Industrie- und Handelskammer
zu Dortmund

Merkblatt "Wirtschaftsspionage"

Kontakt: Ass. Jost Leuchtenberg, j.leuchtenberg@dortmund.ihk.de **(Stand: Januar 2025)**

1 Allgemeines

Wirtschaftsspionage ist nicht nur ein Thema für spannende Unterhaltungsliteratur. Wirtschaftsspionage ist auch längst nicht nur ein Problem für international agierende Konzerne bzw. Großunternehmen. Gerade der „Diebstahl“ von Know-how kann heute fast jeden Teilnehmer am Wirtschaftsleben treffen, markenstarke Konsumgüterhersteller ebenso wie Hightech-Entwickler oder Pharmaforscher. Als Gefahr für Unternehmen gewinnt sie vor dem Hintergrund der Globalisierung und steigenden Wettbewerbs sogar noch an Bedeutung, denn Spionage „spart“ Zeit sowie Forschungs- und Entwicklungskosten. Wirtschaftskriminelle Ausforschung kann den gesamten Lebenszyklus eines Produkts – von Forschung und Entwicklung über Produktion bis hin zur Vermarktung – betreffen. Nicht wenige Unternehmen haben bereits detailgetreue Plagiate ihrer Maschinen und Anlagen auf Fachmessen im Ausland entdeckt. Ist das Plagiat zudem von schlechter Qualität, beeinträchtigt dies zusätzlich den guten Ruf des Originals. Jedenfalls aber mindert der zumeist viel niedrigere Preis der „Kopie“ die Konkurrenzfähigkeit des Originals. Die Folgen sind also gravierend. Steht somit fest, dass die Gefahr von Wirtschaftsspionage nicht zu unterschätzen ist, stellt sich die Frage, wie diese erkannt und möglichst verhindert werden kann.

2 Spionage im Wandel

Zu den Arbeitsmethoden von Nachrichtendiensten gehört schwerpunktmäßig die – sowohl offene als auch konspirative bzw. verdeckte – Informationsbeschaffung. Aggressives Vorgehen bei der „Rekrutierung“ von Agenten, etwa durch Erpressung/Nötigung, existiert zwar auch heute noch, ist aber zunehmend dem Prinzip der freiwilligen Mitarbeit gewichen. Informationen werden möglichst offen beschafft. Dies senkt auch das Risiko der Entdeckung. Weltweit zugängliche Datenbanken, Gespräche bei Tagungen, Messen, Botschaftsempfängen usw. bieten einen großen Informationsfundus. Parallel gewinnt die Auswertung „offener" Quellen an Bedeutung. Hierzu zählen etwa die systematische Erfassung von wissenschaftlichen Forschungsberichten, Diplomarbeiten sowie das Auswerten von Fachliteratur und Werbe- bzw. Informationsmaterial. Zudem ist heute die Übermittlung geheimer Nachrichten über das Internet und mithilfe anderer elektronischer Datenübermittlungsverfahren wesentlich schneller und vor allem risikoärmer möglich. Datenträger sind auf Knopfdruck genauso schnell beschrieben wie gelöscht. Spuren und Beweismittel bleiben kaum zurück. Die global über Satelliten abgewickelte Kommunikation ist vor fremdem Zugriff nur selten geschützt und kann gezielt und unbemerkt abgehört werden. Dennoch können Nachrichtendienste auf menschliche Quellen nicht vollständig verzichten, denn einen „Agenten im Zielobjekt” kann die elektronische Aufklärung allein nicht ersetzen.

Neben der Recherche im Internet und mittels anderer öffentlich zugänglicher Informationsquellen ist die gezielte Verbindungsaufnahme zu Tagungsteilnehmern, Messebesuchern und Ausstellern eine häufig eingesetzte Methode der Informationsbeschaffung. Aus zunächst fachbezogenen, unverfänglich wirkenden Gesprächen sollen vertrauensvolle Beziehungen entstehen. Aber nicht nur von Unternehmensfremden geht Gefahr aus. Eine sogar noch akutere Gefahrenquelle für den ungewollten Abfluss von Know-how stellen „Innentäter“ dar. So hat sich herausgestellt, dass gerade kurzzeitig tätige Praktikanten und Hospitanten relativ mühelos umfangreiches Datenmaterial aus Firmennetzen kopieren und über das Internet ins Ausland transferieren konnten.

3 Abwehr von Wirtschaftsspionage / Sicherheitskonzept

Technischer Schutz ist absolut notwendig – auch er schützt aber nicht sicher vor menschlichen Fehlern. Wenn Unternehmen bemerken, dass vertrauliche Daten bei der Konkurrenz bekannt geworden sind, stellt sich immer wieder heraus, dass Nachlässigkeiten oder sogar absichtlicher Verrat die Ursache für den ungewollten Informationsabfluss bilden. Daher sollten das Wissen der Mitarbeiter, das Bewusstsein um die Gefahren der Spionage und die Schutzmöglichkeiten im Sicherheitssystem eines Unternehmens einen besonders wichtigen Baustein bilden.

Prävention muss professionell betrieben und von Führungskräften verantwortet werden. Der Aufbau eines effizienten Sicherheitskonzepts beginnt mit einer gezielten Risiko- und Schwachstellenanalyse. Besonders wichtig sind der Schutz und der Umgang mit der Informations- und Telekommunikationstechnik. Auf Dauer entfaltet ein Sicherheitskonzept seine Wirkung aber nur, wenn es regelmäßig an veränderte Gefahrenlagen angepasst und von allen Beteiligten aktiv gelebt wird. Grundsätzlich unterliegt jedes IT-System einer Gefährdung durch Viren- oder Trojanerattacken. Diese Formen von Schadsoftware sind in der Lage, alle Arten von Logindaten, Netzwerkinformationen, Datenmaterial und Dokumenten Unbefugten zugänglich zu machen, Dateien zu verändern sowie Netzwerkcomputer zu manipulieren oder zu „kapern". Mit Trojanern versehene E-Mails spähen zunächst die Systemumgebung der angegriffenen Rechner aus, um in einem zweiten Schritt Daten auch abzuziehen. Die Vorgehensweise bei Angriffen auf fremde IT-Systeme mittels Trojanern wird permanent optimiert. Während der klassische Verbreitungsweg über Datenträger immer noch beschritten wird, erfolgen Angriffe immer häufiger mit spezieller, auf das Opfer zugeschnittener Spionagesoftware. Zunächst werden Vorlieben, Interessen oder Hobbys der Zielperson ermittelt, um sie mit einer „passenden" E-Mail zu konfrontieren. Beim Öffnen dieser Mail wird unbemerkt ein Trojaner platziert. Marktgängige Schutzprogramme können hier keine absolute Sicherheit bieten, da Trojaner – ebenso wie die Schutzprogramme selbst – fortlaufend und in einer Art „Wettlauf" mit diesen weiterentwickelt werden.

4 Telekommunikationsanlagen

Moderne Telekommunikationsanlagen (TK-Anlagen) sind weit mehr als nur „Telefone" und werden häufig in hochkomplexe Rechnersysteme integriert. Gefährdungen ergeben sich dabei insbesondere aus dem Abhören von Informationen innerhalb des Systems, unbefugten Zugriffen auf Administration und Datenspeicher sowie durch Missbrauch des „remote access" (= Zugriff auf einen Computer oder ein Netzwerk aus der Ferne). Eine Vielzahl der zur Verfügung stehenden Funktionen kann auch zur unrechtmäßigen Informationsbeschaffung genutzt werden. Zu nennen sind hier etwa die Funktionen „Aufschalten" (auf Verbindungen Dritter), Konferenzschaltung (Gefahr des unbemerkten Aufbaus im Hintergrund), automatischer Rückruf sowie Freisprechen/ Lauthören (ermöglicht das Abhören von Raumgesprächen). Zudem verfügen Mitarbeiter zumeist über Mobilgeräte und sind so bei der Fahrt mit der Bahn, am Flughafen, an einem mobilen Arbeitsplatz oder direkt vor Ort beim Kunden mit ihrem Unternehmen verbunden. Die Funkanbindung von mobilen Endgeräten eröffnet jedoch nicht nur den berechtigten Nutzern, sondern auch Hackern, Konkurrenten oder Nachrichtendiensten Zugangsmöglichkeiten zu IT-Netzwerken und angeschlossenen Systemen. Ebenso hohe Risiken wie drahtlose Verbindungen bergen mobile Endgeräte (z.B. Laptops, Mobiltelefone, Smartphones, Personal Digital Assistants/PDAs und USB-Sticks), mit deren Hilfe die Kommunikation zwischen den Mitarbeitern im Außendienst und dem Unternehmen abgewickelt wird. Leider wird die hohe „Verwundbarkeit" drahtloser Verbindungen viel zu wenig erkannt bzw. nicht hinreichend ernst genommen. Anders ist es nicht zu erklären, dass selbst professionell betriebene Netze mangelhaft oder gar nicht abgesichert sind. **Risikobehaftet sind praktisch alle auf drahtloser Verbindung basierenden Techniken bzw. IT-Komponenten.** Erhebliches Risikopotenzial birgt bereits der unbefugte Zugriff Dritter – gezielt durch Diebstahl, aber auch im Wege des zufälligen Gerätezugriffs – auf mobile Geräte. Werden dann die im Unternehmensnetz vorgesehenen Standard-Sicherheitsmaßnahmen wie etwa Virenschutz, Verschlüsselung und Firewalls nicht oder nicht korrekt eingesetzt, kann sehr leicht ein Zugriff auf vertrauliche Firmendaten erfolgen. Weitere Risiken bestehen im missbräuchlichen privaten Einsatz der Geräte bis hin zur Überlassung an Dritte (Angehörige, Bekannte etc.), der Anschluss an ungesicherte (drahtlose) Verbindungen und die nicht autorisierte Installation ungeprüfter Fremdsoftware. Soweit ein Verzicht auf drahtlose Kommunikationselemente nicht möglich ist, ist es umso wichtiger, Schutzmaßnahmen zu ergreifen. Dies ist allerdings technisch

nicht immer durchführbar, z.B. bei Funktastaturen und –mäusen. Im Hinblick auf WLAN-Verbindungen bietet eine Verschlüsselung dagegen einen adäquaten Schutz. Sie sollte daher auf jeden Fall aktiviert und die voreingestellte Werks-Codierung gewechselt werden.

5 Checkliste für das Verhalten auf (Auslands-)Reisen

Dem Faktor Sicherheit kommt auf (Auslands-)Reisen eine besondere Bedeutung zu. Hier sind die Gefährdungen für Firmenvertreter vielfältig. Die Verfassungsschutzbehörden geben für Reisen insbesondere ins Ausland und Auslandsaufenthalte einige Verhaltensempfehlungen:

- Vor Reiseantritt über das Gastland informieren (Gesetze und Gebräuche) und die allgemeine Gefährdungs- und Sicherheitslage dort in Erfahrung bringen.
- Vorherige Prüfung der Geschäftsverbindung und des Geschäftspartners.
- Klare und eindeutige Angaben zur Person bzw. zum Arbeitgeber im Visumantrag.
- Aktuelle Ein- und Ausfuhrverbote oder -beschränkungen beachten.
- Im Gastland auf keinen Fall kompromittierende Situationen schaffen.
- Zusammenarbeit mit Service- bzw. Sicherheitsunternehmen vor Ort prüfen.
- Misstrauen bei ungewöhnlichen und intensiven Fragestellungen in Gesprächen.
- Niemals Gespräche mit Fremden über Reisezweck und Arbeitgeber führen.
- Kritische Betrachtung von privaten Kontakt- oder Begegnungsversuchen.
- Zurückhaltung im Gespräch, vor allem bei politischen oder berufsbezogenen Themen.
- Sensible Firmenunterlagen nie unbeaufsichtigt im Hotelzimmer, Tagungs- oder Büroraum belassen; Gepäck nie unbeaufsichtigt stehen lassen.
- Möglichst vollständige Vernichtung von nicht mehr benötigten Unterlagen. „Abfall“ kann wertvolle Informationen enthalten!
- Vorsicht vor Trojanern bei der Annahme von USB-Sticks als Geschenk.
- Nutzen Sie für wichtige Kommunikation auch „unterwegs“ nur gesicherte Wege.
- Zum Schutz von PC und Notebook: Passwörter sowie Virenschutz- und Verschlüsselungsprogramme einsetzen (ggf. Ländergegebenheiten beachten).
- Mobiltelefone nie unbeaufsichtigt lassen: Abhörgefahr durch Gerätemanipulation!
- Geschäftliche Daten auf USB-Stick oder DVD speichern und stets am Körper mitführen.
- Notebooks für Reisezwecke nur mit Minimalkonfiguration ausstatten.

6 Sicherheitsbehörden

Die Sicherheitsbehörden der Innenministerien der Bundesländer (Spionageabwehr) unterstützen Unternehmen nach Absprache auch durch firmenbezogene Beratungen.
In NRW ist der Verfassungsschutz/Wirtschaftsschutz erreichbar unter:
Tel.: 0211/871 28 21
E-Mail: wirtschaftsschutz@im1.nrw.de
Nähere Informationen erhalten Sie ferner unter:
https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/wirtschaftsschutz