17.01.2022 – 08:49 Uhr

Die 8 wichtigsten Trends für die Sicherheitsbranche im Jahr 2022

Hangzhou, China (ots/PRNewswire) -

Zu Beginn des Jahres 2022 hat die Welt weiterhin mit der Pandemie zu kämpfen. Aber die Sicherheitsbranche hat sich zweifelsohne weiter verändert, angepasst und weiterentwickelt, trotz aller Widrigkeiten. Einige Trends haben sich sogar noch beschleunigt. Neben der traditionellen „physischen Sicherheit" gibt es eine Vielzahl von Grenzbereichen wie KI, Cloud Computing, IoT und Cybersicherheit, die von großen und kleinen Unternehmen in unserer Branche rasch vorangetrieben werden.

Allem Anschein nach befindet sich die Sicherheitsbranche in einer Phase, in der sie sich neu definiert. Sie geht über den reinen Sicherheitsschutz hinaus und umfasst ein breiteres Spektrum an Aktivitäten, die die Sicherheit erhöhen und gleichzeitig ein neues Maß an Intelligenz und Nachhaltigkeit für Gemeinschaften, Unternehmen und die Gesellschaft bringen werden.

An dieser Stelle möchte Hikvision einige unserer Ideen und Erwartungen zu den wichtigsten Trends vorstellen, die die Sicherheitsbranche im Jahr 2022 und vielleicht sogar noch weiter in der Zukunft beeinflussen werden.

1. KI wird überall sein

Heutzutage ist künstliche Intelligenz in der Sicherheitsbranche weit verbreitet. Immer mehr Kunden in der Branche haben den Wert von KI erkannt und neue Einsatzmöglichkeiten für KI-Anwendungen in verschiedenen Szenarien gefunden. Neben ANPR, automatischen Ereigniswarnungen und der Reduzierung von Fehlalarmen werden KI-Technologien auch für weitere Anwendungen eingesetzt, z. B. zur Erkennung von persönlicher Schutzausrüstung (PSA), zur Sturzerkennung für ältere Menschen, zur Erkennung von Minen und vielem mehr. In der Zwischenzeit haben wir auch eine verstärkte Zusammenarbeit in der Branche beobachtet, wobei Sicherheitshersteller ihre Hardwareprodukte für KI-Anwendungen von Drittanbietern öffnen und offene Plattformen für Kunden einführen, damit diese ihre eigenen KI-Algorithmen erstellen und trainieren können, um individuelle Anforderungen zu erfüllen.

KI ist eine der grundlegenden Technologien, die die Sicherheitsbranche umgestalten wird. Dank der Optimierung der Algorithmen, der verbesserten Rechenleistung und der geringeren Kosten der Chips aufgrund der Fortschritte in der Halbleitertechnologie in den letzten Jahren bilden KI-Anwendungen allmählich die grundlegenden Funktionen und Fähigkeiten, die von allen Sektoren der Industrie akzeptiert werden, und wir sagen eine noch stärkere Tendenz voraus, dass „KI überall sein wird".

2. AIoT wird die Branchen digitalisieren und durchdringen

Da immer mehr Sicherheitskameras und andere Sicherheitsgeräte an das Netzwerk angeschlossen werden, wird die Sicherheitsbranche zu einem wichtigen Teil der IoT-Welt und bereichert ihre visuellen Möglichkeiten. Es ist offensichtlich, dass die Grenzen der Sicherheitsbranche immer mehr verschwimmen und weit über den Bereich der physischen Sicherheit hinausgehen. Durch die Verbreitung der KI-Technologie werden die angeschlossenen Geräte zu intelligenten „Dingen" in der IoT-Welt. Die Kombination aus KI und IoT, oder wie wir es nennen, AIoT, hebt die Sicherheitsbranche auf eine höhere Ebene, automatisiert die Arbeitsabläufe und Verfahren von Unternehmen und unterstützt die digitale Transformation verschiedener Branchen wie Energie, Logistik, Fertigung, Einzelhandel, Bildung, Gesundheitswesen usw.

Aus unserer Sicht bietet AIoT der Branche mehr Möglichkeiten mit schnell wachsenden Anwendungen für Sicherheitsgeräte und -systeme. Inzwischen werden Sicherheitsgeräte und -systeme um weitere Wahrnehmungsfunktionen wie Radar, Lidar, Temperaturmessung, Feuchtigkeitsmessung und Gasleckerkennung erweitert, um sie leistungsfähiger zu machen. Diese neuen Geräte übernehmen eine Vielzahl von Aufgaben, für die noch vor wenigen Jahren mehrere verschiedene Geräte erforderlich waren, und decken sowohl Sicherheitsfunktionen als auch andere intelligente Funktionen für eine sich ständig weiterentwickelnde Welt ab.

3. Konvergente Systeme werden Datensilos aufbrechen

Die Beschäftigten in der Privatwirtschaft und im öffentlichen Dienst würden die Chance nutzen, die hinderlichen „Datensilos" zu beseitigen Daten und Informationen, die in unterschiedlichen Systemen oder Gruppen verstreut und isoliert sind, behindern den Informationsaustausch und die Zusammenarbeit und verhindern, dass Manager einen ganzheitlichen Überblick über ihre Abläufe erhalten. Hier hat sich die Konvergenz verschiedener Informationssysteme als wirksamer Ansatz erwiesen, der hoffentlich ausreicht, um diese Silos aufzubrechen.

Es ist klar - der Trend in der Sicherheitsbranche geht dahin, Systeme zu konvergieren, wo immer dies möglich ist, einschließlich Video, Zugangskontrolle, Alarmanlagen, Brandschutz und Notfallmanagement, um nur einige zu nennen. Darüber hinaus werden immer mehr nicht sicherheitsrelevante Systeme wie Personal-, Finanz-, Bestands- und Logistiksysteme auf einheitlichen Managementplattformen zusammengeführt, um die Zusammenarbeit zu verbessern und das Management bei einer besseren Entscheidungsfindung auf der Grundlage umfassenderer Daten und Analysen zu unterstützen.

4. Cloud-basierte Lösungen und Dienste werden unverzichtbar sein

Wie die künstliche Intelligenz ist auch die Cloud kein neuer Trend in unserer Branche, aber sie ist auf dem Vormarsch. Von kleinen Unternehmen bis hin zu Großunternehmen können wir beobachten, dass immer mehr Unternehmen Cloud-basierte

Sicherheitslösungen und -dienste nutzen wollen. Und wie wir gerade erleben, hat die Pandemie die Umstellung auf Cloud-basierte Operationen für Menschen und Unternehmen in aller Welt beschleunigt.

Alle Unternehmen wünschen sich Plattformen oder Dienste, die einfach zu handhaben sind, bei denen möglichst wenige Ressourcen verwaltet werden müssen und die so einfach wie möglich einzurichten sind. Genau hier setzt die Cloud an. Bei einer Cloud-Hosting-Infrastruktur sind weder ein lokaler Server noch Software erforderlich. Die Benutzer können den Status ihrer Anlagen und Unternehmen in Echtzeit überprüfen, Sicherheitsereignisse und Alarme schnell empfangen und Notfallmaßnahmen einfach über eine mobile App durchführen. Für die Betreiber von Sicherheitsunternehmen bietet die Cloud die Möglichkeit, ihren Kunden aus der Ferne bei der Konfiguration von Geräten zu helfen, Fehler zu beheben, Sicherheitssysteme zu warten und zu aktualisieren und bessere Mehrwertdienste anzubieten.

5. Kristallklare Sicherheitsaufnahmen sind bei jedem Wetter, unter allen Bedingungen und zu jeder Tages- und Nachtzeit Standard

Für Videoüberwachungskameras ist es von entscheidender Bedeutung, dass sie 24 Stunden am Tag, bei jedem Wetter und unter allen Bedingungen ein klares Bild liefern und Details erfassen. Kameras mit Low-Light-Imaging-Technologie, die nachts und in fast völlig dunklen Umgebungen hochauflösende und farbige Bilder wiedergeben, sind auf dem Markt sehr willkommen. Die beeindruckende Technologie kommt bei immer mehr Kameramodellen zum Einsatz, darunter 4K-, Varifokal- und PTZ-Kameras. Darüber hinaus werden für klarere Videoüberwachungsbilder bei schlechten Sichtverhältnissen - insbesondere bei schlechtem Wetter - leistungsstarke Bildsensoren, ISP-Technologie und KI-Algorithmen eingesetzt, die es den Kameras ermöglichen, die Klarheit und die Details des Bildes zu erhalten.

Apropos Bildtechnologie: Der Trend zum Einbau mehrerer Objektive in neue Kameras ist nicht zu übersehen. Kameras mit einem Objektiv sind nur begrenzt in der Lage, mehr Details aus größeren Entfernungen zu erfassen und das gesamte Bild an großflächigen Orten darzustellen. Sie tun nur das eine oder das andere. Durch den Einsatz von zwei oder mehr Objektiven in einer Kamera können Mehrlinsenkameras jedoch gleichzeitig sowohl Panoramen als auch detaillierte, vergrößerte Ansichten desselben großen Standorts liefern. Bei Anwendungen wie Flughäfen, Häfen, Bahnhöfen, Parkplätzen, Stadien und Plätzen werden diese Multilinsen-Kameras in jeder Hinsicht von Vorteil sein.

6. Biometrische Zugangskontrolle bringt mehr Sicherheit und Effizienz

In den letzten Jahrzehnten hat sich die autorisierte Zugangskontrolle weit von Schlüsseln, Pincodes und ID-Karten entfernt. Wir befinden uns nun im Zeitalter der Biometrie. Der Markt für Zugangskontrollen wird immer stärker von biometrischen Authentifizierungen besetzt, von der Erkennung von Finger- und Handabdrücken bis hin zur Gesichts- und Iriserkennung.

Biometrische Zugangskontrollen bringen inhärente Vorteile mit sich, wie höhere Sicherheit und Effizienz bei geringerer Fälschungsgefahr. Sie verifizieren innerhalb von Sekunden - oder Sekundenbruchteilen - und verhindern unnötigen Körperkontakt. Iris-, Handflächenabdruck- und Gesichtserkennung ermöglichen eine berührungslose Zugangskontrolle, eine hygienische Praxis, die aufgrund der Pandemie immer beliebter wird.

7. Der Zero-Trust-Ansatz wird das Rampenlicht auf die Cybersicherheit lenken

Da mehr Sicherheitsgeräte über das Internet verbunden sind, als man sich je vorstellen konnte, ist die Cybersicherheit zu einer großen Herausforderung für die Branche geworden. In jüngster Zeit wurden in den wichtigsten Märkten der Welt strengere Vorschriften für die Datensicherheit und den Schutz der Privatsphäre eingeführt, wie z. B. die EU-DSGVO und das chinesische Datensicherheitsgesetz, die höhere Anforderungen an die Cybersicherheit stellen. Und im Jahr 2021 haben uns mehrere bahnbrechende Ransomware-Angriffe auf eine Vielzahl von Unternehmen eindeutig davon überzeugt, dass Unternehmen in jeder Branche ihre Netzwerksicherheitsarchitektur und ihren Online-Schutz verstärken müssen.

Wie gehen wir also mit den wachsenden Bedenken hinsichtlich der Cybersicherheit um? Obwohl das Konzept bereits 2010 entwickelt wurde, ist der Begriff „Zero Trust" erst in den letzten Jahren zu einem geflügelten Wort geworden. Zero Trust ist eine strategische Initiative zur Verhinderung von Datenschutzverletzungen durch die Eliminierung des Konzepts des Vertrauens aus der Netzwerkarchitektur einer Organisation und beruht auf der Philosophie „never trust, always verify". Das Konzept hat sich in der IT-Branche durchgesetzt und hält nun langsam aber sicher auch Einzug in den Bereich der physischen Sicherheit, da es allmählich zu einem wichtigen Bestandteil der IoT-Welt wird.

8. Grüne Produktion und kohlenstoffarme Initiativen werden große Fortschritte machen

Es herrscht Einigkeit darüber, dass kohlenstoffarme Initiativen von Gesellschaften in aller Welt geschätzt werden. Auf dem Sicherheitsmarkt werden Produkte mit geringem Stromverbrauch von den Kunden bevorzugt, und die Nachfrage nach solarbetriebenen Kameras steigt.

Unterdessen drängen lokale Gesetze, Verordnungen und Richtlinien, die die Kohlenstoffemissionsstandards für Fertigungsunternehmen einschränken, die Industrie dazu, umweltbewusstere Praktiken in ihren täglichen Abläufen und in der Produktion einzuführen, wozu auch die Verwendung umweltfreundlicherer Materialien und die Einführung mehrerer energieeffizienter Designs in den Produktherstellungsprozessen gehören. Wir freuen uns, dass immer mehr Hersteller in der Sicherheitsbranche eine „grüne" Produktion anstreben und sich dafür einsetzen, ihren Kohlenstoffausstoß zu verringern. Auch wenn es noch einige Zeit dauern wird, hat die Bewegung bereits begonnen. Wir gehen davon aus, dass wir 2022 in diesem Bereich erhebliche Fortschritte machen werden.

Weitere Informationen

Um mehr über die hier besprochenen Themen zu erfahren oder um Hikvisions Einblicke in die neuesten Sicherheitstrends zu entdecken, besuchen Sie bitte die Hikvision Blog-Seite.

Foto - https://mma.prnewswire.com/media/1726672/Top_8_trends_security_industry_2022.jpg

Pressekontakt:

Luke Liu,
liuyunlong10@hikvision.com,
+86-15210662217