INTEGRIERTE SICHERHEIT

Erläuterungen & Handlungsempfehlungen

für Anwender, Sicherheitsdienstleister,
Systemlieferanten, Errichter und
Fachplaner / Consultants

IHRE PARTNER FÜR
ganzheitliche Sicherheitslösungen

BDSW BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT

VfS Verband für Sicherheitstechnik eV

VORWORT

Steigende Anforderungen in der Objektsicherung werden vorzugsweise durch den erhöhten Einsatz von Technik oder Sicherheitspersonal oder durch die Veränderung von organisatorischen Maßnahmen abgedeckt. Diese Maßnahmen werden selten aufeinander abgestimmt. Das gilt sowohl für die Prävention als auch für Intervention, Kommunikation und Dokumentation.

Die Ursachen hierfür sind vielfältig. Das liegt zum Teil an organisatorischen Missständen, zum Beispiel an der getrennten Verantwortung für Sicherheitskräfte und Technik. Fehlende Kenntnisse über das mögliche Zusammenspiel von Mensch und Technik sind auch häufig vorzufinden. In seltenen Fällen könnte man auch von blindem Aktionismus sprechen.

In der aktuellen Gefährdungslage stellt die Objektsicherung eine besondere Herausforderung für alle Verantwortlichen dar. Umso wichtiger ist es, Lösungsansätze zu finden, in denen Technik, Organisation und Menschen optimal, abgestimmt und effektiv eingesetzt werden. Dies kann nur gelingen, wenn man hier einen ganzheitlichen Ansatz wählt.

Eine Reihe von Experten aus verschiedenen Bereichen der Sicherheitswirtschaft haben ihre Erfahrungen zusammengetragen, um Ihnen in dieser Handlungsempfehlung wichtige Hinweise zur Fehlervermeidung und Qualitätsverbesserung bereitzustellen.

Experten aller Projektphasen wie Fachplaner, Systemlieferanten, Errichter, Sicherheitsdienstleister und Nutzer von Sicherheitsprodukten sind involviert. Die Handlungsempfehlung ist eine kompakte Zusammenstellung von Strategien, die Anregungen und Hilfestellungen für die Lösung Ihrer Herausforderungen geben kann. Sie kann dabei helfen die Qualität Ihres Projektes zu verbessern und die Sicherheit, unter Berücksichtigung von technischen und wirtschaftlichen Parametern, zu erhöhen.

Dabei erhebt die (erste) Handlungsempfehlung nicht den Anspruch auf Vollständigkeit. Wir wissen, dass die Integration von IT-Sicherheit und physischer Sicherheit immer wichtiger wird. Vorkehrungen gegen die Umgehung und Überlistung von Sicherheitstechnik müssen bereits in der Planungs- und Entwicklungsphase berücksichtigt werden. Dieses und andere Themen werden wir in einem Leitfaden aufnehmen und fortschreiben. Wir freuen uns auf Ihre konstruktiven Anregungen und Rückmeldungen und sichern bereits heute zu, diese zu berücksichtigen.

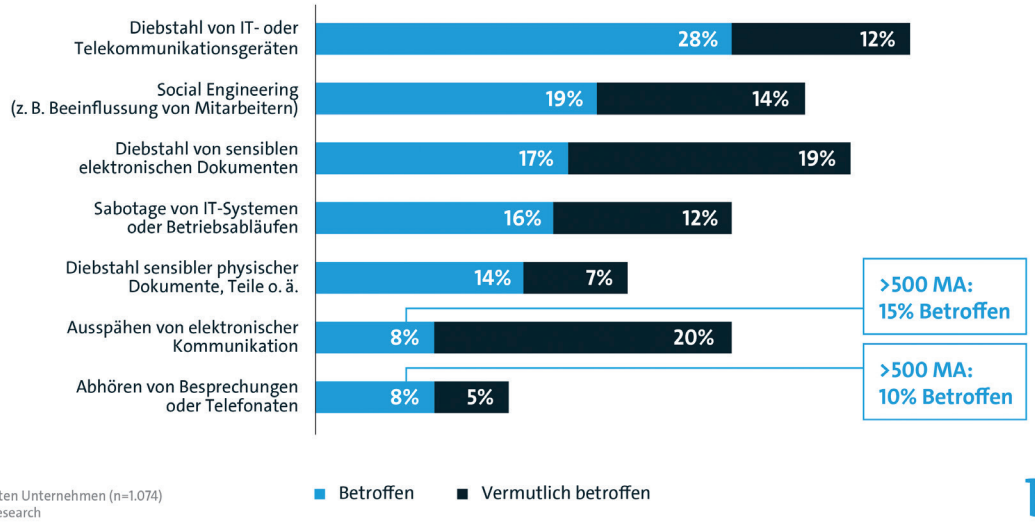
Unser Dank gilt allen Mitwirkenden für die offene Kommunikation, die konstruktive Zusammenarbeit, die Einbringung ihrer Erfahrungen und den damit verbundenen Zeitaufwand.

Dr. Harald Olschok
Hauptgeschäftsführer BDSW

Wilfried Joswig
Geschäftsführer VfS e. V.

Häufigstes Delikt ist der Diebstahl von Daten und Datenträgern

Von welchen der folgenden Handlungen war Ihr Unternehmen innerhalb der letzten 2 Jahre betroffen?



Basis: Alle befragten Unternehmen (n=1.074)
Quelle: Bitkom Research

bitkom

HERAUSFORDERUNGEN IM WIRTSCHAFTSSCHUTZ

Immer stärker besetzt das Thema Sicherheit die aktuelle Agenda von Politik, Wirtschaft und Gesellschaft. Veränderte Bedrohungsphänomene, Abhörskandale, Hackerangriffe auf IT-Systeme und nicht zuletzt die aktuellen Terroranschläge führen nicht nur zu gravierenden volkswirtschaftlichen Schäden, sondern sind auch Auslöser einer Fokussierung auf das Thema Sicherheit. Häufig gerät dabei aber in Vergessenheit, dass die meisten Unternehmen immer noch durch Diebstahl in seinen verschiedenen Ausprägungen geschädigt werden. Dies hat zuletzt der Branchenverband BITKOM in seiner Studie „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter"* überzeugend herausgestellt. Diebstahl von IT- oder Telekommunikationsgeräten, von sensiblen elektronischen und/oder physischen Dokumenten führt zu beträchtlichen Schäden für die deutsche Wirtschaft.

Dazu kommen die gegenwärtig anhaltenden wirtschaftlichen, politischen und gesellschaftlichen Veränderungsprozesse sowie eine nachhaltige Verschlechterung des subjektiven Sicherheitsgefühls in weiten Teilen der Bevölkerung. Vor diesem Hintergrund hat sich ein Begriff als Synonym für eine ganzheitliche, auf kleine und mittelständische Unternehmen (KMU) fokussierte Unternehmenssicherheit etabliert: integrierte Sicherheit.

Ausgehend vom TOP-Ansatz (Technik-Organisation-Personal) versteht man unter dem Begriff integrierte Sicherheit eine ganzheitliche Betrachtung der Unternehmenssicherheit in den Bereichen Technik, Organisation und Personal, bei der einzelne Sicherheitsmaßnahmen aufeinander abgestimmt sind und zu einer ganzheitlichen Lösung führen.

Dabei betrachtet die integrierte Sicherheit den kompletten Prozess von der Projektinitialisierung, der Planung, der Realisierung über die Abnahme bis zum Betrieb einschließlich aller technischen, organisatorischen und personellen Anforderungen.

Ausgehend von der im April 2016 durch das Bundesinnenministerium mit zahlreichen Verbänden vorgestellten Nationalen Wirtschaftsschutzstrategie sind KMU aufgefordert, sich angemessen auf die eingangs skizzierten Herausforderungen vorzubereiten. Allerdings ist in der Praxis häufig zu beobachten, dass die notwendigen personellen, organisatorischen und technischen Ressourcen, die die entsprechenden Risiken für das eigene Unternehmen erkennen und ihnen effektiv begegnen können, nicht vorhanden sind. Aber auch die Sicherheitsunternehmen müssen sich fragen, ob die Voraussetzungen für eine erfolgreiche, marktgerechte integrierte Sicherheit immer gegeben sind.

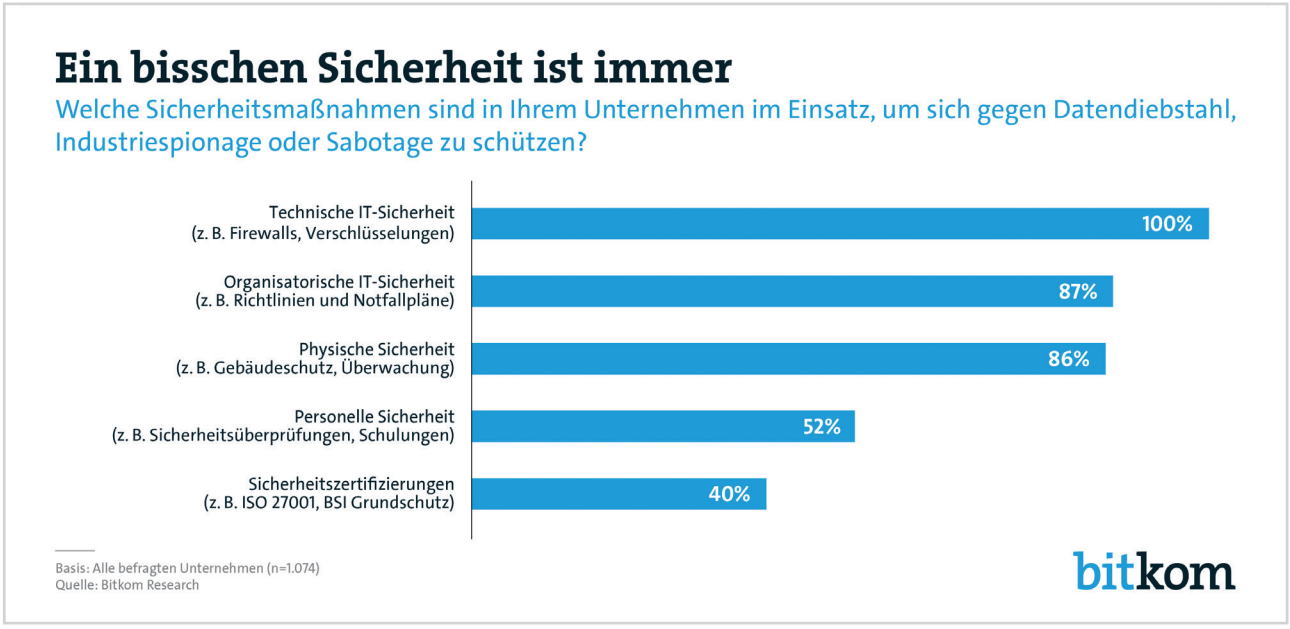
Die Mitgliedsunternehmen des BDSW und des VfS können und werden einen erheblichen Beitrag zur Unternehmenssicherheit in KMU leisten und somit maßgeblich zur Sicherung und Positionierung des Wirtschaftsstandortes Deutschlands beitragen.

*www.bitkom.org/Presse/Presseinformation/Studie-zu-Wirtschaftsschutz-und-Cybercrime.html

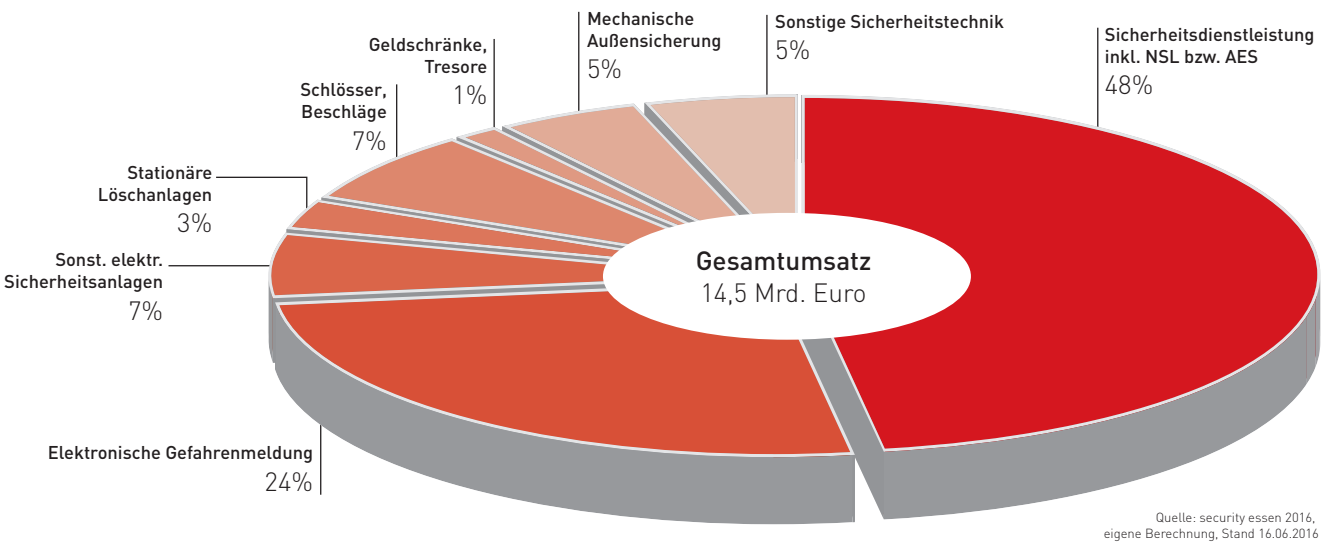
WAS IST INTEGRIERTE SICHERHEIT – BEISPIEL OBJEKTSICHERUNG

Wie das Schaubild der bereits erwähnten BITKOM-Studie zeigt, schützen sich 86 Prozent der befragten Unternehmen mittels physischer Sicherheit, z. B. Gebäudeschutz oder Überwachung, gegen Datendiebstahl, Industriespionage oder Sabotage. 14 Prozent schützen sich nicht. Nicht immer sind die getroffenen Maßnahmen erfolgreich.

Lösungsansätze, in denen Technik, Organisation und Personal optimal aufeinander abgestimmt und effektiv eingesetzt werden, werden immer wichtiger. Dies kann nur gelingen, wenn man hier den ganzheitlichen Ansatz der integrierten Sicherheit wählt. Diese betrachtet den kompletten Prozess von der Projektinitialisierung, der Planung, der Realisierung über die Abnahme bis zum Betrieb einschließlich aller damit verbundenen technischen und organisatorischen Anforderungen. Dazu gehören alle Komponenten des Sicherheitskonzeptes. Von Perimetersicherung über Zutrittskontrolle, Einbruchmeldetechnik, Videoüberwachung bis hin zu Leitstellen, Alarmverfolgung und Kommunikationstechnik. Natürlich beinhaltet die integrierte Sicherheit auch die Bewachung sowie andere Dienstleistungen wie Empfangsdienste, Risikomanagement usw. Daraus ist diese Handlungsempfehlung für die integrierte Sicherheit entstanden.



Sicherheitsmarkt in Deutschland 2015



Quelle: security essen 2016,
eigene Berechnung, Stand 16.06.2016

WARUM INTEGRIERTE SICHERHEIT

Unsere moderne Industriegesellschaft zeichnet sich durch eine hoch spezialisierte, arbeitsteilige und vernetzte Wirtschaft aus. Eine Unterbrechung von Produktion oder Dienstleistungserbringung hat umfangreiche negative Nebenwirkungen und kann existenzbedrohende Auswirkungen für ein Unternehmen haben. Gefahren drohen u. a. durch Kriminalität, Terror, Spionage, Sabotage, Brand, Wasser sowie Klimaveränderungen. Diese erhöhten Sicherheitsanforderungen lassen sich nicht mehr nur durch zusätzliche Technik oder mehr Sicherheitsdienstleistung effektiv erfüllen, sondern nur durch das Zusammenspiel einer Optimierung von Technik und Dienstleistung, der integrierten Sicherheit.

Sicherheitsdienstleistung und Sicherheitstechnik werden dabei enger miteinander verknüpft. Der personelle Objektschutz ist ohne mechanischen Perimeterschutz und Videoüberwachung nur bedingt wirksam.

Dabei ist auch der rasante technische Fortschritt in der Sicherheitstechnik zu beachten. Sicherheitstechnik wird immer effizienter, die Innovationszyklen immer kürzer. Videoüberwachungstechnik wird immer leistungsfähiger. Im Brandschutz gibt es hochsensible Früherkennungssensoren für Rauchentwicklung und Brandlokalisierung. In der Zutrittskontrolle steigt die Leistungsfähigkeit von biometrischen Erkennungsverfahren. Damit verbunden sind deutliche Kostensenkungen.

In der Kombination von Technik und Personal hat dies gravierende praktische Auswirkungen: Videoüberwachung unterstützt nahezu jede Sicherheitsdienstleistung, Produktionsprozesse und Lagerhallen werden durch baulichen und technischen Brand- und Explosionsschutz sowie durch Kontrollstreifen gesichert. Eine rechtzeitige und wirksame Intervention bedarf der Alarmauswertung und -übermittlung durch die Notruf- und Serviceleitstellen und einer situationsgerechten Intervention mittels technischer Fernwirkmaßnahmen und/oder menschlicher Kontrolltätigkeit. Sicherheitstechnik und Sicherheitsdienstleistung können so ausgewählt und aufeinander abgestimmt werden, dass sie alle örtlichen, zeitlichen und betrieblichen Rahmenbedingungen berücksichtigen. Bestehende Sicherheitslücken können immer weiter geschlossen werden.

Eine solche Gesamtlösung wünschen sich zunehmend auch die Kunden. Sicherheitstechnik und Dienstleistung müssen verglichen und bewertet werden. Das Ziel ist die Vernetzung von mechanischer und elektronischer Sicherheitstechnik, von Videoüberwachung, Bildauswertung und Sensorik, von Alarmierung und Intervention.

Die Sicherheitswirtschaft umfasst neben den Sicherheitsdienstleistungen auch die elektronische und mechanische Sicherheitstechnik. Der Gesamtumsatz beträgt 14,5 Milliarden Euro. Die oben stehende Übersicht informiert über die einzelnen Segmente.

ZIELSETZUNG: MEHR SICHERHEIT FÜR DEN ANWENDER

Diese Handlungsempfehlung soll Sie dabei unterstützen, integrierte Sicherheit auch in Ihren Projekten umzusetzen. Jeder Beteiligte muss zum richtigen Zeitpunkt das Richtige tun. Nur dann lässt sich dieses anspruchsvolle Ziel erreichen. Eine integrierte Sicherheitslösung ist die Erstellung eines individuell zugeschnittenen, gesamtheitlichen, branchennahen Konzeptes eines professionellen Sicherheitsexperten für seinen Kunden.
Dies spiegelt die strukturierte, ganzheitliche, intelligente Verknüpfung aller Sicherheitsbereiche eines Unternehmens wider und kann u. a. die folgenden Teilbereiche einschließen:

» Sicherheitsanalyse
» Beratung und Planung
» personelle Dienstleistung
» Sicherheitstechnik inkl. Errichtung und Wartung
» technischer Service
» Instandsetzung
» kompletter Service

Durch die Verknüpfung aller Teilbereiche in einem Sicherheitspaket sollen die Kosten gesenkt und das Sicherheitsniveau erhöht werden. Darüber hinaus wird ein Maximum an Effizienz erzielt.

NUTZEN FÜR DEN ANWENDER

Der Nutzen der integrierten Sicherheit gegenüber einer Kombination von Einzelkomponenten unterschiedlicher Anbieter liegt klar auf der Hand:

Ein Ansprechpartner für alle Sicherheitskomponenten

In einer zeitlich immer mehr durchgetakteten Welt wünscht sich der Anwender eine Problemlösung mit möglichst nur einem Anruf. Er hat einen Ansprechpartner, der sich bereichsübergreifend um die verzahnten Komponenten Consulting, Technik und Dienstleistung kümmert, da er für alle drei Bereiche zuständig ist. Hierbei ist es unerheblich, ob es sich um Planungsfehler, Bedienungsfehler, Softwarefehler oder technische Defekte handelt.
Der Kunde hat am Ende eine Person als „Problemlöser", anstatt sich mit den unterschiedlichen Anbietern über die jeweiligen Teilbereiche austauschen und nach einer Lösung suchen zu müssen.

Optimierung des Prozesses

Alle Sicherheitskomponenten werden gleichmäßig auf ein vorher vereinbartes Leistungsniveau festgelegt. So wird vermieden, dass möglicherweise hochspezialisiertes Personal unterhalb seines Leistungsniveaus mit minderwertiger Technik arbeiten muss oder High-End-Technik von wenig geschultem Personal nicht effizient eingesetzt werden kann.

Planungssicherheit für das Budget

Der Anwender bekommt eine komplett integrierte Sicherheitslösung zu einem Festpreis. Dieser beinhaltet je nach Kundenwunsch Technik, Dienstleistung, Instandhaltung, Instandsetzung, Aufschaltung und andere Komponenten.

Dieses kombinierte Produkt liefert eine planbare Größe für die betriebswirtschaftliche Planung, da sie je nach vertraglicher Ausgestaltung vor unkalkulierbaren Ausgaben wie beispielsweise Tariferhöhungen, Krankengeldzahlungen für Sicherheitspersonal oder Reparaturkosten für Technik schützt. In den Grundzügen ist dies durchaus vergleichbar mit einer Vollkaskoversicherung oder einem „Voll-Service-Leasing".

Schonung der Kundenressourcen

Die integrierte Sicherheitslösung schont sowohl die personellen als auch die monetären Ressourcen des Kunden. Der personelle Aufwand beim Betreiben der integrierten Sicherheitslösung besteht lediglich in einem Anruf beim Anbieter, um notwendigen qualifizierten Ersatz für Sicherheitspersonal und Technik zu bekommen. So kann sich der Kunde voll seinen Kernaufgaben widmen.

Darüber hinaus belasten möglicherweise notwendige Modifizierungsmaßnahmen nicht die firmeninternen Strukturen, wie z. B. Einkauf, Buchhaltung, Personalabteilung oder Qualitätssicherung, sondern laufen ausgegliedert ausschließlich beim Anbieter der integrierten Sicherheitslösung auf. Es wird qualifiziertes Personal gestellt, Zahlungen beispielsweise für Entgeltfortzahlung im Krankheitsfall und den Arbeitgeberzuschuss zum Mutterschaftsgeld für Sicherheitspersonal – aber auch Kosten für defekte Technik – bedürfen keinerlei Arbeitsschritte beim Kunden. Dies gilt auch für Schulungen oder Einweisungen in die neue Technik. Selbstverständlich verbleibt das Kontrollrecht beim Kunden.

Der Dienstleister erhält im Gegenzug aufgrund des monatlichen Festpreises und der üblichen langen Laufzeit eine gewisse Budgetsicherheit. Damit wird die integrierte Sicherheit zur Win-Win-Situation für den Kunden und den Anbieter. Hier ist jedoch unbedingt auf eine seriöse, realistische Kalkulation des Pauschalbetrages zu achten.

ZIELGRUPPEN UND TEILBEREICHE (BRANCHENLÖSUNGEN)

Innerhalb der Wirtschaft werden an die unterschiedlichen Branchen ganz differenzierte Anforderungen an Sicherheitsbedingungen und -standards gestellt. Somit ist jede integrierte Sicherheitslösung auf die Einhaltung der branchenspezifischen Anforderungen zu überprüfen.

Grundsätzlich enthält eine ganzheitliche Lösung immer:

» personelle
» technische
» und beratende Dienstleistungen

Im Bereich der Beratung und Analyse werden u. a. die folgenden Sicherheitskomponenten zu einer integrierten Sicherheitslösung zusammengefasst:

» Objektschutz
» Werkschutz
» Sicherheitstechnik
» Personenschutz
» Veranstaltungsschutz
» Notruf- und Serviceleitstelle
» Mobile Sicherheitsdienste
» Feuerwehrdienste
» Ergänzende Sicherheitsservices
» Finanzierung

Die integrierte Sicherheitslösung wird über eine Monatspauschale abgegolten, die alle vertraglich vereinbarten Leistungen beinhaltet. Hierzu zählen neben dem bereits Erwähnten insbesondere:

» Ersteinweisungs- und Weiterbildungskosten
» Schulungskosten
» tarifliche Lohnsteigerungen
» Wartung der Technik gemäß Vorgaben
» Instandsetzung der Technik gemäß Vorgaben
» sowie der gesamtheitliche Service mit einem festen Ansprechpartner

Integrierte Sicherheitslösungen können auf nahezu alle Kundenbranchen spezifisch zugeschnitten werden. Beispielhaft sei hingewiesen auf den Schutz von kerntechnischen Anlagen, militärischen Liegenschaften und Flughäfen, auf die Luftsicherheit oder die Hafen- und Seesicherheit. Die jeweils geltenden rechtlichen Grundlagen sind zu beachten und zum Vertragsbestandteil zu machen. Branchenlösungen für den Schutz von Häfen und die Seesicherheit müssen dem Standard ISPS-Code entsprechen und von autorisierten RSOs (Recognized Security Organizations) des Sicherheitsdienstleisters geplant und durchgeführt werden. Eine Genehmigung der Planung, Analyse und Durchführung durch die Hafensicherheitsbehörde ist unbedingt erforderlich.



Branchenlösungen für Logistik und Transport wiederum umfassen oft insbesondere die Überwachung und Verfolgung des Güterverkehrs auf Unregelmäßigkeiten durch Techniken wie GPS-Verfolgung, RFID, aber auch verdeckte Ermittler z. B. im Lagerbereich.

Als geeignete Branchen für integrierte Sicherheitslösungen bieten sich an:
» Kritische Infrastrukturen
» Banken und Versicherungen
» Energieversorger
» Hotels
» Industrie
» Justizvollzugsanstalten
» Forensische Kliniken
» Militärische Einrichtungen
» Museen
» Öffentlicher Personennahverkehr
» Rechenzentren
» Veranstaltungen / Events

Beispiel Retail

Die Studie „Inventurdifferenzen 2016“ des EHI Retail Institute e. V., ein Forschungs- und Bildungsinsitut für den Handel, kommt zu dem Ergebnis, dass 2015 in Deutschland Waren im Gesamtwert von 4 Milliarden Euro (Verkaufswert) verschwunden sind.

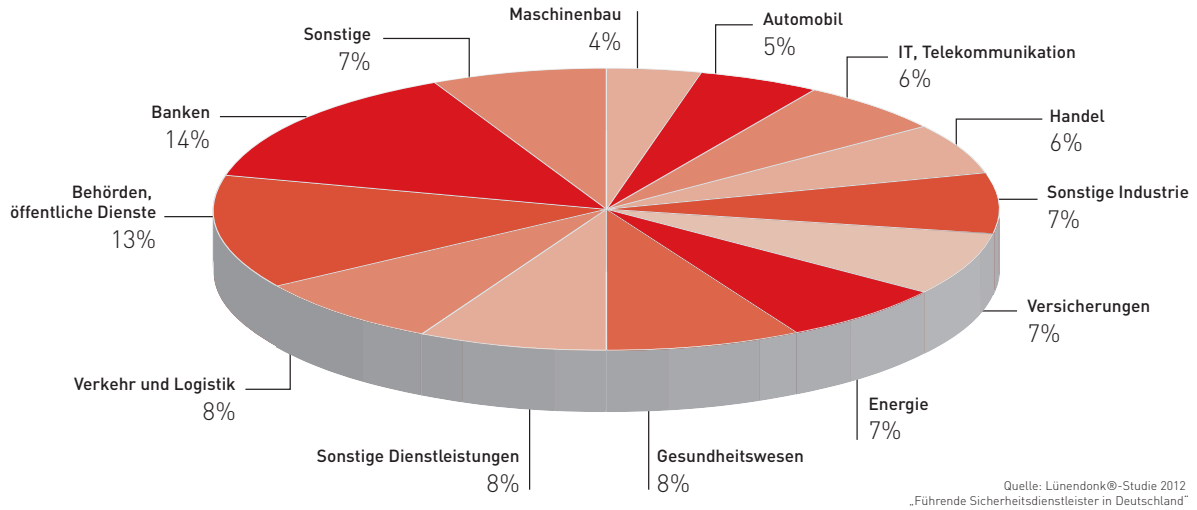
Daher hat im Einzelhandel die Verringerung von Inventurdifferenzen im Bereich Sicherheit die höchste Priorität. Allein die Höhe der Inventurdifferenzen kann hier darüber entscheiden, ob das Betriebsergebnis eines Handelsunternehmens positiv oder negativ ist. Deshalb ist es im Einzelhandel von entscheidender Wichtigkeit, den Fokus neben der allgemeinen Risikoanalyse insbesondere auf die Besucher-, Kunden- und Lieferantenstruktur zu richten.

Eine integrierte Sicherheitslösung „Retail“ bedeutet damit immer die Verzahnung von:
» Analyse und Consulting
» Präventionsmaßnahmen
» Inventurdifferenzreduzierung
» Warensicherung
» personeller, technischer und materieller Sicherung
» unverzüglicher Reaktion auf besondere Ereignisse
» umfassender Dokumentation aller Vorkommnisse
» klarem, bestimmtem Handeln im Kundenkontakt
» freundlicher Kundenansprache
» der Erstellung von Alarmplänen

VORGEHENSWEISE

BDSW und VfS planen als weiteren Schritt, einen Leitfaden zur Vorgehensweise bei der integrierten Sicherheit mit den nachfolgend dargestellten Modulen zu erstellen.
Die diesem Leitfaden zu Grunde liegende Gliederung ist dabei prinzipiell für alle Projekte anwendbar. Hierbei wird ein Gesamtprojekt in unterschiedliche Projektphasen untergliedert, angefangen von der Projektinitialisierung bis hin zum Betrieb der Anlage. In den einzelnen Projektphasen werden die Anforderungen und Aufgaben definiert, die als Zielvorgabe für eine erfolgreiche Projektabwicklung beachtet werden sollten. Der Detaillierungsgrad für die Bearbeitung richtet sich nach dem Gesamtprojektumfang bzw. der Projektkomplexität.
In den einzelnen Kapiteln des separaten Leitfadens „Integrierte Sicherheit" werden anhand von Prozessablaufschemata zusätzlich die Aufgaben bzw. Schnittstellen zwischen Betreiber, Sicherheitsdienstleister, Planer/Consultant, Hersteller/Lieferant und Errichter dargestellt.

Kundenbranchen der privaten Sichherheitsdienstleister
in Deutschland 2013



Quelle: Lünendonk®-Studie 2012
„Führende Sicherheitsdienstleister in Deutschland"

ZIELDEFINITION

PROJEKT-INITIALISIERUNG

- Projektziel definieren
- Aufgabenstellung (Lastenheft)
- Rahmen festlegen (Budget, Termin)
- Risikodefinition
- Kosten / Nutzenanalyse
- Schätzung Eigenleistung / Fremdleistung
- Ressourcenplanung
- Auswahl der erforderlichen und geeigneten Parteien

PLANUNG

- Pflichtenheft erstellen
- Machbarkeit
- Risikobewertung (Strategien bei Eintreffen von Risiken)
- rechtliche Betrachtung
- Projektstrukturplan mit Meilensteinen
- Terminplanung
- Betriebskonzept
- Instandhaltungskonzept
- Kostenplanung
- Projektorganisation
- Detailplanung
- Ausschreibungen
- Vergabe

REALISIERUNG

- Projektcontrolling (Kontrollschritte je nach Projektumfang)
  - Terminverfolgung
  - Kostenüberwachung
- Reporting
- Ressourcenplanung
- Überprüfung Zieldefinition
- Risikomanagement
- Projekt fortschreiben
- Strategien bei Planungsabweichungen
- Restpunktabwicklung

PROJEKT-ABSCHLUSS

- Abnahme durchführen
- Abweichungen festschreiben
- Dokumentation
- Betriebs- und Handlungsanweisungen
- Projektmanagementerfahrungen auswerten
- „Lesson learned"
- Erfahrungssicherung / Nachbewertung
- Schulung
- Wissenstransfer

BETRIEB

- Nachbetreuung
- Betriebserfahrungen auswerten
- Anpassungen vornehmen
- Instandhaltungskonzept
- WKP-Konzept
- Anpassung / Optimierung an Umgebungsbedingungen

VERBAND FÜR SICHERHEITSTECHNIK e. V.
Eulenkrugstraße 7 · 22359 Hamburg

Tel.: +49 40 21970010
Fax: +49 40 21970019

www.vfs-hh.de
Mail: info@vfs-hh.de

BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT
Wirtschafts- und Arbeitgeberverband e. V.
Norsk-Data-Straße 3 · 61352 Bad Homburg

Tel.: +49 6172 94 80 50
Fax: +49 6172 45 85 80

www.bdsw.de
Mail: mail@bdsw.de