ISSN 2198-0527

2/2021

CRISIS PREVENTION

Das Fachmagazin für Gefahrenabwehr, Innere Sicherheit und Katastrophenhilfe

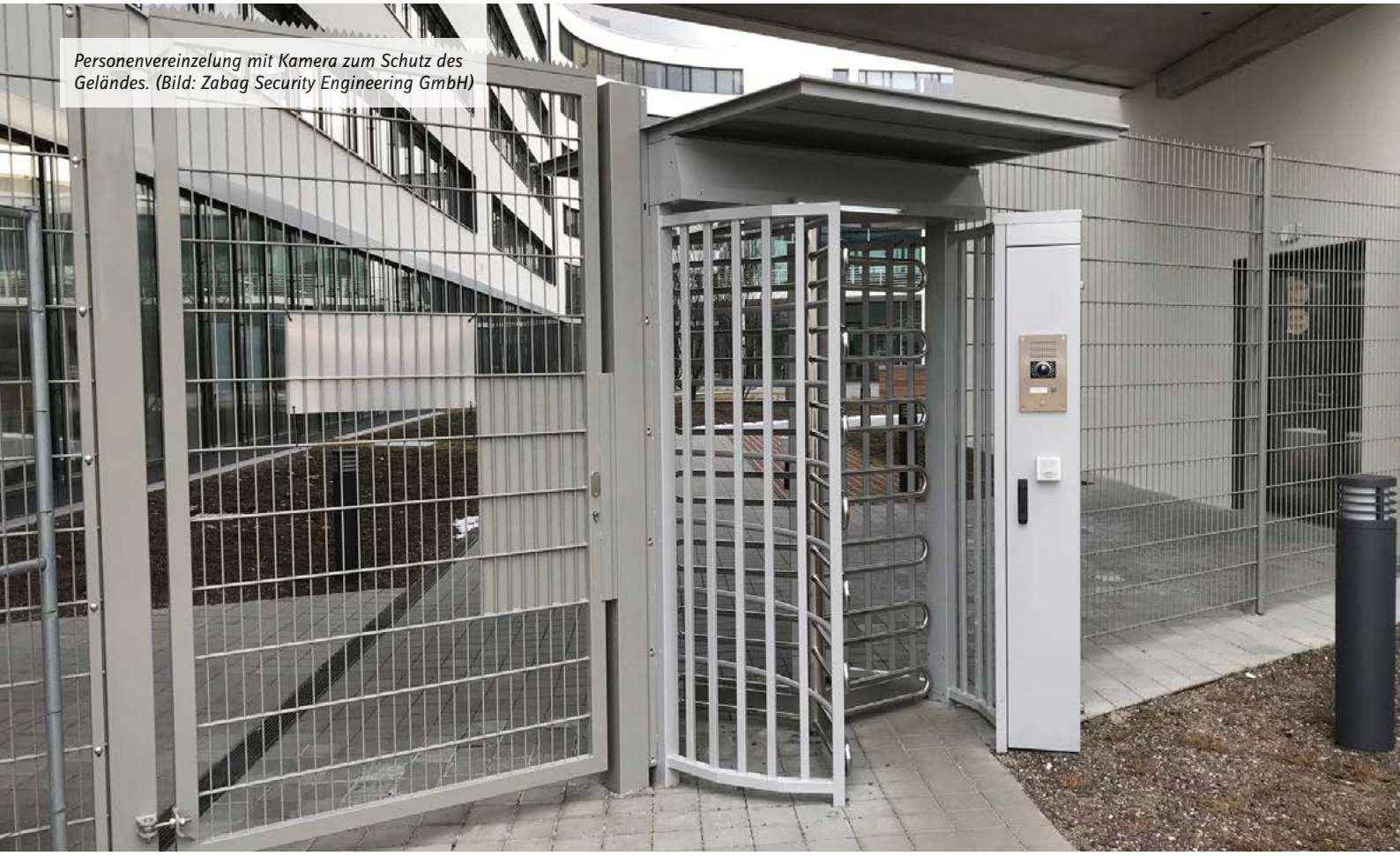
INTERVIEW ARMIN SCHUSTER
Präsident BBK

INNERE SICHERHEIT:
Perimeterschutz
ZMZ & CBRN

FEUERWEHR & KATASTROPHENSCHUTZ:
Pandemie & KRITIS
Nuklearer Notfall

KOMMUNIKATION & INFORMATIONSTECHNIK:
Kommunikation & KRITIS
Digitalisierung

www.crisis-prevention.de



Personenvereinzelung mit Kamera zum Schutz des Geländes. (Bild: Zabag Security Engineering GmbH)

Rundumsicherung sensibler Objekte und Infrastrukturen

Perimeterschutz mit ganzheitlichen Hochsicherheitslösungen

Michael Simon

Unternehmen sind verschiedensten Bedrohungen ausgesetzt. Sie reichen vom Diebstahl materiellen und geistigen Eigentums über Vandalismus und Sabotage bis hin zu Terrorismus und Extremismus. Ein entscheidender Baustein, um diese Gefahren abzublocken, ist ein wirksamer Perimeterschutz. Dazu gehören eine umfassende Zugangskontrolle, die Freigeländeabsicherung bis hin zur Drohnenabwehr sowie die Überwachung, etwa von Grenzzäunen oder Hochsicherheitsbereichen. Um sich sowohl effektiv und nachhaltig als auch effizient zu schützen, wird ein ganzheitliches, auf die individuellen Anforderungen zugeschnittenes Sicherheitskonzept benötigt. Alle Maßnahmen sollten miteinander verbunden sein und sich gegenseitig ergänzen.

Unternehmen und Institutionen stehen im Visier von Kleinkriminellen und der Organisierten Kriminalität. Die Täter verschaffen sich Zugang zu Räumlichkeiten und Anlagen, um diese zu beschädigen oder zu sabotieren, materielle und immaterielle Güter zu stehlen oder um Gewaltakte durchzuführen. Manche Angriffe gehen sogar auf das Konto von Geheimdiensten oder politischen Organisationen. Teilweise hat der Gesetzgeber bereits auf die seit einigen Jahren verschärfte Gefahrenlage reagiert und verbindliche Mindestanforderungen an das Sicherheitsniveau von Unternehmen und Institutionen bestimmter Branchen definiert bzw. sie verschärft. Das betrifft insbesondere kritische Infrastrukturen wie Energie-, Gas- und Wasserversorger, BOS und Blaulichtorganisationen. Doch auch die übrige Wirtschaft und der öffentliche Sektor sollten nicht erst aktiv werden, wenn bereits ein Schaden eingetreten ist.

Wie man sich wirkungsvoll schützen kann

Die gute Nachricht: Solche Gefährdungen durch Menschen lassen sich mit drei aufeinander abgestimmten Maßnahmenpaketen deutlich reduzieren, indem sie unbefugtes physisches Eindringen auf das Gelände verhindern. Wichtig dabei ist, dass physische und elektronische Komponenten eine Symbiose miteinander eingehen.

1. Wirksame Zugangskontrollen: Damit stellt man einerseits sicher, dass nur Befugte das Gelände von außen betreten. Andererseits lassen sich so unternehmensintern besonders sensible Bereiche zusätzlich schützen – gegenüber Fremden, aber auch gegenüber nicht zugangsberechtigten Mitarbeitern.
2. Barrieren gegen gewaltsames Eindringen: Diese sollten die Unternehmen in mehreren Ebenen anlegen. Zunächst ist der Standort als Ganzes zu schützen, beispielsweise durch eine Zaunanlage oder Mauer entlang der Grundstücksgrenze, die man mit Sicherheitsbeleuchtung und einem Einbruchmel-

desystem kombinieren kann. Darüber hinaus sollte man bestimmte Gebäude oder die Schlüsselinfrastruktur zusätzlich abschirmen, beispielsweise mit entsprechenden Sicherheitstoren, Durchfahrtssperren oder Pollern innerhalb des Geländes. So wird das Eindringen, falls Angreifer die erste Hürde überwinden konnten, weiter erschwert sowie verzögert und gibt dem Unternehmen die Möglichkeit, adäquat zu reagieren.

3. Überwachung mit Videotechnik und Alarmgebern: Hier ist es entscheidend, dass die einzelnen, hoch performanten Lösungen, etwa zur Kennzeichenerkennung oder Videoüberwachung, über Schnittstellen miteinander und mit der Unternehmens-IT vernetzt sind. Des Weiteren ist es für einen reibungslosen Ablauf im Unternehmensalltag zweckmäßig, wenn sich die Sicherheitsanlagen mobil via Anruf oder App steuern lassen.

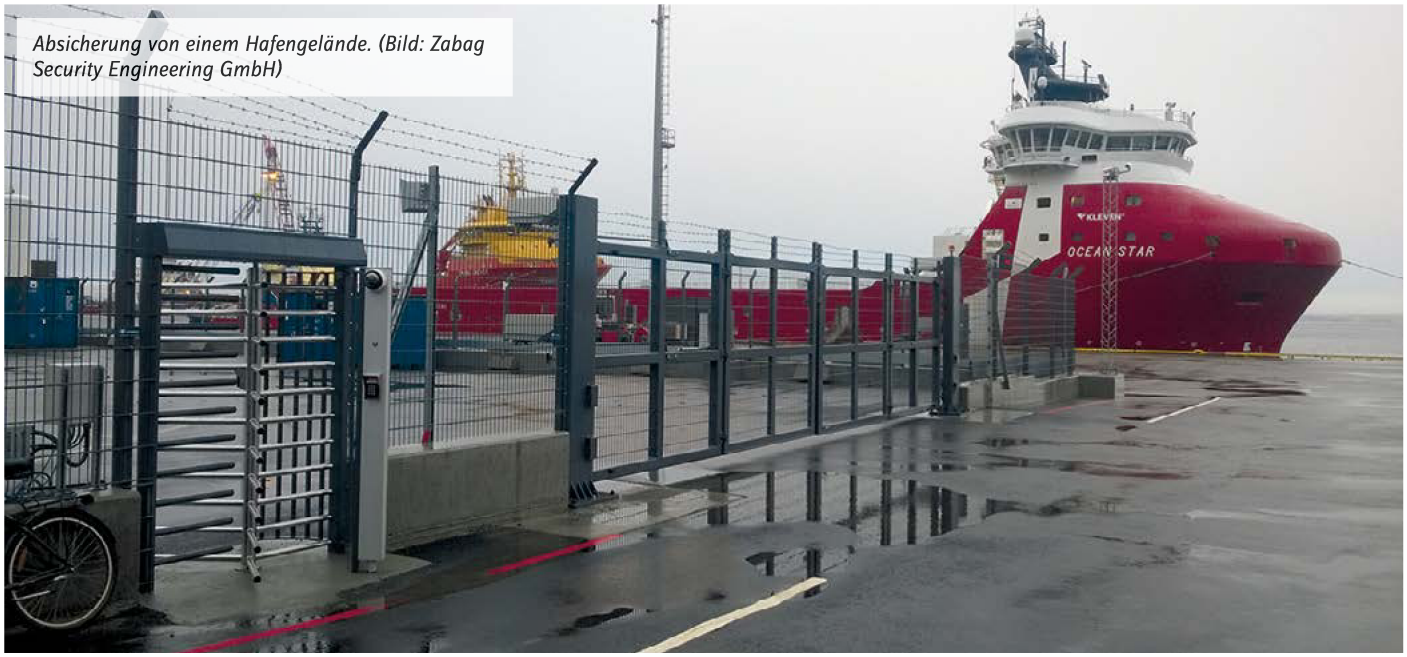
Damit die genannten Maßnahmen ihre volle Wirkung entfalten können, sollten Unternehmen und Organisationen die folgenden Tipps beachten.

Handvenenscanner fungiert als Zutrittskontrolle. (Bild: Zabag Security Engineering GmbH)

Customizing statt One-Fits-All-Konzept

Die Bedrohungsszenarien variieren von Unternehmen zu Unternehmen. Darüber hinaus hat jeder Standort seine eigenen örtlichen Gegebenheiten. Sie spielen für die Auswahl passender Sicherheitssysteme eine entscheidende Rolle. Aus diesen Gründen helfen Standardlösungen nicht weiter. Stattdessen sind Sicherheitskonzepte gefragt, die den individuellen Bedingungen optimal entsprechen. Um diese entwickeln zu können, muss man mit einer gründlichen Analyse der Ist-Situation starten. Folgende Fragen sind dabei zunächst zu klären:

- Welche gesetzlichen Auflagen sind zu erfüllen?
- Risikoanalyse: Welche Bedrohungsszenarien sind denkbar? Wer sind mögliche Angreifer? Wie hoch ist die Wahrscheinlichkeit, dass ein bestimmtes Szenario auftritt?
- Welche örtlichen Besonderheiten liegen vor? Wenn sich beispielsweise das Gelände vom Wasser aus erreichen lässt und diese natürliche Barriere als Schutz gegen ein Eindringen nicht ausreicht, dann sollte man die Kaimauer mittels elektronischer Sensoren sichern.
- Wie sehen die klimatischen Bedingungen aus? Während etwa die Technik für Skandinavien Heizelemente benötigt, müssen Konstruktionen für den Nahen Osten mit Sandstürmen zurechtkommen.
- Gibt es in Bezug auf Videoüberwachung und elektronische Sensoren Störquellen? Das könnten Pflanzen und Tiere auf dem Gelände sein, schwierige Lichtverhältnisse oder auch Vibrationen durch eine nahe gelegene Straße bzw. viel Lkw-Verkehr.
- Welche Personen befinden sich überwiegend auf dem Gelände? Handelt es sich um eine Industrieanlage oder eine öffentliche Einrichtung? Geht es beispielsweise darum, einen Hochsicherheitsbereich zu schützen, ist es neben einem durchbruch- und beschusssicheren Material auch oft wichtig, dass sich die Gestaltung in die jeweilige Umgebung einfügt.



Absicherung von einem Hafengelände. (Bild: Zabag Security Engineering GmbH)

Beachtung von langfristigen Folgen bei der Ermittlung der Wirtschaftlichkeit

Es gilt abzuschätzen, wie hoch die zu erwartenden Schäden für die wahrscheinlichsten Vorfälle sind. Weiterhin geht es darum, dafür die Kosten-Nutzen-Verhältnisse zu ermitteln. In die Betrachtung sollten dabei einerseits auch Folgeschäden wie Imageverluste oder Kundenabwanderung einfließen. Andererseits können positive Zusatzeffekte entstehen, die zu beachten sind. Ein Praxisbeispiel aus der Lebensmittelindustrie: Indem der Produzent die Schranken an der Zufahrt durch eine moderne Toranlage ersetzt hat, konnte er sich als bekannter Versender auditieren lassen und profitiert nun von einer vereinfachten Zollabfertigung.

Insellösungen zu einem ganzheitlichen Sicherheitssystem verbinden

Mechanische und elektronische Schutzmaßnahmen müssen über Schnittstellen miteinander tiefenintegriert sein. Nur so können die Systeme ohne Verzögerungen interagieren bzw. reagieren und es gibt keine Sicherheitslücken. Alarmsysteme wie Brandmeldeanlagen oder Gasdetektoren müssen im Gefahrenfall sofort einen entsprechenden Alarm auslösen – vor Ort, auf den Rechnern und mobilen Endgeräten des Personals, in der Sicherheitsleitstelle und gegebenenfalls auch bei der Feuerwehr oder der Polizei. Dafür ist es notwendig, dass sie in Echtzeit mit den anderen Systemen kommunizieren. Dabei kann es sich beispielsweise um das Zutrittskontrollsystem des betroffenen Bereichs handeln, welches dann sofort die Fluchtwege öffnet. Es könnte auch ein Produktionsmanagementsystem sein, das bei bestimmten Anlagen eine Notabschaltung durchführt. Überwachungssysteme, darunter Videoüberwachung, Sensortechnik, Bewegungs- und Einbruchsmelder, sollten ebenfalls nicht auf den Monitoren des Werkschutzes enden. Bei Unregelmäßigkeiten müssen sie die Verantwortlichen, möglicherweise auch außerhalb des Unternehmens – etwa den externen Wachschutz –, sofort informieren. Mehr noch: Das Unternehmen muss sie konfigurieren können, wenn automatisiert weitere Maßnahmen ablaufen sollen. Denkbar ist, dass sich bei Verdacht eines unberechtigten Zugangs die Türen zu besonders sensiblen Bereichen verriegeln oder zusätzlich ein Passwort abfordern.

Technisch ausgereifte Systeme mit hohem Automatisierungsgrad

Schließlich soll nicht jede Maus, die über das Gelände huscht, einen Alarm auslösen. Allerdings sind auch nach der Erstinstallation moderner Geräte und Anlagen oft weitere Feinabstimmungen oder saisonale Anpassungen erforderlich. Mögliche Gründe sind geänderte Witterungsbedingungen oder Pflanzenwuchs. Die Vorteile automatisierter Abläufe liegen auf der Hand: Sie laufen schneller ab als manuelle Tätigkeiten und befreien Mitarbeiter von Routineaufgaben. Ein digitaler Pförtner etwa oder die Kennzeichenerkennung mittels innovativer Videosysteme entlasten das Sicherheitspersonal. Die Technik ist zudem weniger fehleranfällig als der Mensch, zum Beispiel in Stresssituationen, kaum manipulierbar und unbestechlich. Nicht zu vergessen ist die Nachhaltigkeit. Um das Sicherheitssystem zukunftsfähig zu gestalten, sollte man technologische Weiterentwicklungen der einzelnen Komponenten von Anfang an bestmöglich einplanen und spätere Softwareanpassungen sowie technische Erweiterungen zulassen.

Frühzeitige Prüfung der Machbarkeiten

Ein weiterer wichtiger Punkt ist die Umsetzbarkeit, die man in der Planungsphase mittels entsprechender Machbarkeitsstudien prüfen sollte. Das effektivste Sicherheitskonzept ist wertlos, wenn es sich nicht umsetzen lässt. Ein Beispiel aus der Praxis: Herrschen vor Ort extreme Minustemperaturen – etwa in Sibirien oder Alaska –, darf man nur Stähle auswählen, deren Materialfestigkeit sich unter diesen Bedingungen nicht nachteilig verändert. Dabei reicht es jedoch nicht aus, dass es diese Stahlsorte gibt, sie muss auch am Markt in ausreichender Menge und entsprechend der Zeitvorgaben zu beschaffen sein.

Redundanzen einbauen und smart warten

Selbst die beste Technik gewährleistet keine absolute Fehlerfreiheit. Darum ist es sinnvoll, besonders hohe Risiken zweifach abzusichern. Empfehlenswert ist ein redundanter Datenaustausch im gesamten Sicherheitssystem, beispielsweise per Datenleitung und Funk. Auf diesem Weg ist die Funktionsfähigkeit weiterhin gewährleistet, wenn eine der beiden Übertragungsmöglichkeiten ausfällt. Ein weiteres Muss ist die automatische und permanente Zustandsüberwachung der Sicherheitseinrichtungen und ihrer Funktionstüchtigkeit, von den mechanischen Abläufen über die Sensorikleistung bis hin zur elektronischen Steuerung, etwa in Form eines Not-Aus. Das Monitoring sollte dabei über einen abgesicherten cloudbasierten Fernzugriff erfolgen können. So stellt man sofort – und ohne vor Ort zu sein – fest, wenn Anlagen wie Tore, Schranken, Poller oder Drehkreuze defekt sind, und kann frühzeitig Abhilfe schaffen. Ein weiteres Plus ist die intelligente Überwachung der Wartungsintervalle: Statt starrer Zeiträume richten sie sich nach den realen Nutzungsdaten, etwa danach, wie stark ein Zugangssystem frequentiert ist. Zu der optimalen Betreuung gehört darüber hinaus die statistische Auswertung aller – automatisch protokollierten – Ereignisse. Sie bildet die Grundlage für Rationalisierungsmaßnahmen und technologische Weiterentwicklungen.

Ausblick: Systeme werden intelligenter

Es ist abzusehen, dass Lösungen mit künstlicher Intelligenz (KI) auch im Perimeterschutz immer mehr an Bedeutung gewinnen werden. So ermöglicht KI in der Videoüberwachung die Früherkennung von Bränden. Weitere, zeitnahe Fortschritte sind bei der Objekterkennung und Klassifizierung zu erwarten. Es gibt aktuell technologische Entwicklungen, damit Zugangssysteme künftig bestimmte Fahrzeugtypen wie Rettungs- und Polizeifahrzeuge oder Feuerwehren automatisiert erkennen und ohne Verzug die Einfahrt gewähren. Bei der Zugangskontrolle sind zudem Systeme zur biometrischen Erkennung auf dem Vormarsch, die dann mit den physischen Sicherheitseinrichtungen gut wechselwirken müssen. Dass die zu Beginn skizzierten Bedrohungen für Unternehmen, Institutionen und öffentliche Einrichtungen abklingen werden, ist indes nicht zu erwarten. Ein umfassender Perimeterschutz, der durch intelligente Technologien unterstützt wird, ist daher auf lange Sicht unverzichtbar. CP

Michael Simon
Experte für Hochsicherheitslösungen und Zugangsanlagen im Außenbereich
Am Wasserwerk 38
09579 Grünhainichen