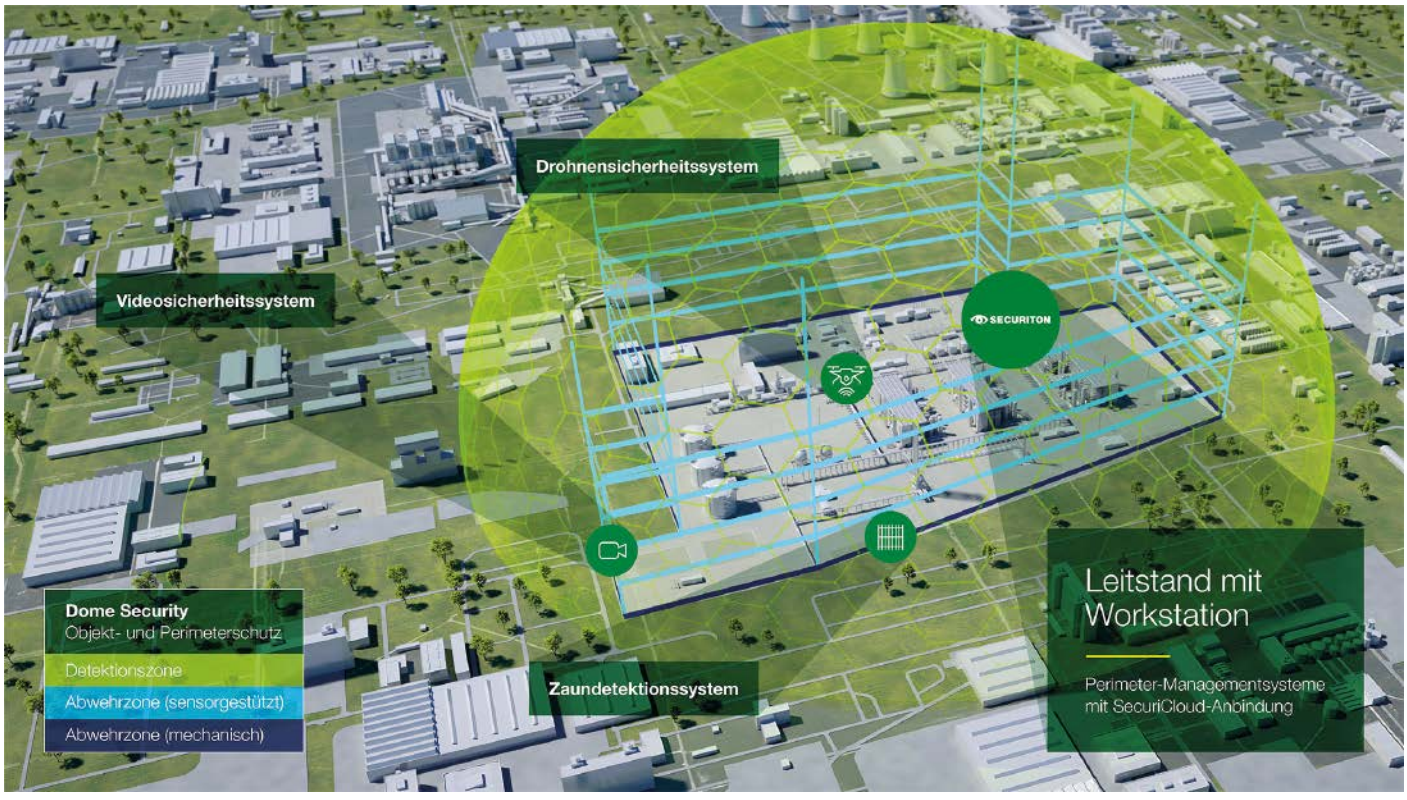
Wichtiges Gesicht und Laptop unterm Arm

Food Defense: Intelligente Abwehr von Angriffen auf die Lebensmittelindustrie

Kritische Ereignisse wie Sabotage, die Kontamination von Produkten oder Datendiebstahl können Unternehmen entlang der Lieferkette in existenzbedrohende Lagen bringen. Mehr noch: Gerade in der Nahrungsbranche gilt es zu verhindern, dass beispielsweise aufgrund der Zugabe von Substanzen Leben gefährdet wird. Mit innovativer Technik lassen sich Sicherheitslücken schließen. Beispiele entlang der Lebensmittelindustrie.

Im Sommer 2016 stürzte eine Drohne auf das Firmengelände einer süddeutschen Brauerei. Mitarbeiter fanden sie zufällig beim Rasenmähen. Ihr Besitzer hatte sein Spielzeug beim Jungfernflug aus den Augen verloren. Auf einem Foto in der Lokalpresse erkannte er es wieder und wurde bei der publikumswirksamen Rückgabe mit Wertmarken für ein Volksfest beschenkt. Sie sei froh darüber, dass die Drohne nachweislich nicht „Bier-Spionagezwecken" gedient habe, meinte die Betriebsleitung. Ob ein solcher Vorfall auch heute Anlass für eine launige PR-Aktion wäre, ist zweifelhaft. Denn die kleinen, wendigen und schnellen Flugobjekte sind inzwischen für ihren Einsatz bei kriminellen Handlungen berüchtigt. In Sicherheitskreisen natürlich bekannt: Wenn Drohnen über einem Firmengelände kreisen, können sie Arbeitsabläufe oder zur Vorbereitung von Einbrüchen Lagerstellen ausspionieren und mit ihren hochauflösenden Kameras durch Bürofenster vertrauliche Unterlagen oder Bildschirminhalte fotografieren. Daneben können sie sich in interne Netzwerke einhacken, Daten abgreifen und Viren einschleusen. Mit anderen Worten: Sie sind ein Musterbeispiel dafür, wie einfach es sein kann, Sicherheitssysteme zu überwinden.

Das Beispiel zeigt aber auch, dass Cyber-Kriminalität und physische Angriffe nicht so scharf voneinander zu trennen sind wie allgemein gerne angenommen. Durch beides können Unternehmen schwere Schäden erleiden. Im März 2021 wurde die US-Brauerei Molson Coors Opfer eines Cyber-Angriffs. Im November traf es dann



Das Vereinen der Maßnahmen von Luft- und Bodensicherung nennt Securiton „Dome Security", weil gleichsam eine schützende Kuppel über ein Gelände gelegt wird

Auch die neue Lieblingswaffe von Ausspähern und Angreifern, die Drohne, lässt sich mit intelligenter Technik abwehren

die zweitgrößte spanische Brauerei Sociaded Anómina Damm, was im übrigen zeigt, dass auch kleinere Unternehmen von Kriminellen ins Visier genommen werden. Große Teile der Produktionen standen tagelang still. Kapitalmarktorientierte Unternehmen müssen über solche Vorfälle öffentlich Bericht erstatten. „Was in die Presse gelangt, ist immer nur die Spitze des Eisbergs", sagt Michael Blaumoser, Geschäftsführer der Sicherheitsberatung SIUS Consulting. Wer nicht zur Publizität verpflichtet ist, schweigt in der Regel, um Kunden und Geldgeber nicht zu verunsichern. Stillstand, Know-how-Verlust, Rufschädigung – all dies kann schnell ein ganzes Unternehmen ruinieren und der Ausfall eines einzigen Lieferanten seinen Auftraggeber oder Weiterverarbeiter. Food Defense und Supply-Chain-Risk-Management kommt höchste Priorität zu.

Sicherheitslücken erkennen

Es steige der Beratungsbedarf von Zulieferern, die von Auftraggebern unmissverständlich die Aufforderung erhielten, ihre Sicherheitsarchitekturen auf den neuesten Stand zu bringen, berichtet Experte Blaumoser. Davon werde die Fortführung der Geschäftsbeziehung abhängig gemacht. Häufig stoße man schon beim ersten Schritt, der Analyse des Ist-Zustands, auf erheblichen Verbesserungsbedarf. Die anerkanntermaßen besonders gefährdete Ernährungswirtschaft unterscheide sich diesbezüglich nicht von anderen Branchen. Auch seien größere Unternehmen nicht signifikant besser aufgestellt als kleinere. So gelangten potentielle Täter allzu leicht und unbemerkt auf Firmengelände und bedrohlich nahe an Produktionen, Lager und Infrastruktureinrichtungen.

Nicht selten reiche ein „wichtiges Gesicht und ein Laptop unter dem Arm", um am Pförtner oder der Rezeption vorbeizukommen, weil keine Regelungen für sicherheitsrelevante Abläufe existierten. Viele Unternehmen verfügten beispielsweise über keine elektronische Zutrittsteuerung. Durch sie hätten nur autorisierte Personen mittels gespeicherter personaler und biometrischer Merkmale Zutritt zu einem Betrieb oder zu einzelnen Bereichen und dies auch nur zu bestimmten Uhrzeiten. Oder aber die installierten Sicherheitstechniken seien nicht aufeinander abgestimmt. Blaumoser: „Ein typischer Fehler ist es, einzelne Funktionen, etwa eine Einbruchmeldeanlage oder eine Videoanlage als separate Einrichtungen anzusehen. Der Effekt wäre ungleich höher, wenn beides im Kontext geplant und betrieben wird." Leider seien Erneuerungen oder Modernisierungen den harten Sparmaßnahmen der letzten Jahre zum Opfer gefallen, heißt es von Seiten des BHE Bundesverband Sicherheitstechnik. Dabei habe die Sicherheitstechnik in den letzten Jahren eine rasante technologische Entwicklung vollzogen. Es entstünden fortwährend neue und smartere Systeme mit vielen Anwendungsmöglichkeiten,

Bitte umblättern ▶

Erforderliche Sicherheitstechnik

Videosicherheit

- **IP-Kameras** (werden über das Netzwerk angeschlossen; IP = Internet-Protokoll).
Im Trend: Cloud-Dienste, bei der die Infrastruktur bei Cloud-Anbietern gemietet wird.
- **Zutrittssteuerung**
Vernetzte Systeme für eine große Anzahl von Türen; elektronische oder mechatronische Schließzylinder, biometrische Erkennung. Speichern der Berechtigungen auf dem Ausweis/Lesegerät oder zentral.
- **Brandmeldesysteme**
Drahtgebundene oder Funk-Kommunikation, Auslösung durch optische oder thermische Einflüsse oder manuell.
- **Sprachalarmierung**
Integriert in die Brandmeldezentrale oder separat, gespeicherte oder situationsabhängige Mikrofon-Durchsagen, mehrsprachig. (Auch zur allgemeinen Beschallung verwendbar.)
- **Fluchtwegesicherung**
Anschluss an Notstromnetz oder Batterien, zentrale Überwachung und Steuerung mittels PC/Funk.
- **Einbruchmeldeanlagen**
Kontaktsicherung von Toren, Türen und Fenstern, Innenraumüberwachung durch Bewegungsmelder; verkabelte oder Funk-Systeme.
- **Perimeterschutz**
Zaundetektionssysteme, Bodensensoren, Videoanalyse, optische Sensorik, mechanische Systeme wie versenkbare Poller, Drehsperren etc., Kombination mit einer intelligenten Videoüberwachung.
- **Drohnensicherheit**
Frühzeitige Detektion, Verifizierung und Neutralisierung der Angriffe aus der Luft.

Quellen: BHE, VdS

Intelligente Videoüberwachung mit IPS-Faktor erkennt und meldet die Gefahr schon, bevor sie entsteht

bei denen Künstliche Intelligenz eine immer wichtigere Rolle spiele.

Technische Möglichkeiten nutzen

Beispielsweise läuft in herkömmlichen Sicherheitsarchitekturen der Alarm einer Einbruchmeldeanlage an einer zentralen Stelle auf. Von dort aus wird versucht, auf den Bildschirmen der Videoüberwachung das Geschehen zu verifizieren. Anhand der Aufzeichnungen lassen sich die Tat rekonstruieren und Täter identifizieren. Die „Retrospektive" hilft bei der Schadenbearbeitung. Moderne Videosicherheitstechnik aber sorgt mittels intelligenter Bildanalyse dafür, dass ein Schaden gar nicht erst entsteht. Programmierte Algorithmen lösen bei kleinsten Auffälligkeiten, etwa im Verhalten von Personen, Alarmsignale und Interventionsmaßnahmen aus. „Moderne Videomanagement-Systeme heben Sicherheitskonzepte auf ein neues Level. Sie verbinden Geokoordinaten mit Bildern. Räume werden im Video berechenbar, es entsteht das Gefühl, selbst im Raum zu sein", erklärt Christian Rentschler das Prinzip. Er ist Produktmanager bei Securiton Deutschland, Projektpartner im Forschungsprogramm des Bundes für die Zivile Sicherheit. In diesem Programm arbeiten Behörden, Wissenschaft und Unternehmen an zukunftsweisenden Konzepten und Technologien zur Kriminalitäts- und Gefahrenabwehr, darunter das Bundeskriminalamt, das Fraunhofer IOSB, die Johannes-Gutenberg-Universität Mainz und Fraport. Nach dem gleichen Prinzip detektiert Videoanalyse Unregelmäßigkeiten in Produktionsabläufen und im Verhalten von Mitarbeitern. Sollte es tatsächlich zu einem Vorfall wie einer Verunreinigung kommen, kann durch Vorlage der Dokumentation der eigene Betrieb als Fehlerquelle ausgeschlossen werden.

Von der Boden- zur Luftabwehr

Videotechnik lässt sich mit mechanischen Schutzmaßnahmen vernetzen, etwa mit Umzäunungen, die mit Detektionssensoren ausgerüstet sind. Sobald einer der Sensoren anschlägt, nimmt das Kamerasystem mittels moderner IPS 3D-Technologie automatisch die Verfolgung auf; es lässt den Angreifer oder Einbrecher nicht mehr aus den Augen. Die Meldungen der Sicherheitssysteme werden in einer Alarmzentrale erfasst und von dort aus wiederum weitere periphere Systeme wie Beleuchtungs- und Beschallungsanlagen ferngesteuert.

Auch die neue Lieblingswaffe von Ausspähern und Angreifern – die Drohne – lässt sich mit intelligenter Technik abwehren. Hochfrequenz-Technologie spannt ähnlich einem militärischen Abwehrschirm gleichsam eine Schutzhülle über das Firmengelände. Nähert sich eine Drohne dem Firmengrundstück, wird diese detektiert und anhand der vorhandenen oder fehlenden, in der EU vorgeschriebenen digitalen Kennung (Remote ID) identifiziert. „Das System kann die Drohne frühzeitig detektieren – oft sogar schon vor dem Start! – und Interventionsmaßnahmen können eingeleitet werden. Beispielsweise kann die Kontrolle über die Drohne vollständig übernommen und eine sichere Landung eingeleitet werden", so Produktmanager Jochen Geiser, ebenfalls von Securiton. Das Vereinen der Maßnahmen von Luft- und Bodensicherung nennt Securiton „Dome Security", weil gleichsam eine schützende Kuppel über ein Gelände oder Gebäude gelegt wird. Es ist die modernste Art von Objekt- und Perimeterschutz.

Professionelle Planung

Eine professionelle Planung legt den Grundstein für eine leistungsfähige Sicherheitsarchitektur. „Oftmals sind sich Unternehmen nicht darüber im Klaren, was sie eigentlich bezwecken. Video ist ein breit einsetzbarer Prozess. Eine Anlage kann detektieren, sie kann informieren, also ein Lagebild übermitteln und aufzeichnen, sie kann Interventionsmaßnahmen auslösen und unterstützen. Man kann sie aber auch anwenden, um Täter zu erschrecken. Die Identifikation und Festlegung von Schutzzielen ist der allererste Schritt", so Volker Kraiss, Geschäftsführer der strategischen Sicherheitsberatung Kraiss Wilke & Kollegen. Es gelte, den

Moderne Videomanagement-Systeme heben Sicherheitskonzepte auf ein neues Level

konkreten Nutzen einer Funktion und der dafür zu tätigenden Investition zu ermitteln. Letztlich gehe es einzig und allein um die Frage, welchen Wertbeitrag die Maßnahmen für das Unternehmen leisten. „Anhand der umfassenden Analyse der Schwachstellen und Optimierungsbedarfe definieren wir Schutzziele und die dafür geeigneten Systemlösungen“, so Christian Rentschler von Securiton. Auch der oft als Hindernis für den Videoeinsatz angesehene Datenschutz lasse sich dank moderner Technologie in nahezu jedem Bereich gewährleisten. Eine spezielle Verschleierungstechnik erkenne und maskiere Objekte wie beispielsweise Personen oder Fahrzeuge automatisch – bei Bedarf auch irreversibel und damit rechtssicher.

Lohnende Investition

Investitionen in mehr Sicherheit begegnen nicht nur einem möglichen Worst Case: einem irreparablem Imageschaden, Kundenverlusten, Regressforderungen oder Strafzahlungen in Millionenhöhe. Die Pandemie und Naturkatastrophen haben die Prämien in der industriellen Sachversicherung seit 2019 um gut 20 Prozent, die Prämien für Haftpflicht-, D&O- und Cyberrisiken um 20 bis 30 Prozent ansteigen lassen. „Dagegen stehen künftig verschiedene kostensenkende Maßnahmen wie Eigentragungsmodelle, höhere Selbstbeteiligungen und vor allem verbessertes technisches, organisatorisches und juristisches Risikomanagement“, so der Industrie-Versicherungsmakler BDJ. Dem Credo, lieber ein Risiko so weit zu minimieren und das Restrisiko selbst zu tragen als es zu versichern, komme in diesen herausfordernden Zeiten eine besondere Rolle zu. ●

Securiton Deutschland
Achern
Tel. +49 7841 6223 0
info@securiton.de
www.securiton.de/ips-faktor