Spionage- und Prototypenschutz für die Automobilindustrie

Experten raten: Informationssicherheit über Standard planen

Die Automobilbranche steht unter Druck: Sie muss einerseits strengere CO2-Vorgaben sowie neue Richtwerte für Feinstaub- und Stickoxid-Emissionen erfüllen. Zudem erfordern die Transformation zur Elektromobilität und der zunehmende Wettbewerb durch Tech-Konzerne eine neue Kernkompetenz der Fahrzeugbauer: Software. Oft gehen diese Veränderungsprozesse mit baulichen Umstrukturierungen einher: Forschungsabteilungen und Rechenzentren brauchen mehr Platz – und oft auch ein erhöhtes Sicherheitslevel. Dabei muss die Corporate Security bestehende und neue Technologien zusammenführen, damit alle Systeme interagieren. Zukunftsfähige Anlagen sind zudem intelligent vernetzt, modular und kompatibel aufgesetzt. Cybersicherheit und Benutzerfreundlichkeit werden von Anfang an mitgedacht. Dafür braucht die Branche starke Partner, denn historisch gewachsene Sicherheitslösungen oder Eigenentwicklungen sind in der aktuellen dynamischen und komplexen Gefährdungslage oft nicht agil genug.

Zum Schutz von Prototypen sind Einbruchmeldeanlagen und Perimetersicherung nur einige Maßnahmen für die Informationssicherheit in Werken der Automobilbranche. Welche Mittel eingesetzt werden sollen, beschreibt der „ISA-Katalog“ (Information Security Assessment) des Verbands der Automobilindustrie (VDA). Zwar nennt die Richtlinie keine genauen Ansprüche an die Systeme selbst, sie benennt jedoch die Techniken, die innerhalb der jeweiligen Sicherheitslevels einzusetzen sind. Je sensibler die zu verarbeitenden Informationswerte sind, desto mehr Schutzmaßnahmen empfiehlt der Leitfaden.

Gut beraten sind also Branchenteilnehmer, die Standards übererfüllen: Mit Videosicherheit, genauer: intelligenter Videoüberwachung mit Videoanalysen, können die geforderten Instrumente in einem System zusammengeführt und abgebildet werden – mit dem Ziel, Gefahren und Unregelmäßigkeiten in Echtzeit automatisiert zu erkennen, bereits während der Gefahrenentstehung zu alarmieren und darüber hinaus das Sicherheitspersonal vollautomatisiert bei der Intervention zu unterstützen.

Gute Schutzkonzepte sind mehrstufig aufgebaut

Sicherheitskonzepte werden zunächst für jeden Bereich erstellt und anschließend clever vernetzt. Dabei können die Lösungen sehr spezifisch ausfallen. Gelungene Planungen berücksichtigen innerhalb verschiedener Sicherheitslevels lokale Gegebenheiten ebenso wie die individuellen Schutzziele eines Unternehmens.

Level 1: An der Grundstücksgrenze

Eine effektive Perimetersicherung kombiniert physikalische Barrieren wie Zäune (teils auch ausgestattet mit Detektionssensoren) und einem Videosicherheitssystem. Unberechtigte Zutrittsversuche werden unmittelbar erkannt

Umfassende Perimetersicherung mit IPS VideoManager: Videomanagement und Videoanalyse aus einem Guss

IPS Outdoor Detection: Alarmierung in Echtzeit bei Eindringversuchen

Wirksame Sicherheitskonzepte für die Automobilindustrie

und gemeldet. Die intelligente Videoanalyse hat dabei entscheidende Vorteile gegenüber anderen Verfahren: Sie arbeitet zu jeder Zeit mit unverminderter Aufmerksamkeit auf zuverlässigem Sicherheitsniveau.

Meldungen und Alarme werden automatisch in Echtzeit generiert und dem Sicherheitspersonal detailliert zur Beurteilung und zur Einleitung von Interventionsmaßnahmen angezeigt. Das System zeigt Vorfälle aus sicherer Entfernung, zeichnet relevante Situationen auf und sichert Beweise. (Lösung: IPS VideoManager)

Halten sich etwa Personen verdächtig lange vor dem Zaun oder in Bereichen von besonderem Interesse auf dem Werksgelände auf, erkennt die intelligente Videoanalyse dies vollautomatisch und warnt. Dabei kann zwischen zwei Zeitfaktoren unterschieden werden. Zum einem der generelle Aufenthalt im Kamerabild (z. B. ausspähen der Situation) oder zum anderen der Aufenthalt an einer Stelle (z. B. Manipulation des Zauns). (Lösung: IPS Loitering Detection)

Level 2: Auf dem Gelände

Bei einem Alarm rückt die Interventionsmannschaft aus. Einige Werksgelände haben indes die Dimension eines kleinen Dorfes und entsprechend lange kann es dauern, bis Einsatzkräfte vor Ort eintreffen. Zu diesem

Videosicherheit: Automatische Verfolgung von Eindringlingen

Zeitpunkt könnte ein Eindringling sich schon nicht mehr an der alarmierten Stelle befinden. Mit 3D-Georeferenzierung können Videosicherheitsanlagen automatisch den mutmaßlichen Täter verfolgen. Dabei überschneiden sich die Erfassungsbereiche der Kameras – relativ nahe am Ende eines Erfassungsbereiches wird das Objekt an die nächste Kamera automatisch übergeben. Der Streckenverlauf wird auf einer Karte visualisiert und den Sicherheitskräften angezeigt. Sie sparen wertvolle Zeit und werden direkt zur observierten Person gelotst. Das System hat zu jeder Zeit den aktuellen Aufenthaltsort von Eindringlingen im Blick. (Lösung: IPS Dome Tracker)

Aus diesem Grund versuchen mutmaßliche Täter oft, eine oder mehrere Kameras im Vorfeld zu manipulieren: Sie werden verdreht, verdeckt, mit Farbe besprüht, geblendet oder defokussiert. Auf kleinste Abweichungen reagiert das System jedoch sofort mit einer Alarmmeldung. Dazu wertet die Analyse permanent Videobilder aus. Sabotageakte werden dadurch schnell und präzise detektiert. (Lösung: IPS Tamper Detection)

Level 3: Überwachung der Gebäudeaußenhaut

Für die Sicherung der Außenhaut selbst kommen eine Einbruchmeldeanlage und wie bereits an der Grundstücksgrenze Zutrittskontrolle zum Einsatz. Wieder punktet die Videosicherheitsanlage mit einem für Forschungs- und Entwicklungsbereiche sehr interessanten Feature: Ihre Aufzeichnungen dienen auch der Nachverfolgung und Identifizierung. Zudem kann mit dem Videosicherheitssystem ein Einbruchschutz realisiert werden, indem die Kameras entlang des Gebäudes ausgerichtet werden und so unberechtigte Zugänge über Türen und Fenster detektieren. (Lösung: IPS Outdoor Detection)

Level 4: Im Gebäudeinneren

Gleiches leisten Kameras im Innenbereich, die bestimmte Räume sichern, beispielsweise Rechenzentren, sensible Planungsbüros oder Entwicklungs- und Testabteilungen. Aus Datenschutzgründen werden Personen auf Videoaufzeichnungen zunächst unkenntlich gemacht. Die Verschleierung der Videobilder kann nur im Sonderfall im Vier-Augen-Prinzip aufgehoben werden, um ein Ereignis aufzuklären – etwa mit Zustimmung von Betriebsrat und Polizei. Dennoch werden die Bilddaten zur Beurteilung der Situationen systemseitig vollumfänglich ausgewertet. (Lösung: IPS Privacy Protection)

Unverzichtbar sind im Automobilsektor Brandmeldeanlagen. Für die Produktionslinien von E-Antrieben und bei Motorenprüfständen von Hybriden sind Ansaugrauchmelder zur Brandfrühesterkennung die richtige Wahl. Denn Lithium-Batterien brennen anders als herkömmliche Motoren: Betroffene Zellen heizen ihre Nachbarzellen auf, bis sie ebenfalls anfangen zu brennen – die Reaktion ist bekannt als Thermal Runaway. Die sekundenschnelle Aufheizung führt zu Stichflammen, extremer Rauchentwicklung und toxischen Dämpfen. Hochempfindliche Ansaugrauchmelder detektieren Brände schon in der Entstehungsphase und verhindern den Worst Case. (Lösung: SecuriRAS ASD)

Level 5: Der Luftraum über dem Gelände

Risiken haben auch eine vertikale Dimension: In Deutschland gibt es eine halbe Million Drohnen; viele sind mit hochauflösenden Kameras bestückt. Sie stellen für Groß-Events wie Aktionärsversammlungen eine direkte Bedrohung aus der Luft dar und ermöglichen Spionage durch ein Fenster oder über den Teststrecken von Prototypen und Erlkönigen. Und die Gefahr nimmt zu, denn der Markt wächst weiterhin.

IPS Dome Tracker: Automatische Verfolgung von Objekten

IPS Tamper Detection: Absicherung der Verfügbarkeit von Videosicherheitssystemen

IPS Privacy Protection: Zuverlässiger Schutz der Privatsphäre ermöglicht datenschutzkonforme Videoüberwachung

TISAX®: Sicherer Informationsaustausch

KI-basierte Systeme detektieren das Fluggerät und die Fernbedienung – also den Standort des Piloten. Und dies bereits beim Einschalten der Drohne, also noch vor dem Abheben. Damit einhergehend übernehmen Drohnensicherheitssysteme auch die Abwehr bzw. kontrollierte Übernahme von unkooperativen Drohnen. (Lösung: SecuriDrone)

Intelligente Videoüberwachung mit IPS-Faktor

Die vielfältigen Lösungen mit Mittel der Videoüberwachung mit intelligenter Videoanalyse vereint Securiton Deutschland in seiner Technologiemarke IPS – kurz der „IPS-Faktor" genannt. Die moderne Videotechnologie bietet auch eine Systemvernetzung mehrerer Unternehmensstandorte. Beim sogenannten Multi Site Management ist z. B. die Unternehmenszentrale für Niederlassungen verantwortlich und fungiert als Leitstelle, in der mit nur einem System alles betrachtet und bedient werden kann.

IT-Sicherheit für die Smart Factory

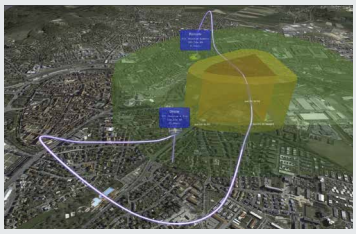
Die Automobilindustrie ist ein beliebtes Ziel für Hackerangriffe, erzwungene Produktionsstopps und Wirtschaftsspionage. Betriebsunterbrechungen und Cyber-Vorfälle gehören laut Allianz Risiko Barometer 2021 zu den größten Geschäftsrisiken. Betroffen sind nicht nur die Hersteller selbst, auch ihre Zulieferer sind bereits ins Fadenkreuz der Angreifer gerückt. Supply-Chain-Attacken schädigen mehrere Systeme gleichzeitig, deswegen gelten sie als so effektiv und schwerwiegend. Mit der Zertifizierung nach dem von der Automobilindustrie definierten Standard für Informationssicherheit TISAX® wird der sichere Informationsaustausch zwischen OEMs (Original Equipment Manufacturer) und Zulieferern nachgewiesen.

Wie alle vernetzten Infrastrukturen sind auch Alarm- und Sicherheitssysteme virtuellen Bedrohungen ausgesetzt: Cyber-Kriminelle greifen sie gezielt mit hochprofessionellen Mitteln an. Eine Videoüberwachungsanlage generiert, verarbeitet und speichert sensible Abläufe und muss daher höchsten IT-Sicherheitsstandards entsprechen.

Angriffsszenarien gibt es viele, aber auch Lösungen zur Abwehr: Bei BruteForce-Attacken werden eine Vielzahl an Passwörtern ausprobiert. Sie werden unterbunden, indem das System eine erneute Eingabe erst nach einiger Zeit wieder erlaubt. Das mehrstufige Benutzerrechtesystem wirkt Man-in-the-Middle-Angriffen entgegen. Bei der Härtung der Systeme kommen nur betriebsrelevante Programme zum Einsatz. Daher hat Securiton IT-Sicherheitspakete im Portfolio, die bereits im Standard den Empfehlungen des BSI folgen.

Die Notwendigkeit, sich neuen Bedrohungen schnell anzupassen, muss Teil jeder Planung sein. Nicht umsonst regelt das IT-Sicherheitsgesetz 2.0 nicht nur Vorgaben für Kritische Infrastrukturen, sondern auch für Unternehmen mit besonderem volkswirtschaftlichem Interesse – darunter fallen die meisten Automobilkonzerne. Je umfassender das Know-how eines Unternehmens, desto höher ist in der Regel auch das Sicherheitsniveau. Ob Hersteller oder Zulieferer, ob Facility-Abteilung, Geschäftsführer, IT- oder Betriebsleiter – sie alle müssen mit zunehmenden Herausforderungen rechnen und Wert legen auf agile, flexible und aufrüstbare Systeme mit dem USP, heute schon mehr als den Sicherheitsstandard zu erfüllen.

SecuriDrone: Luftraumüberwachung zum Schutz vor unbemannten Flugobjekten



SecuriDrone: Visualisierung der Gefahr aus der Luft

Securiton Deutschland
Alarm- und Sicherheitssysteme

Hauptsitz: Von-Drais-Straße 33
77855 Achern | DE
Tel. +49 7841 6223-0

www.securiton.de

Ein Unternehmen der
Securitas Gruppe Schweiz

SECURITON