

SICHERHEIT IN LOGISTIKZENTREN Hinweis – Lösungen – Trends

Fehlende Sicherheitskonzepte können hohe Schäden zur Folge haben. Gerade Logistikzentren mit hochwertigen Gütern sind besonders anfällig für Diebstahl und hohe Fehlerquoten durch menschliches, technisches oder organisatorisches Versagen. Schadensereignisse haben auch Außenwirkung und verursachen Imageschäden. Sicherheit wird dadurch zu einer strategischen Komponente mit Wertschöpfung. Der Umfang der Wertschöpfung wird durch das Sicherheitskonzept bestimmt. Es ist die systematisch erarbeitete Synthese aus baulichen, technischen und organisatorischen Maßnahmen.

Bedrohungs- und Risikopotenziale

Die Risikopotenziale sind vielfältig und in jedem Unternehmen unterschiedlich ausgeprägt. Logistikzentren müssen vorrangig Vorsorge treffen gegen Diebstahl durch Fremde, Lieferanten und Mitarbeiter, Verlust durch organisatorische Mängel, Betriebsunterbrechung durch Versagen der IT-Infrastruktur sowie gegen Brandgefahr. Der Verstoß gegen Vorgaben wie KonTraG und Basel II birgt ebenfalls erhebliche Gefahren für Unternehmen. In vielen Fällen sind es kleine Ereignisse, die eine Kettenreaktion mit verheerenden Folgen verursachen. Im ersten Schritt muss das Risikopotenzial (RP) und das verbleibende Restrisiko genau ermittelt werden. Das Risikopotenzial setzt sich aus den Faktoren Eintrittswahrscheinlichkeit, Entdeckungswahrscheinlichkeit und Bedeutung der Folge eines Ereignisses bzw. Fehlers zusammen. Es bestimmt die Schutzmaßnahmen und die damit verbundenen Investitions- und Betriebskosten.

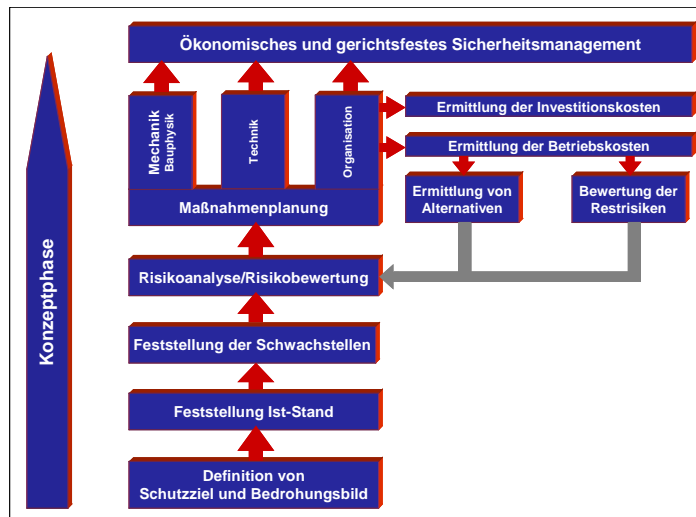


Bild 1 Ökonomisches und gerichtsfestes Sicherheitsmanagement

Gesetzliche Vorgaben

Der Verstoß gegen gesetzliche und wirtschaftliche Regeln hat ein hohes Risikopotenzial. Der Gesetzgeber verlangt die Einrichtung eines Risikomanagements – Vorhalten eines Früherkennungs- und Steuerungssystems für kritische Entwicklungen im Unternehmen. Die präventiv wirkenden Sicherheitsmaßnahmen sind Teil des Risikomanagements und stellen sicher, dass die gesetzlichen Forderungen erfüllt werden.

Diebstahl, Vandalismus und Sabotage

Die Gefahr von Einbruchdiebstahl, Vandalismus und Sabotage durch Fremde ist ebenfalls als hoch zu bewerten. Daher ist eine kompetente Planung notwendig. Die Meldetechnik muss individuell je nach Schutzziel und Funktionalität ausgewählt und eingesetzt werden. Die Erfahrung in der Praxis zeigt jedoch, dass angepriesene Leistungsmerkmale verschiedener Techniken oftmals nicht zutreffen. Hierbei gilt: was teuer ist, muss nicht immer gut sein. Wie wirksam die getroffenen Maßnahmen sind, zeigt sich am Widerstandszeitwert. Der Widerstandszeitwert ist die Reaktionszeit von der Meldung eines Eindringversuches bis zum verhinderten Einwirken durch Interventionskräfte. Die Detektion, der mechanische Widerstand und die Zeit bis zum Eintreffen der Interventionskräfte müssen exakt aufeinander abgestimmt sein. Alle gängigen Umzäunungen können mit Hilfsmitteln überwunden werden. Daher kommt es darauf an, an der äußeren Grenze (erste

Sicherheit in Logistikzentren – Fachartikel GIT

Sicherungslinie) nicht mit großem Aufwand das Eindringen zu verhindern, sondern dieses zu melden und an der Außenhaut des Gebäudes (zweite Sicherungslinie) mechanischen Widerstand zu erzeugen. Das schafft genügend Zeit für das Eingreifen der Interventionskräfte. Die Kombination von Detektion und Videoüberwachung mit gerichtsverwertbarer Bilddokumentation ist hierbei zu empfehlen.

Ein weiteres nicht zu unterschätzendes Risiko ist der Diebstahl durch Lieferanten und Mitarbeiter. Die Sicherung der Transportkette und die lückenlose Verfolgung der Warenströme ist von elementarer Bedeutung. Hierbei müssen auch die Fahrzeuge wie Zugmaschinen, Auflieger und Anhänger sowie die Entlade- und Beladevorgänge mit einbezogen werden. Mit einer videodokumentierten Funkscannerortung können die Warenströme lückenlos überwacht werden. Das Barcodesystem zeichnet das Stückgut mit Positionsdaten bei jedem Scannvorgang digital auf. Anhand von Suchkriterien kann der Verbleib des Stückgutes festgestellt werden. Die Zukunft wird jedoch der RFID-Transpondertechnologie gehören. Gegenüber dem Barcode reift mit den RFID-Tags in Kombination mit dem dazugehörigen Electronic Product Code (EPS) eine Technologie heran, die neue Möglichkeiten eröffnet. Die Kfz-Kennzeichenerkennung kann eine sinnvolle Ergänzung der Schutzmaßnahmen sein. Sie stellt sicher, dass die richtige Kombination von Zugmaschine, Auflieger und Anhänger ein- und ausfährt. Zusätzlich kann damit der Diebstahl von Fahrzeugen verhindert werden. Zugangskontrollen sind ein Muss. Hierzu gehört auch die Zustandsüberwachung der Tür. Die Türzeitoffenüberwachung mit akustischer und optischer Alarmierung an der Tür diszipliniert Mitarbeiter und Fremde. Türalarme sollten jedoch zu einer ständig besetzten Stelle geleitet werden. Videoüberwachung und Bilddokumentation unterstützen diese Maßnahme.

Technisches Versagen

Eine Betriebsunterbrechung durch technisches Versagen kann den Ruin für ein Logistikunternehmen bedeuten. Daher spielt die Verfügbarkeit der IT- und Gebäudetechnik eine wichtige Rolle. EDV-Klimatisierung und Spannungsversorgung müssen über Redundanzen oder Rückfallebenen verfügen. Zudem muss sichergestellt sein, dass Störungen und Ausfälle zeitnah erkannt werden. Neben den klassischen Komponenten wie Notstromversorgung und unterbrechungsfreie Stromversorgung tragen auch kleine Einzelfaktoren zu einer hohen Verfügbarkeit bei. Diese sind unter anderem Überspannungsschutzeinrichtungen, redundante Telekommunikations- und Mittelspannungseinspeisung, Spannungsausfallüberwachungen, Brückenschaltungen, lückenlose Dokumentation, Vorgaben und Verfahren zur Störungsbeseitigung sowie eine einheitliche Managementoberfläche für Sicherheit und Technik mit eindeutigen Interventionsvorgaben.



Bild 2 Kumuliertes Risiko

Sicherheit in Logistikzentren – Fachartikel GIT

Brandgefahr

Der Teil- oder Totalverlust durch Brand ist ein weiteres hohes Bedrohungspotenzial. Für die Brandfrüherkennung bieten sich gerade bei großen gedeckten Lagerflächen Rauchansaugsysteme (RAS) an. Die bereits in einer sehr frühen Phase entstehenden Rauch- und Brandgase werden durch die aktive Rauchansaugung auch bei hoher Packungsdichte in den Regalen rechtzeitig erkannt und gemeldet. Dank neuer Laser- und Scannertechnik werden Störgrößen wie beispielsweise Staub ausgefiltert. Drei Alarmstufen - Infoalarm, Voralarm und Hauptalarm - sind üblich. Anhand der ansteigenden Messwerte ist zu erkennen, ob es sich um eine echte Brandentwicklung handelt oder nicht. Lange bevor der eigentliche Brand in Form eines offenen Feuers entsteht, kann bereits reagiert werden und es bleibt genügend Zeit, den möglichen Brandherd zu verifizieren, zu beseitigen oder zu bekämpfen.

Fazit

Sicherheit muss systematisch konzipiert, richtig geplant, eingesetzt, praktiziert und vermarktet werden. Erst mit einer systematischen Vorgehensweise im Rahmen eines Schutzkonzeptes entsteht Transparenz hinsichtlich der Schutzziele, Schwachstellen, Risikopotenziale, Maßnahmen und der verbleibenden Restrisiken. Ein Sicherheitskonzept bietet die Grundlage für ein ökonomisches Sicherheits- und Risikomanagement. Damit ist Sicherheit messbare Wertschöpfung.

10 wichtige Thesen zur Sicherheit

1. Schutzziele und Gefahrenpotential genau bestimmen
2. Schwachstellen realistisch identifizieren
3. Risikopotential bewerten und dokumentieren
4. Maßnahmen lückenlos aufeinander abstimmen
5. Verbleibende Restrisiken genau bewerten
6. Erst planen - dann kaufen
7. Sicherheitstechnik sinnvoll einsetzen
8. Interventionsmaßnahmen planen
9. Mit regelmäßigen Revisionen die Qualität und die Investition sichern
10. Konsequentes Sicherheitsmanagement betreiben

KRAISS SECURITY CONSULT

Sandeldamm 16

63450 Hanau

Telefon 06181 / 78 05 35

Telefax 06181 / 78 05 65

Email kontakt@kraiss-consult.de

Website www.kraiss-consult.de