Interview September 2015 mit Ing. Andreas H. Nehyba / BETRIEBSSPIONAGE

- Welcher Teilbereich ist bei Ihnen der wirtschaftlich gewichtigere: Compliance/Vorbeugung oder „es ist wieder etwas passiert“?
  Bis jetzt war der Fokus am aufklärenden Aspekt. Die Arbeitsgemeinschaft mit der Unternehmensberaterin Frau Mag. Nina Schwab für den präventiven Bereich besteht seit Anfang 2015. Die zur Zertifizierung von Compliance Management Systemen maßgebliche und internationale ISO-Norm, an der wir uns sehr stark orientieren, ist ebenfalls erst seit Beginn 2015 etabliert.

- Ich lese auf der Webseite, dass es auch für KMU von Interesse ist – gibt es Branchen, die sich besonders häufig an Sie wenden?
  Fehlverhalten wie Untreue, Veruntreuung, Korruption, Betrug, Diebstahl, Weitergabe von Geschäfts- und Betriebsgeheimnissen, ungerechtfertigter Krankenstand, Schwarzarbeit oder Verstöße gegen die Konkurrenzklausel können jedes Unternehmen in jeder Branche betreffen. Dementsprechend breit gefächert über alle möglichen Branchen, Geschäftsfelder und auch Unternehmensgrößen war und ist unsere Klientel. Unser Angebot richtet sich schwerpunktmäßig an KMU`s. Große Unternehmen und Konzerne verfügen über eigene Sicherheitsexperten und/oder sogenannte Compliance-Officer, oder auch eigene Compliance-Abteilungen. Aus unserer Sicht ist in diesen sensiblen Bereichen jedoch die Betrachtung durch firmenexterne Experten Ziel führender. Dies liegt in der Weisungsfreiheit und einer nicht vorhandenen „Betriebsblindheit“ begründet.

- Steigt die Bedeutung des Themas Betriebsspionage an sich?
  Aufgrund technischer und sozialer Entwicklungen wird es der „Gegenseite“ leichter gemacht an Informationen zu kommen, wodurch generell eine Gefährdung durch Betriebsspionage zunehmen muss. Man bedenke zum Beispiel, dass heutzutage viele MitarbeiterInnen über Smartphones und/oder Tablets verfügen. Diese Geräte erleichtern zwar das Arbeiten und den Umgang mit Kunden, bergen aber auch potentielle Angriffspunkte für die Gegenseite. Oder auch die mehr und mehr inflationäre Nutzung von social media wie Facebook ist ein Gefahrenherd für einen nicht gewünschten Informationsabfluss – Stichwort „Social Engineering“. Zitieren möchte ich in diesem Zusammenhang den renommierten amerikanischen Sicherheitsexperten Bob Griffin, Sicherheitschef einer der größten Sicherheitsfirmen: „Es gibt die beunruhigende Tendenz, dass hochkomplexe Angriffswerkzeuge, die bisher nur von Staaten finanziert werden konnten, mittlerweile auch in relativ leicht zugänglichen Internetforen auftauchen. Die zunehmende Vernetzung von Objekten und Maschinen schafft zudem völlig neue Risikoszenarien.“

- Gibt es Zahlen bzgl Schadenssumme pro Jahr? Ich habe nur die Zahl „einige Milliarden“ aus dem Jahr 2009 gefunden. Gibt es in Wien noch den Gedanken des „Kavaliersdelikt“ – wann spricht man von Spionage, wann von Unachtsamkeit oder ähnlichem?
  Sogar eine ältere Statistik aus dem Jahr 2007 spricht bereits von einem jährlichen Schaden von über 15 Milliarden EURO für österreichische Unternehmen. Eine

exakte Evaluierung ist aufgrund der Dunkelziffer nicht möglich. Es liegt aber auf der Hand, dass die Zahlen nicht zurückgegangen sein können.
Von Betriebs- oder Industriespionage spricht man, wenn ein (konkurrierendes) privates Unternehmen Spionageaktivitäten gegen ein anderes betreibt. Wirtschaftsspionage ist die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. Bei Spionage gibt es einen externen „Auftraggeber", den ich vorab als Gegenseite bezeichnet habe – meistens ein konkurrierendes Unternehmen oder auch ein ehemaliger Mitarbeiter. Es wird versucht Informationen hinsichtlich Preiskalkulationen, Produktentwicklungen, Produktionstechnologie, Know-How, kurzfristige Ziele und Entwicklungen oder langfristige Unternehmensstrategien zu gewinnen. Manchmal wird auch auf Basis unlauter gewonnener Informationen versucht, den Konkurrenzbetrieb zu sabotieren, um selbst einen Wettbewerbsvorteil zu erlangen oder einen Image-Verlust beim konkurrierenden Unternehmen herbeizuführen.
Natürlich kann auch durch Unachtsamkeit (Stichwort „Clean-Desk-Policy") und/oder Unwissenheit von MitarbeiterInnen ein großer wirtschaftlicher Schaden entstehen.

- In einem deutschen Artikel habe ich gelesen, dass die „Täter" meistens intern zu finden sind – können Sie das bestätigen? Die ausführenden Täter sind in den meisten Fällen intern zu finden. Wie bereits erwähnt, gibt es aber in der Regel externe Auftraggeber.

- Gibt es überhaupt eine absolute Sicherheit – wie sicher kann ein Firmenchef sein?
„Absolute Sicherheit" kann es niemals geben. Es gibt eine Gegenseite – die setzt sich zumeist zusammen aus einem konkurrierenden Unternehmen und aktueller bzw. ehemaliger Mitarbeiter. Kein Firmenchef ist davor gefeit, nicht zumindest eine Person im Unternehmen zu haben, die entweder unachtsam und dadurch „benutzbar" (Stichwort „Social Engneering") ist oder die über eine zumindest latent vorhandene kriminelle Energie verfügt.
Wir bauen nun gemeinsam mit dem Unternehmen eine Mauer gegen verschiedene Angriffsszenarien. Diese Mauer besteht zum einen aus Regeln und der Bewusstseinsbildung der MitarbeiterInnen zur Notwendigkeit der Einhaltung dieser (COMPLIANCE). Zum anderen gibt es weitere präventive Maßnahmen wie unter anderem die Evaluierung der IT-Sicherheit und der Gebäudesicherheit.
Die Gegenseite wird versuchen, einen Weg über diese Mauer zu finden. Und wir werden wiederum diese Mauer erhöhen, um dies zu erschweren. Unser Ansatz ist, dass nur ein ganzheitlich und dynamisch betrachteter Sicherheitsaspekt für ein Unternehmen ein Höchstmaß an Sicherheit bringen kann. Denn was bringt es, wenn durch Handlungsanweisungen, Verhaltenskodizes und entsprechende Schulungen korruptes oder nicht regelkonformes Verhalten von MitarbeiterInnen eingeschränkt wird, aber z. B. das IT-System über große Schwachstellen verfügt.

- Was entgegnen Sie, wenn ein Kritiker meint, dass man eine Firma nicht auf Misstrauen aufbauen kann (Stichwort fingierte Geschäftsanbahnungen etc.)
Fehlverhalten aufzuklären und Täter zu überführen, ist bedeutend schwieriger und auch weit kostenintensiver als Präventivmaßnahmen zu setzen. Ein

verursachter Schaden übersteigt bei der finanziellen Komponente die Kosten gegenüber präventiv zu setzenden Maßnahmen um ein Vielfaches. Zu erwähnen seien auch ein mit einem Schadensfall einhergehender, möglicher Reputationsverlust, etwaige Schadenersatzklagen und/oder strafrechtliche Konsequenzen. Reagieren ist im Bereich der Sicherheit immer teurer als agieren. Werden Mitarbeiter bei der Einführung eingebunden und über die Sinnhaftigkeit unterschiedlicher Sicherheitsmaßnahmen in Kenntnis gesetzt, kann der Beigeschmack des "Misstrauens" vermieden werden. Mitarbeiterschulungen, die richtige Kommunikation und ein richtungsweisendes Vorangehen der Unternehmensleitung, führen zu Akzeptanz sowie Einhaltung der Gesetze, Richtlinien und Maßnahmen.

- Hätten Sie mir 5 Punkte, die jeder bei sich in der Firma bedenken/checken sollte?
  Eine allgemein formulierte Checkliste gibt es nicht, da jedes Unternehmen seine Schwerpunkte individuell setzt und diese dementsprechend von uns in maßgeschneiderten Maßnahmen, wie z. B. einem CMS festgehalten werden. Einige strategische Überlegungen sollten aber generell sein:

  1. Verabschieden Sie sich von den Gedanken „bei mir bzw. in meinem Unternehmen passiert nichts“. Ich bin der felsenfesten Überzeugung, dass JEDES Unternehmen in irgendeiner Form bereits Opfer von Wirtschaftskriminalität ist oder war.
  2. Zurückkommend auf eine vorige Frage. Die Definition, was für ein Unternehmen ein gerade noch akzeptables „Kavaliersdelikt“ ist, obliegt jedem Unternehmer selbst. Ziehen Sie die Grenze sehr eng, denn auch die Summe an sogenannten „Kavaliersdelikten“ kann einen enormen wirtschaftlichen Schaden verursachen.
  3. Expansionsphilosophie ist zumeist immer noch deutlich wichtiger als Sicherheitsphilosophie – dies ist zu überdenken.
  4. Halten Sie sich folgenden Grundsatz vor Augen: bequem ist unsicher und unbequem ist sicher!
  5. Investieren Sie in die Implementierung und eventuell Zertifizierung eines Compliance Management Systems sowie weiterer präventiver Sicherheitsmaßnahmen. Sollte ein Schadensfall auftreten, ziehen Sie für die Aufklärung dafür legitimierte und ausgebildete Experten heran. Die Wiener Berufsdetektive sind in diesem Fall der Partner für die Wiener Wirtschaft.

Ing. Andreas H. Nehyba,
Firmeninhaber der Agentur Xtrace e. U. für Detektiv- und Sicherheitsoperationen ist Spezialist für die Aufklärung und die Beweisbeschaffung im Bereich der Wirtschaftskriminalität.
Gemeinsam mit einer Unternehmensberaterin werden auch präventive Dienstleistungen angeboten.
Informationen unter www.xtrace.at