Ist das Sicherheitsgewerbe für die Übernahme komplexer Unternehmenssicherheit gerüstet?

Von Manfred Buhl

OUTSOURCING VON DIENSTLEISTUNGEN ist für Unternehmen meist ein Erfolgsfaktor. Doch während Buchhaltung, Rechtswesen oder Facility Management längst umfassend ausgelagert werden können, beschränkt sich dies im Sicherheitsbereich auf einzelne Aufgabensegmente. Liegt es an der Komplexität der Querschnittsaufgabe Sicherheit oder ist der Markt noch nicht reif für Komplettangebote in der Sicherheit?

Beim Nachdenken über den aktuellen Funktionsbereich von Sicherheitsdienstleistern fallen uns die gängigen Aufgabenfelder ein: Objekt- und Werkschutz, Zutrittskontrolle und Empfangsdienste, Betrieb von Notrufanlagen und Intervention im Fall von Alarmmeldungen, Veranstaltungsschutz und Personenschutz, Geld- und Werttransporte. Das sind alles Funktionsbereiche, die vor allem durch physische Anwesenheit und Leistung wahrzunehmen sind. Selbstverständlich müssen solche Dienstleistungen geplant und gemanagt werden. Sie sind nicht etwa frei von geistiger Anstrengung und unternehmerischer Kompetenz, aber die genannten Tätigkeiten bedürfen normalerweise keiner vertieften Branchen- und Unternehmenskenntnisse. Sie laufen nach Vorgaben des Unternehmers und seines Managements ab. Veränderungen der angeordneten Aufgaben ergeben sich aus situativen Bedingungen und Ereignissen, aber in der Regel nicht aus Innovation und Optimierungsplanung.

Unternehmenssicherheit als komplexes Produkt

Die skizzierten Funktionen decken nicht im Entferntesten den gesamten Komplex der Unternehmenssicherheit ab (s. Kasten Funktionsbereiche der Unternehmenssicherheit S. 17). Die Prozesse und Systeme, die erforderlich sind, um die angemessene Sicherheit eines Unternehmens, seiner Mitarbeiter und aller Assets zu gewährleisten, richten sich nach den Erfordernissen, die sich aus der jeweiligen Branche und aus den spezifischen Rahmenbedingungen des einzelnen Unternehmens ergeben. Nicht zuletzt sind sie von der Unternehmensgröße abhängig. Ganz im Vordergrund steht die IT-Sicherheit, seit Computer und IT-Systeme die Produktion, die Geschäftsprozesse und Betriebsabläufe weitgehend steuern. Tendenziell nimmt die Komplexität der Unternehmenssicherheit vor allem infolge der beständig ansteigenden IT-basierten Steuerung von Betriebs- und Geschäftsprozessen, von Sicherheitsorganisation und Sicherheitstechnik und der damit verbundenen Vernetzung der einzelnen Funktionen und Prozesse beständig zu.

MANFRED BUHL ist BDSW-Vizepräsident sowie CEO und Vorsitzender der Geschäftsführung Securitas Sicherheitsdienste Holding Deutschland.

Wir bedanken uns für die Abdruckgenehmigung bei WIK Zeitschrift für die Sicherheit der Wirtschaft.

- Jede Festlegung und Veränderung von Schutzvorkehrungen für die Werte eines Unternehmens muss auf einer Risiko- und Schwachstellenanalyse aufbauen. Es ist zu entscheiden, welche Risiken in welchem Umfang hingenommen, durch Versicherungen abgedeckt oder durch Schutzmaßnahmen zu minimieren sind. Alle Sicherungsmaßnahmen sind in einer Sicherheitskonzeption zu entwickeln und aufeinander abzustimmen, damit sie so effizient und kostengünstig wie möglich angelegt werden können.
- Die Komplexität der verschiedenen Funktionsbereiche ergibt sich auch aus der Notwendigkeit ihrer Vernetzung. Sie sind nicht nur durch die Risikoanalyse, sondern auch in ihrer Ausführung verknüpft. Dies geschieht zunächst in der konzeptionellen Planung und generell durch IT-Funktionen. Vernetzt sind die einzelnen Sicherheitsfunktionen mit den Geschäftsprozessen und Betriebsabläufen des Unternehmens. Nur so können sie ihre volle Wirkung entfalten, ohne dass die Produktions- und sonstigen Geschäftsprozesse gebremst werden.
- Insbesondere diese Vernetzung bedingt, dass die Sicherheitsdienstleistungen nur dann wirkungsvoll sein können, wenn der Sicherheitsdienstleister die Geschäftsprozesse und Betriebsabläufe - und darüber hinaus die Unternehmensstrategie - selbst kennt. Nur so können die einzelnen Funktionen auch die richtigen Schwerpunkte setzen und auf Veränderungen in der Strategie angemessen zeitnah reagieren.

Funktionsbereiche der Unternehmenssicherheit

Ohne Berücksichtigung unternehmensspezifischer Besonderheiten, von Redundanzen und Überschneidungen lassen sich Gefahrenphänomene und Funktionsstrukturen der Unternehmenssicherheit etwa folgendermaßen systematisieren:

1. Personenschutz
- wegen Bekanntheitsgrad
- am Arbeitsplatz
- für Whistleblower
- in Krisenregionen

2. Objektschutz
- Perimeterschutz
- Schutz einzelner Objekte (Werkschutz)
- Zutrittskontrolle

3. Vermögensschutz
- Schutz vor Diebstahl und Unterschlagung
- Schutz vor Untreue
- Schutz vor Betrug

4. Know-how-Schutz
- Spionage
- Patentverletzung
- Produktpiraterie
- Missbrauch von IT-Schwachstellen

5. Produktions- und Produktschutz
- Schutz von Entwicklungsprozessen
- Schutz von Betriebsabläufen
- Schutz von Produktionsphasen
- Produktsicherheit
- Schutz von Lägern
- Transportschutz
- Logistiksicherheit

6. Schutz vor Störungen/Sabotage
- vor physischen Angriffen
- vor IT-Angriffen (DoS)
- Betriebsstörungen

7. IT-Schutz
- Schutz der IT-Infrastruktur
- Datensicherheit
- Schutz von IT-Produkten

8. Datenschutz
- von Kundendaten
- von Mitarbeiterdaten
- von Geschäftspartnerdaten

9. Imageschutz
- Managerkriminalität
- Wirtschaftskriminalität
- Korruption
- Skandale

10. Compliance
- Awareness
- Anzeigenorganisation
- Ermittlungen
- Konsequenzenmanagement

11. Brand- und Explosionsschutz
- organisatorisch
- baulich
- technisch (einschließlich Löschtechnik)

12. Katastrophenschutz
- Notfall
- Krise
- Business Continuity Management

13. Eventschutz
- Personenschutz
- Objektschutz
- Ablaufschutz

14. Arbeitsschutz
- Maschinenschutz
- Persönliche Ausrüstung
- Betriebsärztlicher Dienst

- Die Sicherheitstechnik wird für die Unternehmenssicherheit immer wichtiger. Sie entfaltet Präventionswirkung und kann die Vorbereitung von kriminellen Handlungen detektieren. Immer bedeutsamer wird die IT-Sicherheitstechnik für die Unternehmenssicherheit, und zwar in zweierlei Hinsicht: zur Steuerung und Vernetzung einzelner Funktionsbereiche der technischen wie der Corporate Security - aber auch als Einfallstor für Cyberkriminalität.

Status quo: „Mission impossible" für das Sicherheitsgewerbe

Die Frage drängt sich auf, warum die gesamte komplexe Funktionalität der Unternehmenssicherheit nicht von einem externen Sicherheitsdienstleister wahrgenommen werden kann. Das Management des Unternehmens könnte sich dann voll auf die Geschäftsprozesse und auf den Markt konzentrieren, und das Sicherheitsgewerbe würde dadurch eine beträchtliche Aufwertung erfahren. Die Antwort lautet schlicht: Das Sicherheitsgewerbe ist in der Qualifikation seines Managements und seiner Mitarbeiter, vor allem aber in seinem Denken und Planen nicht darauf vorbereitet. Es fehlt ihm an dem dazu erforderlichen Selbstbewusstsein und der daraus fließenden Konsequenz des Handelns; und es fehlt an der genügend großen Zahl von Unternehmen, die ihre komplexe Unternehmenssicherheit ganz oder größtenteils outsourcen wollen. Einige Aspekte:

- Sicherheitsunternehmen warten zumeist Ausschreibungen ab, um sie buchstabengetreu zu erfüllen. Die meisten dieser Ausschreibungen lassen den Sicherheitsunternehmen gar keinen konzeptionellen Spielraum. Die Ausschreibung bezieht sich zumeist auf eine bestimmte Zahl von Einsatzstunden, und der Zuschlag erfolgt in der Regel nach dem für die Gesamtzahl der Stunden vom Sicherheitsdienstleister angebotenen Preis.
- Die Struktur des Sicherheitsunternehmens ist in der Regel auf eine Übernahme sämtlicher oder eines größeren Teils der Sicherheitsfunktionen gar nicht vorbereitet. Auch größere Sicherheitsdienstleister beschränken sich aus Kostengründen auf ein „lean management". Oft fehlt es an einer Organisationseinheit für konzeptionelle Vorbereitungen für ein komplexes Management der Unternehmenssicherheit. Nur wenige Sicherheitsunternehmen verfügen über einen Key Account, der den Nucleus für eine solche Organisationseinheit bildet.
- Zu wenige Manager haben bisher einen Studiengang des Sicherheitsmanagements an einer Fachhochschule absolviert, in dem ihnen die notwendigen Kenntnisse der Betriebswirtschaft, analytisches und prozessorientiertes Denken, die Beherrschung der IT-Technik und der für die Unternehmenssicherheit wichtigen Sicherheitstechnologien vermittelt wurden.
- Es fehlt auch an Mitarbeitern, die die anspruchsvolleren und komplexen Funktionsbereiche der Unternehmenssicherheit beherrschen. Das gilt vor allem für die sicherheitstechnischen Anlagen und ihre konkrete Anwendung, aber auch für Ermittlungskompetenzen zur Detektion von Vermögenskriminalität einschließlich der Abwehr von Spionage und Produktpiraterie, für IT-Sicherheit und für den Schutz vor IuK-Kriminalität. Die tendenzielle Zunahme der IT-Steuerung von Betriebsabläufen und Geschäftsprozessen und der IT-basierten Vernetzung von Sicherheitsfunktionen mit diesen Betriebs- und Geschäftsprozessen wirkt sich überdies erschwerend auf die Fähigkeit von Sicherheitsunternehmen zur Übernahme komplexer Unternehmenssicherheit aus.
- Die Kapitalausstattung der meisten Sicherheitsunternehmen ist nicht stark genug, um alle notwendigen Vorbereitungen auf die Übernahme der gesamten Unternehmenssicherheit, die Qualifizierung der einzusetzenden Kräfte - vor allem der Führungskräfte - und ein Investment in die erforderliche Sicherheitstechnik und ihre Modernisierung zu finanzieren.
- Es fehlt sehr oft an Branchenkenntnissen und erst recht an ausreichenden Kenntnissen über die Geschäftsstrategie, die Geschäftsprozesse und Betriebsabläufe der Unternehmen, die bisher noch die meisten anspruchsvolleren Funktionen der Unternehmenssicherheit selbst wahrnehmen. Erst wenige große Sicherheitsunternehmen haben damit begonnen, sich auf Branchensegmente zu fokussieren und ihre Unternehmensstruktur danach auszurichten.

Das Ziel ist dennoch erreichbar

Auch wenn also noch mehrere Voraussetzungen für die Übernahme der wichtigsten Funktionen einer umfassenden Unternehmenssicherheit bei den allermeisten Sicherheitsunternehmen fehlen: Das Ziel ist dennoch grundsätzlich erreichbar:

Rechtliche Hürden stehen jedenfalls nicht im Weg. Alle Sicherheitsfunktionen in einem Unternehmen können aufgrund der Eigentums-, Besitz- und „Jedermanns"-Rechte wahrgenommen werden. Das staatliche Gewaltmonopol wird nicht angetastet. Das würde erst im Rahmen von Strafverfolgungsmaßnahmen einsetzen - soweit es sich nicht um die Verfolgung eines Tatverdächtigen „auf frischerTat" handelt.

Für den Unternehmer kann das Outsourcing möglichst vieler Sicherheitsfunktionen an einen Sicherheitsunternehmer kostenmäßig günstig sein, denn erfahrungsgemäß geht der Auftragnehmer mit den für die Auftragserfüllung notwendigen Ressourcen sparsamer um als unternehmenseigene Organisationseinheiten. Hinzu kommt das Niedriglohnniveau im Sicherheitsgewerbe - trotz Mindestlohn. Das würde zwar mit der Übernahme besonders anspruchsvoller Funktionen der Unternehmenssicherheit tendenziell steigen, aber erst in einem längerfristigen Prozess.

Lediglich dort, wo die Wahrnehmung von Sicherheitsfunktionen untrennbar mit Geschäfts- und Betriebsgeheimnissen und mit für das Unternehmen besonders wichtigen Patenten verknüpft ist, kann es aus Sicht des Unternehmens Veranlassung geben, solche Sicherheitsfunktionen nicht „aus der Hand zu geben". Auch der IT-Schutz kann so eng mit den IT-Prozessen innerhalb der IT-Infrastruktur des Unternehmens verknüpft sein, dass es letztlich sachgerecht erscheint, der IT-Organisation auch die IT-Sicherheit zu überlassen. Allerdings darf die Gefahr nicht verkannt werden, dass die IT-Organisation Sicherheitsvorgaben teilweise als Bremse der weiteren IT-Entwicklung wahrnimmt und deshalb eher vernachlässigt. Das aber könnte sich infolge der immer bedrohlicher werdenden Cyberkriminalität verheerend auswirken.

Entscheidungs- und Handlungsbedarf

Wie sollte ein Sicherheitsunternehmen vorgehen, wenn es in Erwägung zieht, über die „klassischen" Aufgaben des Sicherheitsgewerbes hinaus die Sicherheitsfunktionen von Unternehmen ganz oder größtenteils zu übernehmen?

Gründliche Prüfung von Chancen und Risiken: Am Anfang muss eine ebenso gründliche wie realistische Prüfung von Chancen

und Risiken stehen. Sie sollte sich zunächst auf das eigene Unternehmen beziehen und alle Voraussetzungen einbeziehen, die das Unternehmen bisher noch nicht erfüllen kann. Im Vordergrund müssen betriebswirtschaftliche Überlegungen stehen. In einem zweiten Analyseschritt muss überlegt werden, in welcher Branche oder in welchen Branchen sich das Sicherheitsunternehmen engagieren sollte, welche Sicherheitsfunktionen übernommen werden könnten und welche Größe das outsourcende Unternehmen haben könnte. Die Sicherheit eines mittelständischen Unternehmens zu übernehmen, fällt aus vielerlei Gründen grundsätzlich leichter, als für die Unternehmenssicherheit eines Konzerns Sorge zu tragen. Das zeigen schon die Personalressourcen, über die ein Konzern zur Erfüllung aller Sicherheitsfunktionen verfügt. Nicht selten ist das eine dreistellige, ja mitunter sogar eine vierstellige Zahl.

Unternehmerische Grundsatzentscheidung: Letztlich bedarf es einer unternehmerischen Grundsatzentscheidung, ob ein Sicherheitsunternehmen nach Abwägung aller Chancen und Risiken sich an einer entsprechenden Ausschreibung beteiligt bzw. auch ohne Ausschreibung im Wege der Marktforschung auf ein Angebot zum Outsourcing eingeht oder selbst ein entsprechendes Marketing entwickelt.

Investitionen und Qualifikationen: Nach der getroffenen positiven Grundsatzentscheidung ist die Konzeption zur Wahrnehmung der für das Outsourcing in Betracht kommenden Sicherheitsfunktionen nach einem Masterplan und einer darauf aufbauenden Detailplanung zu entwickeln. Das setzt die Einrichtung einer strategischen Abteilung im Sicherheitsunternehmen mit einem kompetenten Risikomanagement und konzeptioneller Erfahrung voraus. Zugleich sind die finanziellen Mittel für alle notwendigen Investitionen zur Verfügung zu stellen oder durch Kreditaufnahme zu beschaffen. Eventuell muss die Kapitalbasis verstärkt werden. Und es muss durch Schulung eigener Kräfte wie durch Einstellung von Experten (möglichst aus der jeweiligen Branche, im Optimalfall durch Übernahme von unternehmenseigenen Sicherheitsexperten) die erforderliche Qualifikation zur Wahrnehmung der verschiedenen Sicherheitsfunktionen gewährleistet werden. Dabei muss der Zeitfaktor berücksichtigt werden. Qualifikation kann nicht „von heute auf morgen" vermittelt werden.

Sicherheitstechnik und IT-Technik: Eine der wichtigsten unabdingbaren Voraussetzungen für die Übernahme der gesamten Unternehmenssicherheit ist der Aufbau einer sicherheitstechnischen Säule. Wenn das Sicherheitsunternehmen bisher über keine sicherheitstechnische Organisation verfügt, die die für die Unternehmenssicherheit wichtigen Sicherheitstechnologien beherrscht, kommt die Akquisition eines sicherheitstechnischen Unternehmens oder eine strategische Partnerschaft mit einem solchen Unternehmen in Betracht. Erst recht gilt das für die IT-Sicherheitstechnik, wenn dieser Bereich ausnahmsweise mit outgesourct wird.

Branchenfokussierung: Parallel dazu muss das Sicherheitsunternehmen sich neben der üblichen regionalen Organisationsstruktur auf die Sicherheitsanforderungen einer oder mehrerer Branchen fokussieren und eine „Hybridstruktur" entwickeln. Diese Fokussierung bildet die Basis für die Übernahme komplexer Unternehmenssicherheitsfunktionen in dieser Branche. Dabei darf sich das Kompetenzteam des Sicherheitsunternehmens nicht auf die Sicherheitsfunktionen in dieser Branche beschränken. Es muss die Betriebsabläufe, die Technologien, die Logistikfunktionen und die Geschäftsprozesse studieren. Zu den Abläufen gehören zum Beispiel im Automotive-Bereich: Forschung und Entwicklung ->Produktion -> Markteinführung -> Verkauf-> After Sales. Und das Kompetenzteam muss „das Denken und die Sprache der Branche" lernen. Je mehr gründliche Kenntnisse und Insiderwissen der Sicherheitsunternehmer und seine für die neue Aufgabenstellung ausgesuchten Manager über die Branche besitzen und in ihre fachliche Analyse und Argumentation übernehmen, umso kompetenter können sie auftreten und in Verhandlungen mit den Branchenunternehmen überzeugen.

Fazit

Wichtig ist, dass ein solcher „Big Deal" überlegt und sorgfältig vorbereitet wird. Dabei ist es notwendig, Schritt für Schritt vorzugehen und nicht etwa eine Grundsatzentscheidung zu treffen, bevor die Voraussetzungen und die Möglichkeit ihrer Erfüllung eingehend analysiert wurden. In vielen Fällen wird es ratsam sein, nicht auf einmal die Übernahme der gesamten Unternehmenssicherheit anzustreben, sondern auch hierbei stufenförmig vorzugehen und einzelne Funktionen erst wahrzunehmen, wenn alle Voraussetzungen dafür gegeben sind. Diese stufenförmige Übernahme muss vertraglich festgelegt und ausgestaltet werden. Alle Vertragsverhandlungen eines solchen „Big Deal" sollten von Vorsicht und Risikobewusstsein getragen werden. Ins kalte Wasser zu springen und dann zu scheitern ist für den Sicherheitsunternehmer, aber auch für das outsourcende Unternehmen, der falsche Weg.