# Whitepaper

# Sicherheitskonzepte (KRITIS)

## Nutzen, Inhalt und Methodik

## Stand: November 2026

INHALTSVERZEICHNIS

**1 Management Summary ..... 4**
**2 KatS-Infrastruktur als besondere Schutzobjekte ..... 5**
2.1 Ein Ausfall hat sofort Außenwirkung ..... 5
2.2 Objektmerkmale, die den Schutzbedarf treiben ..... 5
2.3 Warum Einzelmaßnahmen hier besonders schlecht funktionieren ..... 6
**3 Was ist ein Sicherheitskonzept? ..... 7**
3.1 Definition ..... 7
3.2 Inhalte ..... 7
3.3 Brandschutz und IT ..... 8
3.4 Aufbau ..... 8
**4 Methodik ..... 9**
4.1 Vorbereitung: die Einleitung des Konzepts ..... 9
4.2 Schritt 1: Bedrohungen identifizieren ..... 9
4.3 Schritt 2: Täterprofile identifizieren ..... 9
4.4 Schritt 3: Verknüpfung und Relevanzbewertung ..... 10
4.5 Der Übergang zur Risikoanalyse ..... 11
**5 Schutzzieldefinition ..... 12**
**6 Schwachstellenanalyse ..... 13**
6.1 Die Schwachstellenanalyse ..... 13
6.2 Bewertung: zwei Größen ..... 13
6.3 Die Risikomatrix ..... 14
6.4 Vier Handlungsstrategien ..... 14
6.5 Beispiel einer Bewertung ..... 15
6.6 Zwischenergebnis ..... 15
**7 Womit wird geschützt? ..... 17**
7.1 Vier Maßnahmenebenen ..... 17
7.2 Die Wirkkette: Detektion, Verzögerung, Reaktion ..... 17
7.3 Integration statt Insellösungen ..... 18
7.4 Organisatorische Maßnahmen: Notfall- und Ablaufpläne ..... 18
7.5 Priorisierung: vom Risiko zur Umsetzungsreihenfolge ..... 18
7.6 Zwischenergebnis ..... 18
**8 Was die Umsetzung rechtlich begrenzt ..... 19**
8.1 Warum das gerade hier relevant ist ..... 19
8.2 Die datenschutzrechtliche Seite ..... 19

8.3 Die Beteiligung der Beschäftigtenvertretung ..... 19
8.4 Wirkung auf die Maßnahmenwahl ..... 20
8.5 Konsequenz für den Projektablauf ..... 20
**9 Prüfung, Übung, Fortschreibung ..... 21**
9.1 Wartung und Instandhaltung ..... 21
9.2 Wiederkehrende Prüfungen ..... 21
9.3 Übung ..... 21
9.4 Anlassbezogene Überprüfung ..... 22
9.5 Fortschreibung ..... 22
9.6 Zwischenergebnis ..... 22
**10 Wie ein Sicherheitskonzept entsteht ..... 23**
10.1 Die fünf Schritte ..... 23
10.2 Was der Auftraggeber beisteuert ..... 23
10.3 Welche Personen aus dem Haus einzubinden sind ..... 23
10.4 Was accellonet übernimmt ..... 24
10.5 Zeitlicher Rahmen ..... 24
**11 Was uns auszeichnet ..... 25**

## TABELLENVERZEICHNIS

Tabelle 1 Gefahrenbild als Matrix ..... 10
Tabelle 2 Matrix Schadensausmaß ..... 14
Tabelle 3 Matrix Eintrittswahrscheinlichkeit ..... 14
Tabelle 4 Risikomatrix ..... 14
Tabelle 5 Aufbau Ergebnistabelle ..... 15
Tabelle 6 Maßnahmenebenen ..... 17
Tabelle 7 Übersicht Maßnahmenwahl ..... 20
Tabelle 8 Anlassbezogene Überprüfung ..... 22
Tabelle 9 Übersicht Einbindung Abteilung/Stelle ..... 24

# 1 MANAGEMENT SUMMARY

Ein Sicherheitskonzept bzw. Sicherungskonzept ist das ganzheitliche Planungswerk, das den Schutz von Menschen, Objekten, Anlagen und Werten begründet. Es verbindet eine strukturierte Analyse der Gefahren mit aufeinander abgestimmten baulichen, technischen, organisatorischen und personellen Maßnahmen und beantwortet vier Fragen nachvollziehbar:

- Was soll geschützt werden?
- Wovor soll geschützt werden?
- Welcher Schutz ist bisher noch unzureichend?
- Durch welche angemessenen Maßnahmen lässt sich ein Schutz umsetzen?

Damit stellt das Sicherheitskonzept zugleich eine Entscheidungs-, Genehmigungs- und Betriebsgrundlage dar.

Für Entscheider ergeben sich somit folgende Vorteile aus der Erstellung eines Sicherheitskonzepts:

(1) Ökonomische Gründe: Ausgaben für Schutzmaßnahmen lassen sich gegenüber Kämmerei bzw. Controlling, Rechnungsprüfung und Buchhaltung leichter rechtfertigen, wenn ein dokumentiertes Schutzziel und eine belastbare Risikobewertung mit möglichen Schäden dahinterstehen. Das Sicherheitskonzept liefert diese Begründungskette.

(2) Rechtliche Vorgaben: Auf Bundesebene ist das KRITIS-Dachgesetz seit dem 17. März 2026 in Kraft. Es verpflichtet Betreiber kritischer Anlagen, etwa in den Sektoren Energie, Wasser, Gesundheit oder Transport und Verkehr, erstmals bundeseinheitlich zu Risikoanalysen und risikoreduzierenden Maßnahmen; die Betreiberpflichten greifen gestaffelt ab der Registrierung. Leitstellen, Feuerwehren und kommunale Rettungsdienste unterliegen als Einrichtungen der Länder, Landkreise und Kommunen nicht diesem Bundesrecht, erbringen aber gleichermaßen eine essenzielle Dienstleistung. Für sie ergibt sich der Handlungsbedarf aus Landesrecht, Trägerverantwortung und Fürsorgepflicht; das angemessene Schutzniveau ist dabei selbst festzulegen.

(3) Beschaffungsfähigkeit: Für Sicherheitstechnik, welche auf Basis konkret definierter Ziele beschafft wird, besteht eine höhere Wahrscheinlichkeit, dass die gewünschten Schutzziele erfüllt werden.

Dieses Whitepaper erläutert den methodischen Aufbau eines Sicherheitskonzepts und seine Ergebnisse sowie seine Erstellung durch die Fachplaner von accellonet. Es richtet sich an Entscheidungsträger in Industrieunternehmen und kritischen Infrastrukturen ebenso wie an Verantwortliche in Kommunen, Landkreisen und Zweckverbänden, die Leitstellen, Rettungs- und Feuerwachen, Gerätehäuser oder Einrichtungen des Katastrophenschutzes betreiben. Zudem ist es auf weitere Liegenschaften mit erhöhtem Schutzbedarf übertragbar.

Kernaussage: Ein Sicherheitskonzept an sich erzeugt noch keine Sicherheit. Es liefert jedoch Informationen darüber, welche Risiken existieren, und unterstützt bei den Entscheidungen, welche Risiken getragen und welche Maßnahmen ergriffen werden sollten.

# 2 KATS-INFRASTRUKTUR ALS BESONDERE SCHUTZOBJEKTE

Unabhängig davon, ob eine gesetzliche Pflicht besteht, ist der Schutzbedarf von Leitstellen und Infrastruktur des Katastrophenschutzes (KatS) zweifellos gegeben. Die Gründe werden in den folgenden Abschnitten erläutert; für Leitwarten und Betriebszentralen industrieller Betreiber gelten sie sinngemäß.

## 2.1 Ein Ausfall hat sofort Außenwirkung

Verwaltungsgebäude lassen sich im Störungsfall räumen, schließen und nach einigen Tagen wieder in Betrieb nehmen. Für Leitstellen kritischer Infrastruktur und Einrichtungen der nicht-polizeilichen Gefahrenabwehr gilt das nicht. Der Fokus des Betriebs liegt auf der Dienstleistung selbst: Die Aufgabengebiete der Notrufannahme, Disposition, Alarmierung und des Ausrückens sind essenzielle Bestandteile der Organisation. Von einem Ausfall ist nicht nur die Einrichtung betroffen, sondern auch die Bevölkerung im gesamten Versorgungsgebiet.

Die Planung eines Gebäudes umfasst nicht nur die Konzeption des Bauwerks selbst, sondern beinhaltet auch die Berücksichtigung der potenziellen Ausfallfolgen für das Gemeinwesen.

## 2.2 Objektmerkmale, die den Schutzbedarf treiben

Die folgenden Merkmale treten bei Leitstellen, Rettungs- und Feuerwachen sowie KatS-Einrichtungen typischerweise gemeinsam auf. Jedes einzelne ist beherrschbar; ihre Kombination erzeugt den erhöhten Schutzbedarf.

- **Technikkonzentration auf engem Raum**: Serverraum, Notstromaggregat, Klimatisierung usw. liegen oft in wenigen Räumen desselben Gebäudes. Wo Redundanz fehlt, entstehen Einzelfehlerstellen, deren Ausfall den Gesamtbetrieb beendet.
- **Dauerbetrieb bei Nachtbesetzung**: 24/7-Betrieb bedeutet auch: Zeiten, in denen wenige Personen anwesend sind und eine Eigensicherung faktisch nicht leisten können. Maßnahmen, die auf personelle Reaktion setzen, funktionieren nachts anders als tagsüber. Fehlen entsprechende Richtlinien und Arbeitsanweisungen, können Fehlentscheidungen in schwerwiegenden Konsequenzen resultieren.
- **Offene Liegenschaften mit Publikumsverkehr**: Rettungswachen und Gerätehäuser sind selten abgeschlossene Areale. Fahrzeughallen öffnen im Einsatzfall, Anlieferungen erfolgen laufend. Ein Perimeterschutz, der den Einsatzbetrieb behindert, wird im Betrieb umgangen und wird damit wirkungslos.
- **Wechselnde und heterogene Personengruppen**: Hauptamtliche im Schichtdienst, ehrenamtliche Kräfte, Praktikanten, Fremdfirmen, Wartungsdienste, Fahrzeugüberführungen. Schlüssel- und Zutrittsberechtigungen wachsen über Jahre an; wer aktuell Zutritt hat, ist ohne geregeltes Berechtigungsmanagement oft nicht mehr belastbar zu beantworten.
- **Attraktive Werte und Gefahrstoffe**: Die Lagerung von Betäubungsmitteln und Medizinprodukten, Funk- und Messtechnik, persönlicher Schutzausrüstung und Co. bieten finanzielle Anreize bei der Veräußerung. Diebstahl resultiert hier jedoch nicht nur in Vermögens- und Rufschaden, sondern kann die Einsatzbereitschaft unmittelbar einschränken und die Gesundheit der Einsatzkräfte gefährden.
- **Gewachsene Bausubstanz**: Viele Standorte wurden über Jahrzehnte durch Anbauten, Nutzungsänderungen und nachgerüstete Technik erweitert oder verändert; Brandabschnitte, Fluchtwegführung und Zonierung haben sich dabei mitverändert. In diesen Bereichen wurden die Schutzmaßnahmen jedoch nicht immer adäquat angepasst, was potenziell gefährliche Situationen für Personen und Wertgegenstände schaffen kann.

## 2.3 Warum Einzelmaßnahmen hier besonders schlecht funktionieren

In dieser Gemengelage ist die naheliegende Reaktion – eine Kamera hier, ein Zutrittsleser dort – besonders unwirksam. Der Grund ist nicht mangelnde Qualität der Einzelkomponenten, sondern das Fehlen einer gemeinsamen Zielsetzung: Solange nicht definiert ist, welche Zone welches Schutzziel hat, lässt sich nicht beurteilen, ob eine Kamera am richtigen Ort hängt, ob die Meldung irgendwo ankommt und ob jemand darauf reagieren kann und darf. Kapitel 6 zeigt, welche verketteten Schwachstellen daraus entstehen können.

# 3 WAS IST EIN SICHERHEITSKONZEPT?

## 3.1 Definition

Ein Sicherheitskonzept ist ein schriftlich dokumentiertes, ganzheitliches Planungswerk zum Schutz von Objekten, Anlagen, Menschen und Werten. Sein Kern ist die Verknüpfung einer strukturierten Analyse der Gefahren mit konkreten, aufeinander abgestimmten Schutzmaßnahmen aus Bau, Technik und Organisation.

Ganzheitlich heißt: Die Schutzebenen werden gemeinsam betrachtet, nicht gewerkeweise. Ein Zaun, eine Kamera und eine Dienstanweisung sind keine drei Projekte, sondern drei Beiträge zu demselben Schutzziel.

## 3.2 Inhalte

Für Gefahrenmeldeanlagen gibt DIN VDE 0833-1 die Mindestinhalte des Sicherungskonzepts vor, das Bestandteil des Sicherheitskonzepts ist:

„Das Sicherungskonzept muss mindestens Angaben enthalten über:

- die Gebäudenutzung,
- das Risiko für das Objekt,
- zu den Schutzzielen der Gefahrenmeldeanlage wie Personen- und/oder Sachschutz,
- den mit automatischen Meldern zu überwachenden Bereichen,
- den von Personen zu betätigenden nichtautomatischen Meldern,
- zu gegebenenfalls vorhandenen Steuerfunktionen,
- Personenschutzmaßnahmen,
- Alarmierungseinrichtungen,
- Alarmierungsbereichen,
- zu hilfeleistenden Stellen.“

Die geforderten Inhalte werden abgedeckt, wenn das Sicherungskonzept folgende Fragen beantworten kann:

- Was wird geschützt? Welche Personen, Räume, Anlagen, Daten und Funktionen sind Gegenstand des Schutzes und in welcher Rangfolge.
- Wovor? Welche Bedrohungen sind für dieses Objekt relevant, und welche nicht.
- Warum? Aus welchem Schutzziel, welcher Rechtspflicht, welcher Risikobewertung leitet sich der Aufwand ab.
- Wie? Mit welchen baulichen, technischen, organisatorischen und personellen Maßnahmen wird das Schutzziel erreicht.
- Was passiert im Ereignisfall? Welche Meldung (automatisch/manuell) löst was aus, welche Bereiche werden alarmiert, welche Steuerfunktionen greifen, und wer wird gemeldet bzw. wer interveniert?

## 3.3 Brandschutz und IT

Zwei Abgrenzungen verdienen besondere Aufmerksamkeit.

Da ist zum einen das Brandschutzkonzept, das im Widerspruch zum Sicherungskonzept stehen kann: Der Brandschutz will Menschen möglichst schnell hinausbringen, die Sicherungstechnik will Unbefugte draußen halten. Fluchttüren, Vereinzelungsanlagen und Zutrittskontrolle sind genau die Punkte, an denen sich beide Konzepte widersprechen können. Wo beide Dokumente unabgestimmt nebeneinanderstehen, entsteht entweder ein rechtliches Problem oder eine faktisch offene Tür. Hier gilt es, Kompromisse zu finden, die beidem gerecht werden. An dieser Stelle kommen unsere geschulten Fachberater ins Spiel, die mit technischen Lösungen oder Ideen für organisatorische Ansätze den Grat treffen, der dem Anspruch an Sicherheit und der Aufgabe, im Brandfall Menschenleben zu schützen, gerecht wird.

IT-Sicherheit hingegen ist ein eigenes Regime. Für Informationssicherheit gelten eigene Rahmenwerke und seit dem 6.12.2025 auch ein eigener gesetzlicher Rahmen, das NIS2-Umsetzungsgesetz, das ohne Übergangsfrist in Kraft trat. Physische und informationstechnische Sicherheit überschneiden sich jedoch an konkreten Stellen: Serverraum, Zutritt zu Technikräumen, Netzersatzanlage, Verkabelungswege. Das BSI adressiert genau diese Schnittmenge in den INF-Bausteinen des IT-Grundschutzes, unter anderem INF.1 Allgemeines Gebäude, INF.2 Rechenzentrum sowie Serverraum, INF.3 Elektrotechnische Verkabelung und INF.4 IT-Verkabelung. Ein Sicherheitskonzept ersetzt kein Informationssicherheitsmanagement – es liefert ihm aber die physische Grundlage. Um den Anforderungen des BSI baulich gerecht zu werden, berücksichtigt accellonet auch diese von Anfang an.

## 3.4 Aufbau

Ein Sicherheitskonzept folgt idealerweise einer festen Gliederung, die zugleich die Bearbeitungsreihenfolge abbildet:

(1) Einleitung und Objektbeschreibung: Zuerst wird das zu schützende Objekt beschrieben inklusive der geltenden und herangezogenen Regelwerke. Darüber hinaus wird aber auch der Betrachtungsumfang eingegrenzt sowie die beteiligten Parteien aufgelistet und in Beziehung zueinander gesetzt, beispielsweise als Organigramm.
(2) Durchführung einer Gefahrenanalyse: Diese besteht aus der Identifikation und Bewertung möglicher Bedrohungen und Täterprofile.
(3) Durchführung der Risikoanalyse für die vorab identifizierten Gefahren: Einteilung des Objekts in Sicherheitszonen, Definition zonenspezifischer Schutzziele, Identifikation von Schwachstellen und Durchführung einer Risikobewertung für diese Schwachstellen.
(4) Zusammenstellung von Maßnahmen zur Erfüllung der Schutzziele: Diese setzen sich zusammen aus baulichen (präventiven), technischen (detektierenden), organisatorischen (Handlungsvorgaben) und personellen Maßnahmen (Intervention), jeweils priorisiert.
(5) Anhang (optional): Umfangreiche Pläne, umfangreiche Zonenkarten, Bewertungstabellen und -matrizen, Regelwerksverzeichnis.

Die Reihenfolge ist nicht beliebig. Jeder Schritt setzt das Ergebnis des vorangegangenen voraus; eine Maßnahme ohne zugeordnete Schwachstelle und ohne nachgewiesenes Risiko aus der Risikobewertung ist im Nachhinein nicht begründbar.

# 4 METHODIK

Dieses Kapitel folgt der Bearbeitungsreihenfolge des Sicherheitskonzepts: erst wird erhoben, wovor zu schützen ist, dann wo und mit welchem Ziel, dann wie schwer das jeweilige Risiko wiegt, und erst zuletzt, mit welchen Mitteln.

Die Gefahrenanalyse steht am Anfang, weil sie den Betrachtungsraum aufspannt. Sie beantwortet nicht, wie gefährdet ein Objekt ist (das leistet erst die Risikoanalyse), sondern welche Bedrohungen überhaupt in Betracht kommen und welche begründet ausgeschlossen werden können. Der Ausschluss ist dabei genauso wichtig wie die Aufnahme: Ein Konzept, das jede denkbare Bedrohung mitführt, wird unbrauchbar, und eines, das eine relevante übersieht, ist wertlos.

## 4.1 Vorbereitung: die Einleitung des Konzepts

Vor der eigentlichen Analyse sind vier Festlegungen zu treffen, die im Kapitel „Einleitung und Objektbeschreibung“ dokumentiert werden und den gesamten weiteren Verlauf bestimmen.

Zu klären ist erstens, wer beteiligt ist: Träger, Betreiber, Nutzer, Fachämter, gegebenenfalls Mitnutzer derselben Liegenschaft, usw. Zweitens, welches Objekt betrachtet wird und wo die Grenze des Betrachtungsraums liegt: Gebäude, Liegenschaft, Perimeter, angrenzende Flächen, mitgenutzte Zufahrten. Drittens, was der Anlass ist: Neubau, Umbau, Audit, Kooperationsvorhaben, Fördermittelantrag oder ein konkreter Vorfall; der Anlass bestimmt den Detaillierungsgrad. Und viertens, welche Regelwerke herangezogen werden.

## 4.2 Schritt 1: Bedrohungen identifizieren

Die Erhebung der Bedrohungen erfolgt strukturiert entlang dreier Ursachenkategorien. Die Kategorisierung ist kein Selbstzweck: Sie verhindert, dass die Betrachtung bei den naheliegenden Szenarien stehenbleibt, und sie erleichtert später die Zuordnung zu Maßnahmenebenen, weil verschiedene Ursachen verschiedene Gegenmaßnahmen erfordern.

Naturereignisse umfassen Blitzschlag, Hochwasser, Starkregen, Sturm, Erdbeben und vergleichbare Einwirkungen. Ihre Relevanz ist stark standortabhängig: Ein Kellerstandort in einem Überschwemmungsgebiet ist anders zu bewerten als ein Obergeschoss in Hanglage. Für Leitstellen ist der mittelbare Weg oft kritischer als der unmittelbare: Nicht das Wasser im Technikraum ist das wahrscheinlichste Szenario, sondern der Ausfall der Zuwegung, der Stromversorgung oder der Anbindung.

Technische Gefahren umfassen Brand, Unfall, technischer Ausfall, Ausfall der Energieversorgung, Havarie an haustechnischen Anlagen. Hier liegt bei Einrichtungen mit Technikkonzentration typischerweise der Schwerpunkt – und hier fallen auch die Wechselwirkungen an, die in reinen Brandschutzbetrachtungen nicht auftauchen: Löschwasser, das Technik zerstört, die es zu schützen galt.

Vorsätzliche Handlungen umfassen Sabotage, Raub und Diebstahl, Vandalismus, Einbruch und unbefugten Zutritt, Brandstiftung, Bedrohung und Übergriffe auf Beschäftigte. Diese Kategorie unterscheidet sich von den beiden anderen grundlegend: Sie setzt einen handelnden Akteur voraus, der Gegenmaßnahmen umgehen kann.

## 4.3 Schritt 2: Täterprofile identifizieren

Bedrohungen durch Täter lassen sich nicht sinnvoll bewerten, ohne zu betrachten, wer sie ausführt. Ein und dasselbe Ereignis, etwa ein unbefugter Zutritt zum Technikraum, hat abhängig vom Täterprofil völlig unterschiedliche Eintrittswahrscheinlichkeiten, Vorgehensweisen und Gegenmaßnahmen.

Typische Profile sind unzufriedene eigene Mitarbeitende, externe Mitarbeitende und

Fremdfirmen mit legitimem Zutritt, Gelegenheitstäter, politisch motivierte Akteure sowie organisierte Kriminalität. Sie unterscheiden sich in drei Dimensionen, die für die Maßnahmenwahl entscheidend sind: Vorwissen über das Objekt, Zugangsberechtigung und Mittel- sowie Zeitaufwand, den sie einzusetzen bereit sind.

Daraus folgt eine Konsequenz, die bei Einrichtungen der Gefahrenabwehr besonders schwer zu vermitteln ist: Der Innentäter ist der planerisch anspruchsvollste Fall. Er kennt die Abläufe, besitzt Zutritt und weiß, welche Anlage wann unscharf ist. Perimeterschutz wirkt gegen ihn nicht. Wirksam sind hier andere Mittel: Zonierung innerhalb des Gebäudes, protokollierte Zutrittsberechtigungen, Vier-Augen-Regelungen, Berechtigungsentzug bei Personalwechsel. Wer diesen Fall nicht betrachtet, plant an einer relevanten Bedrohung vorbei. Die Betrachtung erfolgt dabei nicht als Verdacht gegen Beschäftigte, sondern als planerische Annahme.

## 4.4 Schritt 3: Verknüpfung und Relevanzbewertung

Bedrohungen und Täterprofile werden anschließend in einer Matrix zusammengeführt und liefern das Gefahrenbild. Für jede Bedrohung wird gekennzeichnet, welche Täterprofile als Verursacher in Betracht kommen, und die Bedrohung wird in ihrer Relevanz eingestuft: unkritisch, relevant oder kritisch.

Die Darstellung als Matrix hat einen praktischen Grund: Sie macht sowohl die belegten als auch die leeren Felder sichtbar. Eine Bedrohung ohne zugeordnetes Täterprofil ist entweder ein Naturereignis oder ein Hinweis darauf, dass die Täterbetrachtung unvollständig ist. Ein Täterprofil ohne zugeordnete Bedrohung wirft die Frage auf, warum es aufgenommen wurde.

Die folgende Darstellung zeigt den Aufbau schematisch; die Einträge sind beispielhaft und ersetzen keine objektbezogene Bewertung.

| Bedrohung | Unzufriedene Mitarbeitende | Externe / Fremdfirmen | Gelegenheitstäter | Organisierte Kriminalität | Relevanz |
|---|---|---|---|---|---|
| Starkregen / Hochwasser | — | — | — | — | relevant |
| Ausfall der Energieversorgung | — | — | — | — | kritisch |
| Brand (technische Ursache) | — | — | — | — | kritisch |
| Brandstiftung | X | X | X | — | relevant |
| Einbruch und unbefugter Zutritt | X | X | X | X | kritisch |
| Sabotage an Technikanlagen | X | X | — | X | relevant |
| Übergriff auf Beschäftigte | — | — | X | — | relevant |

**Tabelle 1 Gefahrenbild als Matrix**

Die Einstufung in der rechten Spalte ist noch keine Risikobewertung. Sie beantwortet ausschließlich die Frage, ob eine Bedrohung im weiteren Verlauf des Konzepts vertieft betrachtet wird. Als unkritisch eingestufte Bedrohungen werden mit Begründung dokumentiert und dann nicht weiterverfolgt, dieser dokumentierte Ausschluss ist Teil der Nachweisführung und gehört ausdrücklich ins Konzept.

## 4.5 Der Übergang zur Risikoanalyse

Das Ergebnis dieses Kapitels ist eine begründete Liste relevanter und kritischer Bedrohungen mit zugeordneten Täterprofilen und eine ebenso begründete Liste dessen, was nicht weiter betrachtet wird.

Was damit noch nicht beantwortet ist: wo im Objekt diese Bedrohungen wirken, was dort konkret geschützt werden soll, und wie schwer ein Schaden dort wäre. Diese drei Fragen behandeln die folgenden beiden Kapitel.

# 5 SCHUTZZIELDEFINITION

Nachdem klar ist, wovor zu schützen ist, wird im nächsten Schritt definiert, was konkret eigentlich geschützt werden muss. Die Schutzzieldefinition erfordert eine enge Zusammenarbeit zwischen Fachberater und Objektverantwortlichem.

Am Anfang steht die Besinnung auf die obersten Schutzgüter: Menschen, Sach- und Vermögenswerte sowie Ordnung und Rechte. Ausgelöst wird die Formulierung von Schutzzielen durch unterschiedliche Treiber: den betrieblichen Selbstschutz, die Fürsorgepflicht des Arbeitgebers, Auflagen von Kunden und gegebenenfalls gesetzliche Vorschriften. In der Praxis steht dabei die Wirtschaftlichkeit in der Regel im Vordergrund; ein Hinweis darauf, dass Schutzziele nicht beliebig hoch gesteckt, sondern gegen Aufwand und Nutzen abgewogen werden.

Methodisch wird zweistufig vom Groben ins Feine gearbeitet. Grobziele benennen die Schutzrichtung noch unscharf, etwa die Dokumentation der Grundstücksgrenze, den Schutz vor unbefugtem Zutritt, vor Einbruch und Diebstahl oder vor Vandalismus. Für Einrichtungen der KRITIS reicht das Spektrum vom Schutz vor betrieblichem Ausfall über den Schutz vor unbefugtem Zutritt und vor Vandalismus/Sabotage bis zum Schutz vor Ausspähung/Spionage sowie vor Einbruch und Diebstahl. Solche Grobziele machen die Stoßrichtung sichtbar, taugen aber noch nicht als Planungs- oder Prüfmaßstab.

Deshalb werden sie zu Feinzielen zugespitzt. Als Qualitätsraster dient hier das SMART-Prinzip: Ein Feinziel soll spezifisch (das Ziel deutlich beschrieben), messbar (Erfolg objektiv erkennbar), ausführbar (mit den vorhandenen Mitteln erreichbar), realistisch (sicher erreichbar) und terminiert (mit festem Zeitrahmen) sein. Der Nutzen liegt in der Messbarkeit: Nur ein spezifisch und messbar formuliertes Schutzziel lässt sich später gegen die realisierte Technik und Organisation prüfen. Auf diese Weise wird Sicherheit nachweisbar.

Schutzziele werden Bereichen zugeordnet. Dafür hat sich als Methodik das Zonenmodell bewährt: Dabei wird der zugelassene Personenkreis von außen nach innen gestaffelt. Zone 0 als öffentlicher Bereich (jedermann), Zone 1 als frei zugänglicher, aber nicht öffentlicher Bereich (z. B. Grundstück, Parkplatz), Zone 2 als betrieblicher Bereich (nur Mitarbeitende, Dienstleister, Handwerker, Lieferanten) und Zone 3 als eigentlicher Schutzbereich (nur bestimmte Mitarbeitende, Externe ausschließlich in Begleitung). Je weiter innen, desto höher das Schutzniveau.

Die Schutzzonen selbst werden in enger Abstimmung mit dem Auftraggeber erstellt, insbesondere für Objekte der KRITIS werden erfahrungsgemäß oft vier oder sogar fünf Zonen definiert.

# 6 SCHWACHSTELLENANALYSE

Nach Zonierung und Schutzzieldefinition steht fest, was wo erreicht werden soll. Dieses Kapitel beantwortet die Frage, ob es im heutigen Zustand erreicht wird und wo nicht, wie dringend der Handlungsbedarf ist. Es besteht aus zwei aufeinander aufbauenden Schritten: dem Auffinden der Schwachstellen und ihrer Bewertung.

## 6.1 Die Schwachstellenanalyse

Die Leitfrage lautet schlicht: Was kann wo schieflaufen? Genauer: An welche Möglichkeiten des Eintretens von Schäden wurde bisher noch nicht gedacht? Die Analyse zielt also ausdrücklich nicht auf die bekannten Defizite – die stehen ohnehin auf der Mängelliste –, sondern auf das, was trotz der bisher getroffenen Maßnahmen an Schäden entstehen kann.

Kennzeichnend für die Ergebnisse ist, dass es sich meist um eine Kombination aus kleineren Ursachen handelt, die zusammen schwere Konsequenzen haben können. Einzelne Ursachen sind in aller Regel durch Normen, Prüfungen und Abnahmen abgedeckt; ihre Verkettung ist es nicht.

Zwei Beispiele illustrieren das Muster. Ein fehlender Sabotageschutz an einer Videokamera ist für sich genommen ein Detail. In Verbindung mit einem unbeobachteten Anfahrtsweg und einer nicht überwachten Meldung wird daraus ein vollständiger Umgehungspfad. Ebenso die Steuerung einer Einbruchmeldeanlage, die außerhalb des von ihr überwachten Bereichs montiert ist: Jede Komponente arbeitet bestimmungsgemäß, die Anlage ist abgenommen und lässt sich dennoch unterlaufen, ohne den überwachten Bereich zu betreten.

Dieser Arbeitsschritt ist die kreative Königsdisziplin bei der Erstellung eines Sicherheitskonzepts. Er lässt sich nicht durch Checklisten ersetzen, weil Checklisten genau das abfragen, woran bereits gedacht wurde. Detailwissen über das Objekt und über mögliche Gefahren ist hier sinnvoll bis notwendig und er erfordert eine Begehung vor Ort. Aus Plänen allein ist nicht erkennbar, welche Tür im Betrieb dauerhaft verkeilt ist, welcher Melder durch ein Regal verdeckt wurde und welche Sicherheitsüberprüfung regelmäßig umgangen wird, weil der offizielle Weg zu lang ist.

## 6.2 Bewertung: zwei Größen

Jede gefundene Schwachstelle wird anschließend über zwei Größen bewertet: Wie schwerwiegend wäre der Schaden, und wie oft ist mit ihm zu rechnen. Die Bewertung erfolgt anhand definierter Stufen, damit sie zwischen verschiedenen Schwachstellen und verschiedenen Bearbeitern vergleichbar bleibt.

Das Schadensausmaß wird an der Betreibbarkeit der Anlage und an der Qualität der erbrachten Dienstleistung festgemacht, also an der Auswirkung auf die Aufgabe, nicht am Sachwert. Die folgende Tabelle zeigt die Einstufung beispielhaft:

| Stufe | Bezeichnung | Auswirkung |
|---|---|---|
| S1 | gering | Anlage mindestens im Standardmodus betreibbar, geringe Einschränkung der Dienstleistungsqualität |
| S2 | mäßig | Anlage nicht mehr vollständig betreibbar, Dienstleistungsqualität merklich eingeschränkt, Qualität unterhalb der Grenzen |
| S3 | hoch | Anlage nur noch teilweise betreibbar, Dienstleistung nur noch teilweise möglich, Qualität erheblich unterhalb der Grenzen |

| Stufe | Bezeichnung | Auswirkung |
|---|---|---|
| S4 | kritisch | Anlage nicht mehr betreibbar, Dienstleistung kann nicht mehr erbracht werden |

**Tabelle 2 Matrix Schadensausmaß**

Analog dazu wird die Eintrittswahrscheinlichkeit geschätzt, wobei eine Häufigkeit leichter zu ermitteln ist als eine prozentuale Wahrscheinlichkeit.

| Stufe | Bezeichnung | Häufigkeit |
|---|---|---|
| W1 | sehr gering | seltener als einmal in fünf Jahren |
| W2 | mittel | bis zu einmal im Jahr |
| W3 | hoch | bis zu dreimal im Jahr |
| W4 | sehr hoch | mehr als dreimal im Jahr |

**Tabelle 3 Matrix Eintrittswahrscheinlichkeit**

Beide Bewertungen sind Schätzungen. Das ist kein Mangel des Verfahrens, sondern seine Voraussetzung, denn belastbare Eintrittsstatistiken existieren für die meisten hier betrachteten Ereignisse nicht. Entscheidend ist deshalb nicht die Genauigkeit der einzelnen Zahl, sondern dass alle Schwachstellen nach demselben Maßstab bewertet werden und die Einstufung nachvollziehbar dokumentiert ist.

## 6.3 Die Risikomatrix

Aus beiden Größen wird eine Risikozahl gebildet, die die Schwachstellen in eine Rangfolge bringt. Die Bewertung erfolgt methodisch angelehnt an DIN EN IEC 31010.

Das Schadensausmaß wird dabei nicht linear, sondern gespreizt gewichtet (mit den Werten 1, 3, 5 und 7), während die Wahrscheinlichkeit mit 1 bis 4 eingeht. Diese Spreizung ist eine bewusste Entscheidung: Sie sorgt dafür, dass ein zwar seltenes, aber existenzbedrohendes Ereignis nicht von einem häufigen Bagatellereignis überholt wird.

| | W1 = 1 | W2 = 2 | W3 = 3 | W4 = 4 |
|---|---|---|---|---|
| S4 = 7 | 7 | 14 | 21 | 28 |
| S3 = 5 | 5 | 10 | 15 | 20 |
| S2 = 3 | 3 | 6 | 9 | 12 |
| S1 = 1 | 1 | 2 | 3 | 4 |

**Tabelle 4 Risikomatrix**

Über die Matrix wird eine Risikoakzeptanzschwelle gelegt. Sie ist keine Rechengröße, sondern eine Festlegung des Trägers: Bis zu welchem Wert wird ein Risiko ohne weitere Maßnahmen getragen? Diese Schwelle gehört dokumentiert und freigegeben, weil sie die Grenze zwischen „akzeptiert“ und „handlungsbedürftig“ definiert und damit den Umfang des Maßnahmenkatalogs bestimmt.

## 6.4 Vier Handlungsstrategien

Die Position einer Schwachstelle in der Matrix führt zu einer von vier Strategien. Dass es mehrere und nicht nur eine gibt, ist der für Entscheider wichtigste Punkt, denn nicht jedes erkannte Risiko muss durch eine Investition beantwortet werden.

**Akzeptanz**: geringes Ausmaß, geringe Wahrscheinlichkeit. Das Risiko wird bewusst getragen. Die Entscheidung wird dokumentiert; damit ist sie eine Entscheidung und kein Versäumnis.

**Reduktion**: hohe Wahrscheinlichkeit bei begrenztem Ausmaß. Ziel ist die Senkung der Eintrittswahrscheinlichkeit durch bauliche, technische oder organisatorische Maßnahmen. Dies ist der Regelfall und führt zum Maßnahmenkatalog.

**Vermeidung**: hohes Ausmaß bei hoher Wahrscheinlichkeit. Die risikobehaftete Nutzung oder Anordnung wird aufgegeben oder grundlegend verändert, etwa durch die Verlagerung eines Technikraums aus einem hochwassergefährdeten Untergeschoss. Planerisch ist dies die wirksamste Strategie, im Bestand jedoch häufig die aufwendigste.

**Übertragung**: hohes Ausmaß bei geringer Wahrscheinlichkeit. Die finanziellen Folgen werden ganz oder teilweise auf Dritte übertragen, etwa durch Versicherungen oder vertragliche Regelungen mit Dienstleistern. Die Einsatz- bzw. Betriebsfähigkeit selbst lässt sich nicht übertragen; diese Strategie ist daher nur ergänzend geeignet.

## 6.5 Beispiel einer Bewertung

Die folgende Zusammenstellung zeigt den Aufbau der Ergebnistabelle anhand eines typischen, anonymisierten Beispiels: einer Leitstelle mit angeschlossener Feuer- und Rettungswache. Sie verdeutlicht zwei Punkte: wie unterschiedlich gleichartige Schwachstellen ausfallen können und dass mittelbare Folgen ebenso zu bewerten sind.

| Schwachstelle | Ausmaß (1…7) | Wahrscheinlichkeit (1…4) | Gesamtrisiko |
|---|---|---|---|
| Brandfallsteuerung schaltet die Klimatisierung des Serverraums mit ab; Überhitzung der Systemtechnik bei Fehlalarm | 7 | 3 | 21 |
| Zutritt zum Technikraum (USV, Server) über mechanische Schlüssel, Verbleib der Schlüssel nicht nachvollziehbar | 7 | 2 | 14 |
| Rolltor der Fahrzeughalle bleibt nach dem Ausrücken offen, keine Schließüberwachung | 3 | 4 | 12 |
| Betäubungsmittelschrank der Rettungswache ohne Einbruchmeldung | 5 | 2 | 10 |
| Fehlender Rauchmelder im Batterieraum der USV | 7 | 1 | 7 |
| Videokamera an der Zufahrt ohne Sabotageerkennung, Bild nicht aufgeschaltet | 3 | 2 | 6 |
| Fehlender Rauchmelder im Lager für Verbrauchsmaterial | 1 | 2 | 2 |

**Tabelle 5 Aufbau Ergebnistabelle**

Aufschlussreich ist die Spreizung innerhalb derselben Schwachstellenart: Fehlende Rauchmelder ergeben je nach Raum Werte zwischen 2 und 7. Ausschlaggebend ist, was der betroffene Raum für die Betriebsfähigkeit bedeutet. Ebenso bemerkenswert ist, dass die höchste Bewertung in diesem Beispiel nicht auf ein Schadensereignis entfällt, sondern auf eine Folge der Brandfallsteuerung, also einer Schutzmaßnahme selbst. Genau solche Wechselwirkungen bleiben unentdeckt, wenn Brandschutz und Sicherungstechnik getrennt betrachtet werden.

## 6.6 Zwischenergebnis

Nach diesem Schritt muss eine vollständige Schwachstellenliste vorliegen, je Schwachstelle

eine dokumentierte Bewertung beider Größen, die daraus gebildete Risikozahl, die festgelegte Akzeptanzschwelle sowie die zugeordnete Handlungsstrategie.

Damit ist die Grundlage für die Maßnahmenplanung gelegt und zugleich die Begründungskette geschlossen. Welche konkreten Maßnahmen daraus folgen, beschreibt Kapitel 7.

# 7 WOMIT WIRD GESCHÜTZT?

Erst an dieser Stelle des Konzepts geht es um Technik. Das ist kein Zufall der Gliederung, sondern ihr Zweck: Jede Maßnahme dieses Kapitels lässt sich auf ein Schutzziel aus Kapitel 5 und eine bewertete Schwachstelle aus Kapitel 6 zurückführen. Diese Rückführbarkeit ist die Eigenschaft, die das Dokument prüffähig macht – und sie ist der Grund, weshalb der Maßnahmenkatalog nicht am Anfang stehen kann.

## 7.1 Vier Maßnahmenebenen

Maßnahmen werden auf vier Ebenen geplant, die jeweils eine andere Wirkung entfalten. Die Unterscheidung zeigt, dass ein Schutzziel in der Regel auf mehreren Wegen erreichbar ist und dass die Wahl zwischen ihnen eine wirtschaftliche und betriebliche Entscheidung ist, keine technische.

| Ebene | Wirkprinzip | Typische Maßnahmen |
|---|---|---|
| Mechanisch/baulich | Widerstandswert, Verzögerung | Mauern, Zäune, Umzäunung und Perimeter, einbruchhemmende Bauteile, Flucht- und Rettungswege, Brandabschnitte |
| Elektronisch/technisch | frühzeitige Erkennung, Meldung | Einbruchmeldeanlage, Videosicherheit, Zutrittskontrolle und Vereinzelung, Brandmeldeanlage, Sicherheitsbeleuchtung, Gefahrenmanagement und Aufschaltung |
| Organisatorisch | sicherer Betrieb, geregelte Abläufe | Zuständigkeiten, Zutritts- und Schlüsselregelungen, Alarmierungs- und Notfallpläne, Schulungen und Unterweisungen, Arbeitsanweisungen |
| Personell | Intervention | Definition der Interventionskräfte, etwa Polizei, Feuerwehr, beauftragter Sicherheitsdienst |

**Tabelle 6 Maßnahmenebenen**

Für Entscheider in Verwaltung und Unternehmen ist die dritte Zeile die wichtigste. Organisatorische Maßnahmen verursachen keine Investition, sondern Aufwand im laufenden Betrieb und sind im Haushalt bzw. Budget anders zu behandeln und personell zu unterlegen. Sie sind zugleich der Teil des Maßnahmenkatalogs, der nach Projektabschluss regelmäßig als Erstes verfällt, wenn ihn niemand pflegt.

## 7.2 Die Wirkkette: Detektion, Verzögerung, Reaktion

Die vier Ebenen wirken nicht nebeneinander, sondern in einer Kette. Erst das Zusammenspiel ergibt wirksamen Schutz.

Detektion bedeutet, dass eine Gefahr früh erkannt wird, beispielsweise durch Einbruchmeldeanlage, Brandmeldeanlage oder Videotechnik. Verzögerung bedeutet, dass bauliche und mechanische Hürden Zeit erzeugen. Reaktion bedeutet Alarmierung, Aufschaltung und Intervention durch Kräfte, die eintreffen und handeln können.

Der Zusammenhang zwischen diesen drei Gliedern ist quantitativ und lässt sich in einem Satz prüfen: Die Verzögerungszeit muss mindestens so lang sein wie die Zeit von der Detektion bis zum Wirksamwerden der Interventionskräfte. Ist sie kürzer, ist der Schaden eingetreten, bevor jemand vor Ort ist. Im schlimmsten Fall dokumentiert die Anlage dann nur noch ein Ereignis, statt es zu verhindern.

Diese Prüfung ist der eigentliche Bemessungsvorgang der Sicherungsplanung, und sie hat zwei praktische Konsequenzen. Erstens ist die Interventionskraft mit ihrer realistischen Eintreffzeit vor der Auswahl der Technik festzulegen, nicht danach. Zweitens verändert jede

Änderung auf einer Seite die Anforderung auf der anderen: Verlängert sich die Eintreffzeit, etwa weil eine Aufschaltung wegfällt oder ein Streifendienst reduziert wurde, steigt der erforderliche mechanische Widerstandswert.

Für Einrichtungen mit Nachtbesetzung kommt hinzu, dass die Reaktionsfähigkeit tageszeitabhängig ist. Ein Konzept, das nur den Tagbetrieb vorsieht, bemisst die Verzögerung zu kurz.

## 7.3 Integration statt Insellösungen

Einzelanlagen, die nicht zusammengeführt werden, erzeugen Folgeaufwand: mehrere Bedienplätze, getrennte Berechtigungen, separate Wartungsverträge und Störungsmeldewege. Die Zusammenführung erfolgt über vier Elemente.

Ein Gefahrenmanagementsystem dient als zentrale Oberfläche, auf der Meldungen aller angeschlossenen Anlagen auflaufen und bearbeitet werden. Die Aufschaltung auf eine Leitstelle oder eine Notruf- und Serviceleitstelle stellt sicher, dass Meldungen auch dann einen Empfänger finden, wenn vor Ort niemand anwesend ist. Schnittstellen zu Gebäude- und IT-Systemen verhindern, dass Sicherungstechnik parallel zu bestehender Infrastruktur betrieben wird. Und die normkonforme Planung (z. B. nach einschlägigen DIN-/VDE-Normen und VdS-Richtlinien) stellt die Vergleichbarkeit von Angeboten und die Prüffähigkeit der Ausführung sicher.

## 7.4 Organisatorische Maßnahmen: Notfall- und Ablaufpläne

Notfall- und Ablaufpläne legen fest, wer im Ereignisfall was tut, schnell und ohne Zögern. Sie umfassen die Alarmierungskette, also wer wann und wie informiert wird; die Evakuierung mit Flucht- und Rettungswegen und Sammelplätzen; die Zuständigkeiten mit klaren Rollen und Verantwortlichen; die Kommunikation intern und mit Behörden und Rettungskräften; sowie die Übung, denn regelmäßige Tests sichern die Wirksamkeit.

Der letzte Punkt entscheidet über den Wert der bisher genannten: Ein Notfallplan, der nicht geübt wurde, ist lediglich eine Absichtserklärung. Bei Einrichtungen mit Schichtbetrieb und ehrenamtlichem Personal kommt hinzu, dass eine einmalige Unterweisung nicht ausreicht, da der Personalkörper schneller wechselt als das Dokument.

## 7.5 Priorisierung: vom Risiko zur Umsetzungsreihenfolge

Der Maßnahmenkatalog ist das Ergebnis der Risikomatrix. Maßnahmen werden nicht gleichrangig aufgelistet, sondern nach der Risikozahl geordnet, die ermittelt wurde. Daraus entsteht eine Umsetzungsreihenfolge, die zwei Zwecke erfüllt.

Sie ermöglicht erstens eine Umsetzung über mehrere Haushalts- bzw. Geschäftsjahre, ohne dass die Reihenfolge jedes Jahr neu verhandelt werden muss. Sie liefert zweitens die Begründung dafür, warum eine bestimmte Maßnahme jetzt und eine andere später erfolgt.

Für jede Maßnahme sind dabei anzugeben: Das adressierte Schutzziel, die adressierte Schwachstelle, die Maßnahmenebene, die zuständige Stelle, die Auswirkung auf die Risikobewertung und der Aufwand, sowohl investiv als auch betrieblich. Nicht umgesetzte Maßnahmen werden mit Begründung und dem verbleibenden Restrisiko dokumentiert.

## 7.6 Zwischenergebnis

Nach diesem Schritt liegt ein priorisierter Maßnahmenkatalog vor, in dem jede Maßnahme auf Schutzziel und Schwachstelle zurückgeführt ist, sowie eine dokumentierte Restrisikoübersicht.

Damit ist das Sicherheitskonzept zwar inhaltlich vollständig, aber noch nicht wirksam. Es fehlen noch die rechtlichen Randbedingungen, unter denen die Maßnahmen überhaupt eingeführt werden dürfen und die Frage, wie das Konzept im laufenden Betrieb gültig bleibt.

# 8 WAS DIE UMSETZUNG RECHTLICH BEGRENZT

Der Maßnahmenkatalog beschreibt, was fachlich erforderlich ist. Ob es auch zulässig und durchsetzbar ist, entscheidet sich an zwei Stellen, die außerhalb der Sicherungsplanung liegen: im Datenschutzrecht und in der Beteiligung der Personalvertretung bzw. des Betriebsrats.

Für öffentliche wie private Auftraggeber ist das keine Randbedingung, sondern ein Projektrisiko. Videoüberwachung und elektronische Zutrittskontrolle erfassen personenbezogene Daten, überwiegend von den eigenen Beschäftigten. Wer diese Beteiligungen erst nach der Vergabe einleitet, riskiert, dass eine bereits beschaffte Anlage nicht oder nur eingeschränkt in Betrieb gehen darf.

## 8.1 Warum das gerade hier relevant ist

In einer Leitstelle oder auf einer Rettungswache fällt zusammen, was sonst getrennt liegt. Die Räume, in denen der Schutzbedarf am höchsten ist, sind zugleich die Räume, in denen Beschäftigte ihren Dienst verrichten: Einsatzleitplatz, Technikraum, Fahrzeughalle, Eingangsbereich. Eine Kamera, die den Zugang zum Technikraum überwacht, erfasst damit zwangsläufig auch, wer dort wann wie lange gearbeitet hat. Eine Zutrittskontrolle, die unbefugten Zugang verhindern soll, erzeugt als Nebenprodukt eine Bewegungshistorie des Personals.

Diese Doppelwirkung ist technisch nicht vermeidbar, aber planerisch gestaltbar, vorausgesetzt, sie wird vor der Festlegung der Maßnahme betrachtet und nicht danach.

## 8.2 Die datenschutzrechtliche Seite

Vier Fragen sind vor der Maßnahmenfestlegung zu klären, und zwar je Maßnahme, nicht pauschal für das Projekt.

Zu klären ist erstens die Rechtsgrundlage: Auf welcher Grundlage werden die Daten verarbeitet? Zweitens die Erforderlichkeit: Gibt es ein milderes Mittel, das dasselbe Schutzziel erreicht? Ein baulicher Verschluss erreicht denselben Zweck wie eine Kamera, ohne Daten zu erzeugen, bringt aber gegebenenfalls andere Nachteile mit sich, die überwiegen. Genau diese Abwägung gehört dokumentiert. Drittens die Zweckbindung: Wofür dürfen die Daten verwendet werden, und wofür ausdrücklich nicht? Viertens die Speicherdauer: Wie lange werden Aufzeichnungen vorgehalten, und wie wird gelöscht?

Hinzu kommen die Transparenzanforderungen, denen mit Hinweisbeschilderung, Information der Betroffenen, Eintrag im Verarbeitungsverzeichnis begegnet werden kann, sowie die Frage, ob für die geplante Verarbeitung eine Datenschutz-Folgenabschätzung durchzuführen ist. Bei umfangreicher systematischer Überwachung öffentlich zugänglicher Bereiche ist damit regelmäßig zu rechnen.

Der praktische Rat lautet: Die oder der behördliche bzw. betriebliche Datenschutzbeauftragte wird vor der Maßnahmenfestlegung eingebunden, nicht vor der Inbetriebnahme. Die Einbindung kostet im Planungsstadium Tage, nach Beschaffung Monate.

## 8.3 Die Beteiligung der Beschäftigtenvertretung

Einrichtungen, die zur Überwachung von Verhalten oder Leistung der Beschäftigten geeignet sind, unterliegen typischerweise der Mitbestimmung der Personalvertretung bzw. in Unternehmen des Betriebsrats (§ 87 Abs. 1 Nr. 6 BetrVG). Maßgeblich ist dabei die Eignung: Dass eine Zutrittskontrolle zur Zugangssicherung und nicht zur Arbeitszeiterfassung beschafft wurde, ändert nichts daran, dass sie dazu geeignet wäre.

Betroffen sind damit praktisch alle Maßnahmen der elektronischen Ebene, also Videosicherheit, Zutrittskontrolle, teilweise auch Gefahrenmanagementsysteme mit Protokollfunktion. Der übliche Lösungsweg ist eine Dienst- bzw. Betriebsvereinbarung, die Zweck, Umfang,

Auswertungsbefugnisse, Beteiligung bei Auswertung und Löschfristen regelt. Sie zu verhandeln braucht Zeit; diese Zeit gehört in den Projektterminplan.

## 8.4 Wirkung auf die Maßnahmenwahl

Die folgende Tabelle ordnet die Maßnahmenarten aus Kapitel 7 danach ein, wie stark sie Datenschutz und Mitbestimmung berühren, und zeigt, welche Festlegungen das Sicherheitskonzept dafür bereits treffen sollte. Sie ist als Arbeitshilfe für die Projektplanung gedacht, nicht als rechtliche Prüfung.

| Maßnahme | Datenschutz-relevanz | Mitbestimmung wahrscheinlich ? | Im Konzept festzulegen |
|---|---|---|---|
| Videosicherheit Perimeter/Außenhaut | hoch | ja | Erfassungsbereiche, Speicherdauer, Auswertungsanlässe |
| Videosicherheit Innenbereich | sehr hoch | ja | Erforderlichkeitsbegründung je Kamera, Ausschluss von Arbeitsplätzen |
| Elektronische Zutrittskontrolle | hoch | ja | Protokollumfang, Auswertungsbefugnis, Löschfristen |
| Einbruch- und Brandmeldeanlage | gering | im Einzelfall | Zuordnung von Meldungen zu Personen vermeiden |
| Mechanische Sicherung, bauliche Maßnahmen | keine | nein | — |
| Organisatorische Regelungen (Zutritt, Schlüssel) | mittel | im Einzelfall | Umfang personenbezogener Führung von Berechtigungslisten |

**Tabelle 7 Übersicht Maßnahmenwahl**

Bemerkenswert an dieser Übersicht ist die unterste Hälfte: Mechanische und bauliche Maßnahmen erzeugen keinen dieser Klärungsbedarfe. Das ist kein Argument gegen Technik, aber ein Argument dafür, die Abwägung zwischen den Maßnahmenebenen bewusst zu führen. Wo ein baulicher Verschluss dasselbe Schutzziel erreicht wie eine Überwachung, ist er nicht nur datenschutzrechtlich, sondern auch betrieblich und im Lebenszyklus häufig die einfachere Lösung.

## 8.5 Konsequenz für den Projektablauf

Aus beidem folgt eine Reihenfolge, die im Projektterminplan abzubilden ist: Schutzziele festlegen, Maßnahmen ableiten, dann Datenschutzbeauftragte und Personalvertretung bzw. Betriebsrat einbinden, dann ausschreiben. Wird die Reihenfolge verschoben, entstehen die beiden typischen Verzögerungsfälle: eine Vergabe/Beauftragung, die zurückgenommen werden muss, oder eine beschaffte Anlage, die nicht in Betrieb gehen darf.

Das Sicherheitskonzept unterstützt diese Beteiligungen unmittelbar, weil es liefert, wonach beide Stellen als Erstes fragen: die dokumentierte Erforderlichkeitsbegründung je Maßnahme.

# 9 PRÜFUNG, ÜBUNG, FORTSCHREIBUNG

Mit der Übergabe des Konzepts und der Abnahme der Anlagen ist zwar das Sicherheitsniveau hergestellt, jedoch nicht erhalten. Ein Sicherheitskonzept ist ein lebendes Dokument, das mit der Übergabe nicht erledigt ist. Der Grund liegt nicht in der Qualität der Planung, sondern darin, dass sich alle drei Größen verändern, auf denen sie beruht: das Objekt, die Gefährdungslage und die Organisation.

Dieses Kapitel beschreibt, was erforderlich ist, damit das Konzept gültig bleibt. Für den Auftraggeber ist das zugleich die Antwort auf die Frage, welcher Aufwand nach Projektabschluss dauerhaft anfällt.

## 9.1 Wartung und Instandhaltung

Technische Anlagen benötigen regelmäßige Instandhaltung. Das ist weder überraschend noch strittig. Der Punkt, der in der Praxis Probleme bereitet, ist ein anderer: Eine gestörte Anlage ist nicht nur unwirksam, sie erzeugt zusätzlich eine falsche Sicherheitsannahme. Solange keiner die Störung bemerkt, wird im Betrieb unterstellt, der Bereich sei überwacht.

Daraus folgt eine organisatorische Anforderung, die über den Wartungsvertrag hinausgeht: Es muss festgelegt sein, wer Störungsmeldungen entgegennimmt, in welcher Frist reagiert wird und welche kompensierenden Maßnahmen während der Störung gelten. Diese Festlegung gehört in die organisatorische Maßnahmenebene und nicht in den Wartungsvertrag.

## 9.2 Wiederkehrende Prüfungen

Wiederkehrende Prüfungen erfolgen nach Normen und Herstellervorgaben. Für Gefahrenmeldeanlagen ist dabei die Normenreihe DIN VDE 0833 maßgeblich, die Anforderungen an Gefahrenmeldeanlagen für Brand, Einbruch und Überfall festlegt und sich in vier Teile gliedert: Teil 1 mit den allgemeinen Festlegungen, Teil 2 für Brandmeldeanlagen, Teil 3 für Einbruch- und Überfallmeldeanlagen und Teil 4 für Anlagen zur Sprachalarmierung im Brandfall. Teil 1 gilt für das Planen, Errichten, Erweitern, Ändern und den Betrieb von Gefahrenmeldeanlagen und ist jeweils gemeinsam mit dem anlagenspezifischen Teil anzuwenden.

Auch Perimeter-Sicherungssysteme sind in diese Betrachtung einzubeziehen: DIN VDE V 0826-20 definiert ausdrücklich auch Standards für Überprüfung, Betrieb, Instandhaltung und Verbesserung solcher Systeme, nicht nur für deren Errichtung.

Für den Träger bzw. Betreiber ist entscheidend, dass die Prüfnachweise auffindbar und einer Stelle zugeordnet sind. Bei Liegenschaften, deren Anlagen über Jahre aus verschiedenen Beschaffungen stammen, ist das keine Selbstverständlichkeit und es ist genau der Punkt, an dem eine Prüfung oder eine Schadensregulierung ansetzt.

## 9.3 Übung

Organisatorische Maßnahmen verfallen schneller als technische, weil ihr Träger das Personal ist. Regelmäßige Tests sichern die Wirksamkeit der Notfall- und Ablaufpläne und sie sind die einzige Möglichkeit festzustellen, ob die geplanten Abläufe unter realen Bedingungen funktionieren.

Bei Einrichtungen mit Schichtbetrieb und ehrenamtlichen Kräften ist dabei ein Umstand zu berücksichtigen, der in anderen Liegenschaften keine Rolle spielt: Eine Übung, an der nur eine Schicht teilnimmt, erreicht einen Bruchteil der Belegschaft. Übungsplanung ist hier deshalb Teil der Dienstplanung.

Aufschlussreich sind Übungen typischerweise weniger für die Frage, ob der Plan richtig ist, als für die Frage, ob er bekannt und praktikabel ist. Die häufigsten Befunde betreffen nicht die Konzeption, sondern Erreichbarkeiten, veraltete Kontaktlisten und Abläufe, die im Alltag anders gelebt werden als in der Dokumentation beschrieben.

## 9.4 Anlassbezogene Überprüfung

Unabhängig von festen Intervallen ist das Konzept anlassbezogen zu überprüfen: bei Umbau, Nutzungsänderung und neuen Risiken. Die folgenden Anlässe sollten im Konzept selbst als Auslöser benannt sein, damit die Überprüfung nicht von individueller Aufmerksamkeit abhängt:

| Anlass | Betroffener Konzeptteil |
|---|---|
| Bauliche Veränderung, Anbau, Umnutzung von Räumen | Zonierung, bauliche Maßnahmen |
| Änderung der Aufgabe, etwa Leitstellenkooperation oder Aufgabenzuwachs | Schutzziele, Risikobewertung |
| Personelle Veränderung, Wechsel von Verantwortlichen | organisatorische Maßnahmen, Berechtigungen |
| Wegfall oder Änderung der Interventionskraft | Wirkkette, Bemessung der Verzögerung |
| Vorfall oder Beinaheereignis | Gefahrenanalyse, Schwachstellenanalyse |
| Neue oder geänderte Rechtslage, neue Regelwerksfassung | Einleitung, Regelwerksbezug |
| Austausch oder Erweiterung technischer Anlagen | technische Maßnahmen, Integration |

**Tabelle 8 Anlassbezogene Überprüfung**

## 9.5 Fortschreibung

Die Fortschreibung passt das Sicherheitskonzept an die veränderte Lage an. Sie ist keine Neuerstellung: Zonierung und Schutzziele bleiben in aller Regel bestehen, überarbeitet werden Schwachstellenliste, Risikobewertung und Maßnahmenkatalog.

Drei Festlegungen machen die Fortschreibung praktikabel. Erstens ein Turnus für die regelmäßige Überprüfung, unabhängig von Anlässen. Zweitens eine zuständige Stelle, die für die Fortschreibung verantwortlich ist, nicht eine Person, sondern eine Funktion, damit die Zuständigkeit Personalwechsel übersteht. Drittens eine Versionsführung, aus der hervorgeht, welcher Stand wann von wem freigegeben wurde; das ist die Voraussetzung dafür, dass das Dokument im Haftungsfall aussagefähig ist.

## 9.6 Zwischenergebnis

Der dauerhafte Aufwand nach Projektabschluss besteht damit aus vier Bestandteilen: Wartung und Störungsbehandlung, wiederkehrende Prüfung mit Nachweisführung, Übung der organisatorischen Abläufe und die Fortschreibung des Dokuments selbst.

Dieser Aufwand ist Teil der Lebenszyklusbetrachtung und gehört bereits bei der Maßnahmenauswahl berücksichtigt. Eine Maßnahme, deren Betriebsaufwand im Haus nicht dauerhaft geleistet werden kann, ist keine geeignete Maßnahme, unabhängig davon, wie gut sie das Schutzziel technisch erfüllt.

# 10 WIE EIN SICHERHEITSKONZEPT ENTSTEHT

Die vorangegangenen Kapitel haben beschrieben, was ein Sicherheitskonzept enthält. Dieses Kapitel beschreibt, wie es zustande kommt und vor allem, was der Auftraggeber dabei selbst leisten muss. Diese zweite Frage wird in Angeboten selten beantwortet und ist für die Terminplanung beim Auftraggeber die wichtigere: Ein Sicherheitskonzept lässt sich nicht extern beauftragen und dann abholen. Ein wesentlicher Teil der inhaltlichen Substanz kommt aus dem Haus des Auftraggebers.

## 10.1 Die fünf Schritte

Der Planungsprozess folgt fünf Schritten:

(1) Ist-Analyse: Objekt, Umfeld und bestehende Maßnahmen werden erfasst. Dies umfasst die Begehung und Bestandsaufnahme vor Ort.
(2) Schutzziele: sie werden gemeinsam mit dem Auftraggeber festgelegt.
(3) Risikoanalyse: Bedrohungsszenarien werden bewertet und priorisiert, auf Basis einer strukturierten Risiko- und Schutzbedarfsanalyse.
(4) Maßnahmenplanung: organisatorisch, baulich, technisch.
(5) Dokumentation und Umsetzung: Ausarbeitung des schriftlichen Konzepts, anschließend Ausschreibung und Inbetriebnahme.

Nach Abschluss erfolgt eine kontinuierliche Fortschreibung auf Basis von regelmäßigen Überprüfungen im Betrieb.

Die Reihenfolge ist zwingend, nicht empfehlend. Jeder Schritt setzt das Ergebnis des vorangegangenen voraus.

## 10.2 Was der Auftraggeber beisteuert

Drei Mitwirkungsleistungen bestimmen maßgeblich, wie zügig und wie belastbar das Konzept entsteht.

Die erste ist die Bereitstellung von Unterlagen und Zugang: Bestandspläne, vorhandene Brandschutz- und Fluchtwegunterlagen, Dokumentation vorhandener sicherheitstechnischer Anlagen, Wartungs- und Prüfnachweise, Zutritts- und Schlüsselregelungen sowie ein Begehungstermin mit Zugang zu allen Bereichen, einschließlich der Technikräume.

Die zweite ist die Auskunft aus dem Betrieb. Die Schwachstellenanalyse lebt davon, was im Alltag tatsächlich geschieht: welche Tür regelmäßig verkeilt wird, welcher Weg abgekürzt wird, welche Meldung routinemäßig quittiert wird, ohne dass jemand nachsieht. Diese Informationen stehen in keinem Plan. Sie kommen von den Beschäftigten vor Ort und sie kommen nur, wenn die Befragung erkennbar nicht auf Schuldzuweisung zielt.

Die dritte und wichtigste ist die Entscheidung über die Schutzziele. Hier wird das Anspruchsniveau und damit der Kostenrahmen festgelegt. Diese Entscheidung erfordert eine entsprechend befugte Stelle und eine dokumentierte Freigabe. Wird sie vertagt, kommt der Prozess zum Stillstand.

## 10.3 Welche Personen aus dem Haus einzubinden sind

Ein Sicherheitskonzept berührt mehr Zuständigkeiten, als der Anlass zunächst vermuten lässt. Die folgende Übersicht benennt die Stellen, die typischerweise zu beteiligen sind, und den Zeitpunkt. Eine verspätete Einbindung ist eine häufige Ursache für Projektverzögerungen.

| Stelle | Beitrag | Einzubinden ab |
|---|---|---|
| Fachamt / Wach- und Leitstellenleitung | Betriebswissen, Abläufe, Schichtrealität | Ist-Analyse |

| Stelle | Beitrag | Einzubinden ab |
|---|---|---|
| Entscheidungsbefugte Leitung | Festlegung und Freigabe der Schutzziele | Schutzzieldefinition |
| Gebäudemanagement / Bauamt | Bestandsunterlagen, bauliche Machbarkeit, Bauunterhalt | Ist-Analyse |
| Brandschutzbeauftragte / Brandschutzdienststelle | Auflösung von Zielkonflikten Flucht gegen Zutritt | Maßnahmenplanung |
| IT / Informationssicherheitsbeauftragte | Schnittstellen, Netz, Serverraum | Maßnahmenplanung |
| Datenschutzbeauftragte | Erforderlichkeit, Zweckbindung, Speicherdauer | Maßnahmenplanung, vor Vergabe |
| Personalvertretung / Betriebsrat | Dienst- bzw. Betriebsvereinbarung zu überwachungsgeeigneten Anlagen | Maßnahmenplanung, vor Vergabe |
| Kämmerei / Controlling | Mehrjahresplanung, investiv und betrieblich getrennt | Priorisierung |
| Vergabestelle / Einkauf | Verfahrenswahl, Leistungsbeschreibung | Dokumentation und Umsetzung |

**Tabelle 9 Übersicht Einbindung Abteilung/Stelle**

Die beiden Zeilen zu Datenschutz und Beschäftigtenvertretung tragen bewusst den Zusatz „vor Vergabe“. Kapitel 8.5 beschreibt, was andernfalls eintritt.

## 10.4 Was accellonet übernimmt

Die Leistung gliedert sich in drei Stufen, die getrennt oder gemeinsam beauftragt werden können.

Stufe 1 stellt einen Sicherheitscheck dar, der als Standortbestimmung für einen bereits laufenden Betrieb beschrieben werden kann. Hierbei untersuchen unsere Fachplaner die Bausteine Schutzziele, Schwachstellen sowie Maßnahmenkatalog und identifizieren konkrete Optionen zur Optimierung. Der Umfang richtet sich nach den Anforderungen des Auftraggebers und wird in einem gemeinsamen Kick-Off abgestimmt.

Stufe 2 besteht aus der Erstellung des vollständigen Sicherheitskonzepts; die Ergebnisse einer bereits beauftragten Stufe 1 fließen dabei unmittelbar ein, da die Fachplaner mit der Anlage bereits vertraut sind.

Stufe 3 beinhaltet die fachplanerische Betreuung der in Stufe 2 entwickelten Maßnahmen hinsichtlich Vergabe und Umsetzung.

## 10.5 Zeitlicher Rahmen

Die Dauer hängt von Objektgröße, Anzahl der Standorte, Verfügbarkeit von Bestandsunterlagen und, erfahrungsgemäß am stärksten, von der Dauer der internen Abstimmung über die Schutzziele ab.

Zwei Terminpunkte sollten in Verwaltung und Unternehmen von Beginn an mitgeplant werden, weil sie nicht vom Planungsbüro beeinflusst werden können: die Beteiligung von Datenschutz und Personalvertretung bzw. Betriebsrat vor der Vergabe und die Einbindung des Konzepts in den Haushaltsaufstellungs- bzw. Budgetzyklus. Wer die Priorisierung erst nach Abschluss der Haushalts- bzw. Budgetberatungen vorliegen hat, verliert ein Jahr, unabhängig davon, wie zügig das Konzept entstanden ist.

# 11 WAS UNS AUSZEICHNET

Wir erstellen Sicherheitskonzepte für Unternehmen und öffentliche Auftraggeber – von der Analyse bis zur Ausführungsreife.

Dabei folgen wir diesen Grundsätzen:

- **Herstellerneutral und normkonform.** Wir planen im Interesse des Auftraggebers, nicht im Interesse eines Produkts. Für öffentliche Auftraggeber ist das keine Präferenzfrage: Eine Leistungsbeschreibung, die produktneutral formuliert ist, eröffnet den Wettbewerb und stellt die Vergleichbarkeit der Angebote her.
- **Ganzheitlich.** Bauliche, technische und organisatorische Maßnahmen werden aus einer Hand geplant. Damit entfällt der Abstimmungsaufwand zwischen mehreren Fachplanern und vor allem werden Zielkonflikte zwischen den Ebenen in der Planung aufgelöst und nicht auf der Baustelle.
- **Prüf- und umsetzungsfähiges Ergebnis.** Das Konzept ist so aufgebaut, dass jede Maßnahme auf ein Schutzziel und eine bewertete Schwachstelle zurückführbar ist. Es dient damit gleichzeitig als Nachweis gegenüber Aufsicht und Rechnungsprüfung und als Grundlage für Ausschreibung und Vergabe.
- **Ein Ansprechpartner über alle Gewerke.** Über die gesamte Laufzeit: von der Begehung bis zur Abnahme und, auf Wunsch, in der Fortschreibung.
- **Nachweislich qualifiziert.** Unsere Fachplaner sind als Fachkraft für Sicherheitskonzepte (BHE) und als BSI IT-Grundschutz-Praktiker qualifiziert; accellonet ist nach ISO 9001 zertifiziert.

Sie möchten wissen, wo Ihre Liegenschaft steht? Sprechen Sie uns an – gern zu einem unverbindlichen Erstgespräch.

Telefon 0731 9792317-0
sicherheitskonzepte@accellonet.com
www.accellonet.com