

Fachartikel vom 01.04.2009

Rubriken: Wirtschaftsschutz: Compliance, Wirtschaftsschutz: Know-how-Schutz, Wirtschaftsschutz: Sicherheitskonzepte

Risiken für den Mittelstand **Gefahrenbarometer 2010 veröffentlicht**

Die Corporate Trust GmbH hat ihre Studie „Gefahrenbarometer 2010“ veröffentlicht. Die Erhebung untersucht die Sicherheitsrisiken für den deutschen Mittelstand vor dem Hintergrund der Wirtschaftskrise.



Der Safe kann Unternehmen nicht vor Korruption und Hackerangriffen schützen. (Bild: Corporate Trust)

Da insbesondere der Mittelstand eine hohe Innovationskraft besitzt, nehmen Wirtschaftskriminalität und Industriespionage in diesem Sektor zu. Zur Bewertung des Risikos wurden die tatsächlichen Schäden der letzten drei Jahre sowie die Einschätzung der zukünftigen Gefahren berücksichtigt. Dazu wurden mehr als 5000 mittelständische deutsche Unternehmen befragt.

Die Ergebnisse der Studie zeigen, dass größere mittelständische Unternehmen häufiger von einem Schaden betroffen sind als kleinere Unternehmen. Das größte Schadensrisiko haben Mittelständler in dem Segment 50 bis 250 Millionen Euro Jahresumsatz oder 250 bis 1000 Mitarbeiter.

Unzureichend vorbereitet

„Große Konzerne haben häufig die nötigen Sicherheitsstrukturen aufgebaut. Mittelständler hingegen sind zum Teil unzureichend auf diese veränderten Sicherheits Herausforderungen vorbereitet“, erklärt Christian Schaaf, Geschäftsführer der Corporate Trust, Business Risk & Crisis Management GmbH. Dies führe dazu, dass sie leichter Opfer werden und manche Schäden erst zu spät entdeckten. „Wenn ein krimineller Angriff bemerkt wird und es im Unternehmen keine geeigneten Strukturen gibt, um ihn abzuwehren oder Schäden schnellstmöglich aufzudecken, kann sich ein solcher Vorfall sehr schnell zu einer Krise ausweiten“, sagt Schaaf.

Hohe Dunkelziffer

Leider würden viele der Vorfälle im Bereich Wirtschaftskriminalität oder Industriespionage gar nicht erst aufgedeckt oder von den Unternehmen vertuscht. Zu groß sei die Angst vor einem Reputationsschaden. „Dies führt dazu, dass die Kriminalstatistik nur einen Bruchteil der tatsächlichen Vorkommnisse und finanziellen Schäden widerspiegelt“, so Schaaf.

Diebstahl, Einbruch und Überfall sind mit 20,1 Prozent die häufigste Schadensursache bei mittelständischen Unternehmen. Korruption, Betrug und Untreue stehen mit 15,1 Prozent auf dem zweiten Rang der Sicherheitsrisiken, dicht gefolgt von Hackerangriffen mit 14,1 Prozent.

Gegen Risiken versichern

Die Absicherung der Unternehmen gegen diese Schäden und Risiken ist jedoch eher unzureichend. Nur knapp die Hälfte sind gegen die kriminellen Risiken versichert. Obwohl Korruption das zweithöchste Risiko darstellt, hat nur ein Fünftel aller Unternehmen einen eigenen Compliance-Verantwortlichen, der rechtskonformes und verantwortungsbewusstes Handeln im Unternehmen sicherstellt. Mit 17,7 Prozent verfügt nur ein geringer Anteil der befragten Unternehmen über ein professionelles Krisenmanagement.

Fehlende Geheimhaltungsstufen

Mehr als die Hälfte der Unternehmen macht ihren Mitarbeitern und Geschäftspartnern keine klaren Vorgaben zum Umgang mit vertraulichen Informationen. Nur bei 39,8 Prozent gibt es eine Klassifizierung der Geheimhaltungsstufe. „Wir erkennen aber einen positiven Trend“, weiß Christian Schaaf, dessen Unternehmen Corporate Trust auch in der präventiven Sicherheitsberatung tätig ist. „Die Studie bestätigt eine steigende Sensibilisierung für sicherheitsrelevante Fragestellungen. 53,1 Prozent der befragten Unternehmen wollen ihr Personal zukünftig besser sensibilisieren.“

Dazu bestünde auch eine rechtliche Verpflichtung, betont Alexander Haudan, Rechtsanwalt bei Taylor Wessing. „Nach dem Gesetz zur Kontrolle und Transparenz im Geschäftsverkehr ist die Geschäftsleitung dazu verpflichtet, die nötigen Vorkehrungen zu treffen, um Risiken frühzeitig zu erkennen und Gefahren vom Unternehmen abwenden zu können.“

Praxishinweis Taylor Wessing

Die anwaltliche Beratungspraxis zeigt, dass die Fälle von Geheimnisverrat und Spionage deutlich zunehmen und die meisten Rechtsverletzungen aus dem Unternehmen selbst heraus geschehen. Dieses Risiko sollten Unternehmer und Führungskräfte stets im Blick haben. Die betrieblichen Sensoren für Industriespionage sind in der Regel die Mitarbeiter. Daher sollten Meldepflichten und auch Melderechte für Mitarbeiter bei Verdachtsmomenten als präventive Regelungen Gegenstand der Arbeitsverhältnisse sein.

Das so genannte „Whistleblowing“ von Verstößen an eine zuständige Stelle sollte Teil der Corporate-Compliance-Regelungen sein und eingeführt werden. Es eignen sich sogenannte „Codes of Conduct“, die auch Sanktionen für Verstöße vorsehen sollten. Soweit ein Betriebsrat besteht, sind die Mitbestimmungsrechte bei der Einführung derartiger Regelungen zu beachten.

Auch der Hinweis auf die Strafbarkeit von Industriespionage (§ 17 UWG, Verrat von Geschäfts- und Betriebsgeheimnissen) in Arbeitsverträgen, Verhaltensrichtlinien oder Betriebsvereinbarungen hat regelmäßig erheblich abschreckende Wirkung, verbunden mit der Androhung entsprechender Schadensersatzansprüche.

