▲ Beim Sicherheitsdienstleister Securitas ist das Risk Assessment (RA) ein fester Bestandteil der Sicherheitsberatung

RISIKOBEURTEILUNG

Nicht nur zur Coronazeit

Risk Assessment als Grundlage der Sicherheitsberatung und dynamischer Prozess

Risk Assessment und Risk Management gehören in der Coronakrise zur Überlebensstrategie jedes von der Krise betroffenen Unternehmens. Das gilt auch für die Sicherheitswirtschaft. Ein Übersichtsbeitrag von Jens Müller, COO Securitas Deutschland, Vizepräsident BDSW.

Ohne Risk Management (RM) ist eine wirksame und verlässliche, den Ressourcen des Unternehmens angepasste Lösung der Gesamtrisikoproblematik nicht möglich. Je nach der Rechtsform und Größe des Unternehmens besteht auch eine Rechtspflicht zum RM nach § 91 Abs.2 AktG. Im Grunde handelt es sich um ein Gebot der Compliance und eine Grundpflicht des Geschäftsführers als „ordentlicher Kaufmann" (§ 43 Abs.1 GmbHG).

RA als Komponente der Sicherheitsberatung

Für den Sicherheitsdienstleister ist das Risk Assessment (RA) darüber hinaus für Vertrieb und Kundenbeziehungen von entscheidender Bedeutung. Kompetente Sicherheitsdienstleister beschränken sich nicht mehr auf den Einsatz einer vom Auftraggeber vorgegebenen Zahl an Sicherheitsmitarbeitern, sondern bieten ihm eine für den Kunden spezifisch entwickelte intelligente Sicherheitslösung an. Und die beginnt mit einer Sicherheitsberatung.

Um diese Beratung professionell durchführen zu können, braucht der Sicherheitsdienstleister eine Vielzahl von Informationen über das Unternehmen und seinen gegenwärtigen Sicherheitsstatus, sowie eine Fülle unternehmensexterner Daten. Vor allem KMU, die sich oft weder einen Sicherheitsbeauftragten noch eine Sicherheitskonzeption

Jens Müller, COO Securitas Deutschland, Vizepräsident BDSW

leisten, brauchen eine professionelle Sicherheitsberatung durch externe Fachleute.

Selbstverständlich bezieht sich dieses RA nicht auf den Gesamtbereich der Unternehmensrisiken, sondern ausschließlich auf den betreffenden Sicherheitsbereich. Der ist aber in seiner Gesamtheit einzubeziehen, umfasst also Security und Safety, physische, vermögensbezogene und virtuelle Gefahren, kriminelle Angriffe ebenso wie die Gefahr von Bränden und Explosionen, Gefahren durch Naturereignisse, Cyberattacken, Risiken in der Logistik und auf Geschäftsreisen, Gefahren für den Datenschutz und die Datensicherheit einschließlich Datenausspähung und Betriebsspionage, Gefahren, die durch betriebliche Anlagen und Prozesse entstehen.

Soweit für den IT-Bereich dem Sicherheitsdienstleister die fachliche Kompetenz fehlt, sollten externe IT-Sicherheitsexperten in die Sicherheitsberatung einbezogen werden. Das Ausmaß der Risiken, ihre Eintritts- und Schadenswahrscheinlichkeit sind selbstverständlich je nach Unternehmensgröße, Branche, Geschäftstätigkeit und Standort höchst unterschiedlich.

Schutzziele des Risk Assessments

Das Schutzziel der dem Kunden anzubietenden Sicherheitslösung – und damit auch des RA – bilden sowohl die Mitarbeiter des Unternehmens und externer Personen als Partner, Besucher oder Nachbarn, als auch alle Vermögenswerte, die den Risiken ausgesetzt sind. Zu priorisieren sind die sogenannten Kronjuwelen, also Geschäftsgeheimnisse und besonders sensible Bereiche der kritischen Infrastruktur – etwa das Rechenzentrum.

Systematische Durchführung des RA

Risk Assessment ist ein strukturierter Prozess. Nacheinander sind die Risiken zu identifizieren, zu analysieren, zu quantifizieren und – wenn sie sich gegenseitig verstärken, auch zu aggregieren -, zu bewerten und dementsprechend zu priorisieren. Standards für das methodische Vorgehen gibt die ISO 31000. Weitere Details zum Planungsprozess, zu Bewertungstechniken, zur Anwendung und Evaluierung, enthält die ISO 31010, die 2019 mit mehr Details neu gefasst worden ist.

Beim Sicherheitsdienstleister Securitas ist das RA ein fester Bestandteil der Sicherheitsberatung. Zur systematischen Durchführung erhält der Sicherheits- und Vertriebsspezialist spezifische Vorgaben auf seinem Tablet. Der Risikokatalog wird strukturiert in Bereiche mit unterschiedlichem Risikobezug. Einzelne Gefahren und Bedrohungen mit deren spezifischen Szenarien (Modus Operandi) werden in vier Stufen (schwach, mittel, hoch und sehr hoch) sowohl für die Eintrittswahrscheinlichkeit wie für die Schadensauswirkungen analysiert. So entsteht eine interaktive Risikomatrix für das Beratungsgespräch.

Der (potentielle) Kunde erhält nach eingehender Kommunikation über das methodische Vorgehen und über das Ergebnis des RA ein Risiko-Exposé mit Lösungsvorschlägen, die eine ganzheitliche, dem objektiven Sicherheitsbedarf unter besonderer Berücksichtigung der „Key Assets" entsprechende Sicherheitslösung darstellen. Der Gesamtprozess der von Securitas Deutschland praktizierten RA ist auf der Webseite des Unternehmens beschrieben (www.securitas.de/leistungen/risikobewertung-iso-31000/).

Predictive RA

Auf Konzernebene wird derzeit eine Erweiterung des Risk Assessments entwickelt und getestet, die das Leistungsangebot von Protective Services hin zu Protective Predictive Services optimieren wird. Das geschieht durch die Verwertung einer Fülle weiterer Daten („Big Data"), die sich aus der Geschäftstätigkeit des Sicherheitsdienstleisters und seinen „Best Practices", aus Datenbeständen des Betriebs und der Geschäftstätigkeit des Kunden, aus geographischen und demographischen Rahmenbedingungen und aus verwertbaren Datenbeständen von Sicherheitsbehörden ergeben und durch intelligente Algorithmen mit „deep learning"-Fähigkeiten ausgewertet werden.

So wie die Polizei durch Auswertung von kriminaltopographischen Erkenntnissen, Ermittlungsergebnissen, soziologischen und verkehrsstrukturellen Daten insbesondere für die lokale Wohnungseinbruchs-, Kfz- und Straßenkriminalität Prognosen für die Wahrscheinlichkeit der Begehung solcher Delikte in bestimmten, besonders belasteten, Bezirken aufstellt, könnten solche Daten auch Predictive Analytics bei der Sicherheitsberatung ermöglichen.

Aufgrund der zwischen dem BDSW oder seinen Landesverbänden und den Innenministerien oder Polizeidienststellen der Bundesländer geschlossenen Partnerschaften könnten die Sicherheitsbehörden gebeten werden, im Rahmen der vereinbarten Unterstützung solche Datenbestände zur Verfügung zu stellen, soweit Ermittlungen oder Datenschutzvorschriften nicht entgegenstehen.

Diese Möglichkeit der auf Millionen von Daten gestützten Risk Prediction, die den Kunden dynamische Risikoprognosen bietet, wird vom Konzern in Schweden getestet und auch in Deutschland eingeführt werden. Insgesamt erscheint dieser Weg der Risikoprognose fundierter und zielführender als die sogenannte Szenario-Methode. Nach ihr werden zunächst Rahmenbedingungen bestimmt, die auf den Untersuchungsgegenstand Einfluss haben. Die Einflussfaktoren werden beschrieben und alternative Annahmen für ihre künftige Ausprägung und Eintrittswahrscheinlichkeit festgelegt. Alle Entwicklungsannahmen aller Deskriptoren werden dann in einer formalisierten Wechselwirkungsanalyse aufeinander bezogen und mittels Algorithmen daraus Szenario-Gerüste und Szenario-Typen erarbeitet.

RA als dynamischer Prozess

Die RA ist kein einmaliger Vorgang, sondern Bestandteil der Sicherheitsberatung während der Gesamtdauer der Kundenbeziehung. Sie ist in Absprache mit dem Kunden in periodischen Abständen ebenso wie nach wesentlichen Veränderungen von Risiken und ihren Einflussfaktoren zu wiederholen, gegebenenfalls auch nach Schadensereignissen oder unerwartet aufgetretenen Risiken – die Coronapandemie ist ein Beispiel – neu zu justieren. Und natürlich ist das RM unverzichtbar für die Vorbereitung auf Krisenszenarien. ■

Risk Assessment und Risk Management gehören in der Coronakrise zur Überlebensstrategie jedes von der Krise betroffenen Unternehmens

Kontakt

Securitas Holding GmbH
Berlin
Tel.: +49 30 501 000 615
presse@securitas.de
www.securitas.de