestehende Vertraulichkeitsvereinbarung der neuen Position gerecht wird und diese gegebenenfalls anpassen. Empfehlenswert sind auch nachvertragliche Verschwiegenheitsklauseln.

„ALLE ZENTRALEN REGELN FÜR DEN UMGANG MIT GESCHÄFTSGEHEIMNISSEN MÜSSEN IM UNTERNEHMEN KOMMUNIZIERT WERDEN UND VERBINDLICH SEIN. DER SCHUTZ VON GESCHÄFTSGEHEIMNISSEN MUSS FÜR ALLE MITARBEITER SELBSTVERSTÄNDLICH SEIN"

F. Compliance-Dokumentation und Compliance Management System

Alle zentralen Regeln für den Umgang mit Geschäftsgeheimnissen müssen schriftlich festgehalten und im Unternehmen kommuniziert werden. Sie sollten auch im Intranet abgelegt werden und leicht auffindbar sein. Zudem muss darauf geachtet werden, dass die im Unternehmen aufgestellten Regeln auch (rechts-)verbindlich sind.

Um das Bewusstsein für die Wichtigkeit des Geheimnisschutzes weiter zu schärfen, sollten die betroffenen Personen auch laufend über den richtigen Umgang mit Geschäftsgeheimnissen geschult und über Entwicklungen (zB der Internetkriminalität) informiert werden.

Selbst die besten Regeln und Schulungen helfen aber wenig, wenn nicht zwei Voraussetzungen erfüllt sind:

- Die Geschäftsführung muss den richtigen Umgang mit Geschäftsgeheimnissen vorleben. „Tone from the Top“ und „Leading by Example“ sind essentiell, um die Compliance-Anstrengungen im Unternehmen nicht zu untergraben. Die Geschäftsleitung muss sich zum Schutz der Geschäftsgeheimnisse bekennen, die Regeln vorexerzieren und Verstöße angemessen verfolgen.

2 Abrufbar auf der Webseite des Bundeskanzleramts https://www.sicherheitshandbuch.gv.at/.

„DIE GESCHÄFTSFÜHRUNG MUSS DEN RICHTIGEN UMGANG MIT GESCHÄFTSGEHEIMNISSEN VORLEBEN. ‚TONE FROM THE TOP' UND ‚LEADING BY EXAMPLE' SIND ESSENTIELL, UM DIE COMPLIANCE-ANSTRENGUNGEN IM UNTERNEHMEN NICHT ZU UNTERGRABEN."

- Die Einhaltung der Vorschriften muss laufend kontrolliert werden. Werden dabei Lücken im System aufgedeckt, sind diese zu schließen. Zeigt sich, dass die Regeln missverständlich sind, sind sie zu verbessern.

III. Interne Untersuchung bei Verdacht des Geheimnisverrats

A. Einleitung

Die möglichen Schäden für Unternehmen durch den Verlust von Geschäftsgeheimnissen sind enorm. Bei einem Unternehmen sollten daher die Alarmglocken schrillen, wenn es Hinweise auf grundlose, ungewöhnliche Arbeitszeiten gibt, wenn berufliche E-Mails regelmäßig an private Adressen weitergeleitet, große Datenmengen en bloc heruntergeladen oder Akten ohne ersichtlichen Anlass mit nach Hause genommen werden.

Bei einem begründeten Verdacht des Geheimnisverrats ist Eile geboten. Im Idealfall kann die Verbreitung eines Geschäftsgeheimnisses verhindert bzw dessen Verwendung gestoppt werden. Jedenfalls geht es um Schadensbegrenzung und die Vorbereitung von arbeits-, zivil- und/oder strafrechtlichen Schritten.

Vor diesem Hintergrund empfiehlt es sich, Notfallpläne vorzubereiten. Diese Pläne geben vor, wer über den Verdacht zu informieren ist, welche externen Personen hinzuzuziehen sind und wo sich die relevanten Daten und Informationen befinden. So kann im Ernstfall vermieden werden, dass wichtige Zeit verloren geht oder in der Aufregung die falschen Schritte gesetzt werden.

Bei internen Untersuchungen zu einem möglichen Geheimnisverrat ist eine Vielzahl von Fallgestaltungen möglich. Meist sind die Untersuchungen delikat, insb wenn sie sich gegen führende Mitarbeiter richten. Bei den Ermittlungen ist daher besondere Diskretion angesagt, dennoch aber Eile geboten. Andernfalls besteht die Gefahr, dass wichtige Unterlagen manipuliert und die Verdächtigen gewarnt werden.

„INTERNE NOTFALLPLÄNE FÜR DEN FALL DES GEHEIMNISVERRATS KÖNNEN ERHEBLICH ZUR SCHADENSBEGRENZUNG BEITRAGEN."

B. Wesentliche Schritte einer internen Untersuchung

INTERN

1. Untersuchungsplan

Zu Beginn ist ein Untersuchungsplan zu erstellen. Er soll alle über den Vorfall bekannten Informationen, die verdächtigen Personen und die möglichen Rechtsverletzungen enthalten. Das Untersuchungsteam, die Kommunikation innerhalb des Teams und die Berichtswege innerhalb des Unternehmens sind mit Bedacht auszuwählen und festzuhalten.

Darüber hinaus sind der Untersuchungsgegenstand und die Ziele der Untersuchung zu formulieren (zB Strafanzeige, zivilrechtliche Schritte [Unterlassung, Verwertungsverbot, Herausgabe, Schadenersatz etc] und arbeitsrechtliche Schritte [Abmahnung, Kündigung, Entlassung etc]) und die dafür benötigten Ressourcen zu benennen. Es sollten auch ein Zeitplan aufgestellt sowie die Reihenfolge der Untersuchungsschritte und eine grobe Vorgehensstrategie festgelegt werden.

2. Sicherung von Daten und Dokumenten

Sobald der Entschluss gefasst ist, eine interne Untersuchung einzuleiten, ist es ratsam, sämtliche relevanten elektronischen Unterlagen zu sichern, um diese vor Zerstörung und Manipulation zu schützen. Dabei sind die datenschutzrechtlichen Grenzen zu beachten.

3. Durchsicht der Daten

Das Durchsuchen von E-Mails kann Aufschluss darüber geben, ob die Verdachtspersonen um den Zeitpunkt des Datentransfers herum mit den Empfängern in Kontakt standen. Mit diesen Erkenntnissen können die Verdächtigen dann konfrontiert werden.

Die Auswertung betrieblicher E-Mails hat im Einklang mit datenschutzrechtlichen Vorgaben zu erfolgen. In diesem Zusammenhang ist vorab zu eruieren, ob den Mitarbeitern die private Nutzung des betrieblichen E-Mail-Systems erlaubt bzw ob es eine Betriebsvereinbarung gibt, welche die begründete Sichtung von E-Mails vorab genehmigt.

Es ist ratsam, bei der Auswertung elektronischer Daten mit forensischen Experten zusammenzuarbeiten. Insb bei großen Datenmengen erleichtern technische Hilfsmittel die Suche nach belastendem Material enorm. EDV-Spezialisten können oft auch verloren geglaubte Daten und E-Mails wiederherstellen sowie Informationsabflüsse rekonstruieren und dokumentieren.

4. Befragung von Mitarbeitern und anderen Informationsquellen

Untersuchungen zu einem möglichen Geheimnisverrat sind häufig mit einer großen Anzahl möglicher Informationsquellen konfrontiert, insb wenn der Zugriff auf das fragliche Geschäftsgeheimnis nicht beschränkt war. Neben den unmittelbaren Verdächtigen sind auch – soweit möglich und zielführend – ehemalige Kollegen und Geschäftspartner zu befragen. Die Weitergabe von Geschäftsgeheimnissen ist oft auch Ausfluss eines internen Machtkampfs oder von Spannungen innerhalb des Unternehmens. Insofern dürfen widersprüchliche Aussagen und gegenseitige Anschuldigungen die Interviewer nicht verwundern. Jedenfalls sind die Gesprächspartner zu strikter Verschwiegenheit zu verpflichten. Die Befragungen und Gespräche sind zu protokollieren.

Sofern ein Mitarbeiter den Diebstahl oder die Weitergabe gesteht, sind durch geeignete Maßnahmen (zB Mitarbeiteramnestie) die weitere Kooperation in der Aufarbeitung des Falls und, wenn möglich, die Rückgabe der entwendeten Daten oder das Bereitstellen von privaten Geräten für weitere Untersuchungsschritte sicherzustellen.

5. Abschlussbericht

Der Untersuchungsbericht ist das (vorläufige) Ende der Untersuchung. Dieser enthält insb eine chronologische Auflistung der Untersuchungsmaßnahmen sowie eine rechtliche Bewertung und einen Vorschlag für weitere interne und externe Schritte.

6. Konsequenzen

Haben sich im Rahmen einer internen Untersuchung die Vorwürfe gegenüber Mitarbeitern oder Dritten erhärtet, müssen die erforderlichen Konsequenzen gezogen werden. Diese Schritte können eine Strafanzeige, zivilrechtliche Schritte und/oder Disziplinarmaßnahmen umfassen.

Unabhängig davon, ob die Untersuchungsergebnisse ausreichen, um weitere rechtliche Schritte gegenüber Dritten zu setzen, sollten die Erkenntnisse jedenfalls verwendet werden, um die Compliance-Prozesse zu verbessern und Lücken im System zügig zu schließen.

IV. Zusammenfassung – Checkliste für effektiven Geheimnisschutz

- Ist klar, welche schutzwürdigen Geschäftsgeheimnisse vorhanden sind? Bestehen interne Vorschriften, wie mit diesen umzugehen ist?
- Sind die Personen, die auf die Geschäftsgeheimnisse zugreifen dürfen, definiert und werden Zugriffe protokolliert?
- Sind die Geschäftsgeheimnisse durch technische Lösungen ausreichend geschützt?
- Sind alle relevanten Mitarbeiter über den Umgang mit Geschäftsgeheimnissen geschult? Enthalten ihre Verträge ausreichende Vertraulichkeitsvereinbarungen und sind die aufgestellten Verhaltensregeln auch verbindlich?
- Bestehen effektive Vertraulichkeitsvereinbarungen in Verträgen mit Geschäftspartnern?
- Gibt es Notfallpläne, um beim Verdacht eines Geheimnisverrats unverzüglich reagieren zu können?
- Wenn ein möglicher Geheimnisverrat untersucht werden muss:
  - Wer soll untersuchen und wer muss von der Untersuchung wissen?
  - Welches Ziel verfolgt die Untersuchung?
  - Wo und wer muss untersucht werden?
  - Welche Daten- und Informationsquellen werden verwendet?
  - Welche rechtlichen und faktischen Grenzen gibt es?
- Werden nach der Untersuchung die erforderlichen externen (Strafanzeige, zivilrechtliche Schritte, arbeitsrechtliche Maßnahmen) und internen (Verbesserung des Systems) Schritte gesetzt?