Willkommen in einer Welt, in der das Verbrechen zu Hause ist!

Kein Tag ohne Cybercrime, Identitätsdiebstähle und Datenhacking. Die Angreifer wurden zu globalen Akteuren und die Polizei agiert weiterhin auf lokaler Ebene. Wenn früher ein Unternehmen in Frankfurt überfallen wurde, wussten wir: Tat, Opfer, Videoaufzeichnungen und Fingerabdrücke waren in Frankfurt, und die örtliche Polizei war für die Ermittlungen verantwortlich. Heute kann jemand in Land A sitzen, ein Unternehmen in Land B ins Visier nehmen – über verschiedene internationale Server gesteuert – und danach in Land C ans Werk gehen. Zudem erschweren unterschiedliche Rechtsordnungen den Strafverfolgungsbehörden die Arbeit erheblich. Als wären diese externe Bedrohungen nicht schon ausreichend komplex, kommen ständig steigende Anforderungen an das Verhalten der Mitarbeiter und die Governance innerhalb von Unternehmen hinzu und treiben das Thema Compliance weiter voran.

Wir befinden uns im zunehmendem Maße im Fadenkreuz von Wirtschaftskriminalität und Wirtschaftsspionage. Als wirtschaftsstärkstes Land der EU wird Deutschland hier eine strategische Rolle zugesprochen. Dementsprechend wächst das Engagement der Bundesbehörden wie der Wirtschaft. Immer mehr Kooperationen durch Politik, Wirtschaft und Gesellschaft entstehen zum Vorteil aller. Diese Art der institutionalisierten Zusammenarbeit ist ein wichtiger Bestandteil des Bollwerks gegen derzeitige und zukünftige Risiken. Zukunftsweisende Trends, wie Industrie 4.0, werden absehbar völlig neue Herausforderungen mit sich bringen.

Dazu gehören Diebstahl, Unterschlagung, Betrug und Untreue, die Verletzung von Geschäfts- und Betriebsgeheimnissen, Produkt- und Markenpiraterie, Erpressung, Geldwäsche, Korruption und Datenmissbrauch. Die zunehmende globale Vernetzung erhöht für jedes Unternehmen die Gefahr, selbst zum Opfer wirtschaftskriminellen Handelns zu werden. Die Wettbewerber und nicht selten auch Staaten haben es vor allem auf die geschäftsentscheidenden Informationen abgesehen. Das heißt, es geht um Patente, Innovationen, Kundendaten und Ausschreibungsverfahren ebenso wie um Marktstrategien und Informationen zu strategischen Veränderungen eines Unternehmens. Es handelt sich dabei um Geschäftsgeheimnisse, deren Wahrung über den Geschäftserfolg und mitunter über die Zukunft eines Unternehmens entscheidet.

Auch wenn viele Themen Dauerbrenner sind, hat doch die Geschwindigkeit, Intelligenz und Komplexität der Angriffe durch die Digitalisierung und Vernetzung weiter zugenommen. Und aus genau diesem Grund haben die Herausgeber ihren Schwerpunkt hervorragend gewählt: Fraud & Compliance Management – Trends, Entwicklungen, Perspektiven.

So ideenreich wie die Tatbestände müssen auch die Gegenmaßnahmen sein. Die Herausgeber haben dazu eine kenntnisreiche Auswahl von Autoren aus der Praxis getroffen.

Es wird klar aufgezeigt, dass wichtige Partner in Sachen Wirtschaftsschutz die staatlichen Sicherheitsbehörden sind. Sie bieten auf Bundes- und Landesebene eine breit gefächerte und gut organisierte Unterstützung. Das Bundeskriminalamt ist einer der Hauptansprechpartner, wenn es um organisierte Wirtschaftskriminalität geht. Auch das Zollkriminalamt spielt vor allem in den Bereichen Produktpiraterie und Schmuggel eine wichtige Rolle. Das Bundesamt für Verfassungsschutz sammelt zum Zwecke der Spionageabwehr Informationen über sicherheitsgefährdende und geheimdienstliche Tätigkeiten und wertet diese aus. In der IT-Welt ist das Bundesamt für Sicherheit in der Informationstechnik ein Hauptansprechpartner speziell im Bereich Cyber-Security.

Um sich über die eigenen Maßnahmen hinaus zu schützen, schließen sich immer mehr Unternehmen zusammen und suchen den aktiven Expertenaustausch auch mit den zuständigen Sicherheitsbehörden und der Politik. Denn nur gemeinsam, durch den Austausch von Erfahrungen und Kenntnissen, können der Eigenschutz und der Schutz der gesamten Wirtschaft auf ein hohes Niveau gebracht und dort gehalten werden.

Gerade deshalb ist es so wichtig, dass wir unter Federführung des Bundesinnenministeriums die Initiative Wirtschaftsschutz ins Leben gerufen haben – sozusagen als Public Private Partnership zwischen Regierungsstellen, Sicherheitsbehörden und Wirtschaftsverbänden.

Der ASW Bundesverband fördert die Entwicklung eines gemeinsamen Sicherheitsverständnisses durch enge Zusammenarbeit zwischen Unternehmen, staatlichen Stellen und Verbänden auch über Landesgrenzen hinaus. So unterstützen wir die Institutionalisierung der Zusammenarbeit für einen nachhaltigen Wirtschaftsschutz, damit alle Beteiligten Zugang zu den entscheidenden Sicherheitsakteuren haben, sei es in der Politik, in den Behörden, der Wirtschaft oder der Wissenschaft. Denn nur ein offener Informationsaustausch und der Zugang zu fundiertem Wissen ermöglichen es, eigene Sicherheitsmaßnahmen erfolgreich umzusetzen.

Konkret engagiert sich der ASW Bundesverband mit dem Projekt WIRTSCHAFTSGRUNDSCHUTZ zum Aufbau eines Werkzeugkastens für Unternehmen gegen Fraud, Spionage, Sabotage und Organisierte Kriminalität. Zusammen mit dem Projektpartner HiSolutions hat der ASW Bundesverband ein Handbuch mit nicht-informationstechnischen, also personellen, prozessualen, organisatorischen und allgemein technischen Maßnahmen für den Wirtschaftsschutz entwickelt. Mit diesem Grundschutzhandbuch wurde ein Pendant zum IT-Grundschutz und somit das fehlende Glied in der Schutzkette geschaffen.

Berlin, im Frühjahr 2018

Volker Wagner
Vorstandsvorsitzender ASW Bundesverband
Allianz für Sicherheit in der Wirtschaft e.V.