ENTSCHEIDER KNOW-HOW FÜR FOOD & BEVERAGE

LVT LEBENSMITTEL Industrie

1-2 68. Jahrgang Februar 2023

Interpack
s. 22

Branchenfokus • Getränkeindustrie
Schlauchpumpen bei Alpirsbacher Klosterbräu

Die erste Braustätte für eine Berliner Craft Brewery

Anlagentechnik für das Weingut Famille Perrin

Special • Nachhaltigkeit
Palettenkennzeichnung bei Rothaus

Nachhaltige Getränkeverpackungen

Zuckerrüben unter Dampf

Verfahrenstechnik
Explosionsrisiken bei der Sprühtrocknung

Betriebstechnik
Schädlingsbekämpfung durch Druckentwesung

Hygiene • Steril-, Reinraumtechnik
Green Cleaning bei Schädel's Beilagen

Software • IT
IT zwischen Troubleshooting und Wohlbefinden

Titelstory: Securiton

Food Defense: Intelligente Abwehr

Leistungsfähige Sicherheitskonzepte gegen Angriffe auf Unternehmen

Seite 28

Special • Modernes Management und Betriebsführung

WILEY

© Securiton

Abb. 1: Drohnensicherheitssysteme bieten umfassende Lösungen mit Funktionalitäten zum Detektieren, Lokalisieren und Identifizieren ferngesteuerter sowie autonomer Drohnen und ermöglichen eine kontrollierte Übernahme.

Food Defense: Intelligente Abwehr

Leistungsfähige Sicherheitskonzepte gegen Angriffe auf Unternehmen

Die Lebensmittelindustrie gehört zu den besonders gefährdeten Branchen. Kritische Ereignisse wie Sabotage, die Kontamination von Produkten oder Datendiebstahl können Unternehmen entlang der Lieferkette in existenzbedrohende Lagen bringen. Die Täter gehen immer raffinierter vor. Mit innovativer Technik lassen sich Sicherheitslücken schließen.

Es 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. Die Betriebsleitung zeigte sich froh darüber, dass die Drohne nachweislich nicht „Bier-Spionagezwecken" gedient habe.

Ob ein solcher Vorfall auch heute Anlass für eine launige PR-Aktion wäre, ist zweifelhaft. Denn die kleinen, wendigen und schnellen Flugmaschinen sind inzwischen für ihren Einsatz bei kriminellen Handlungen berüchtigt. Sie können zur Vorbereitung von Einbrüchen Lagerstellen ausspionieren, durch Bürofenster vertrauliche Unterlagen fotografieren und sich in interne Netzwerke einhacken. Sie sind zudem ein Beispiel dafür, dass Cyber-Kriminalität und physische Angriffe nicht so scharf voneinander zu trennen sind wie allgemein angenommen.

Immer häufiger werden Unternehmen Opfer solcher Attacken, in deren Folge komplette Produktionen und Firmenverwaltungen stillstehen. 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.

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 bekanntermaßen besonders gefährdete Ernährungswirtschaft unterscheide sich diesbezüglich nicht von anderen Branchen. Auch seien größere Unternehmen nicht signifikant besser aufgestellt als kleinere. Es reiche nicht selten 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 bspw. 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." Moderne Sicherheitstechnik bietet inzwischen die passenden Systeme unter Einsatz von künstlicher Intelligenz.

Technische Möglichkeiten nutzen

Exemplarisch 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 verifizie-

ren. Anhand der Aufzeichnungen lassen sich die Tat rekonstruieren und Täter identifizieren. Die „Retrospektive" hilft bei der Schadenbearbeitung. Moderne Videotechnik 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, einem führenden Spezialisten für gewerbliche und industrielle Sicherheitstechnik und 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 Frankfurt und die Fraport AG. 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

© Securiton

Abb. 2: Umfassender Objektschutz durch Grundstückssicherung und Videoanalyse.

den Angreifer oder Einbrecher nicht mehr „aus den Augen". Die Meldungen der Sicherheitssysteme werden in einer Alarmzentrale erfasst. Von dort werden wiederum weitere periphere Systeme wie Beleuchtungs- und Beschallungsanlagen ferngesteuert. Auch die neue Lieblingswaffe von Ausspähern und Angreifern lässt sich mit intelligenter Technik abwehren. Hochfrequenz-Technologie spannt ähnlich einem militärischen

© Securiton

Abb. 3: Moderne Videotechnik sorgt mittels intelligenter Bildanalyse dafür, dass ein Schaden gar nicht erst entsteht, da rechtzeitig interveniert werden kann.

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 – gegebenenfalls schon vor dem Start – und Interventionsmaßnahmen können eingeleitet werden. Bspw. kann die Kontrolle über die Drohne vollständig übernommen und eine sichere Landung eingeleitet werden", so Produktmanager Jochen Geiser, ebenfalls von Securiton.

Professionelle Planung

Eine professionelle Planung legt den Grundstein für eine leistungsfähige Sicherheitsarchitektur. „Anhand der umfassenden Analyse der Schwachstellen und Optimierungsbedarfe definieren wir Schutzziele und die dafür geeigneten Systemlösungen", so Christian Rentschler. Auch der oft als Hindernis für den Videoeinsatz angesehene Datenschutz lasse sich dank moderner Technologie in nahezu jedem Bereich gewährleisten. Eine spezielle Verschleierungsstechnik erkenne und maskiere Objekte wie z. B. Personen oder Fahrzeuge automatisch – bei Bedarf auch irreversibel und damit rechtssicher.

Autor: Manfred Godek, Presse- und Redaktionsbüro

Kontakt:
Securiton Deutschland
Achern
Christian Rentschler
Tel.: +49 7841/6223-0
christian.rentschler@securiton.de
www.securiton.de