17. Juni 2024

Axon Portfolio und Datenschutz

Als Carrier-Unternehmen ist sich Aritech der Bedeutung von Datenschutzgesetzen bewusst. Carrier hat auf globaler Ebene datenschutzbezogene Prozesse und Richtlinien implementiert, um die Einhaltung zu gewährleisten.

Gesetze zum Datenschutz

Nationale und regionale Regierungen auf der ganzen Welt verschärfen die Gesetzgebung zur Einhaltung des Datenschutzes und führen neue und strengere Gesetze zur Verwendung und Aufbewahrung von personenbezogenen Daten ein. Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, die direkt oder indirekt mit den Daten in Verbindung gebracht werden kann, insbesondere durch Zuordnung zu einer Identifikationsnummer oder zu einem oder mehreren spezifischen Faktoren, die sich auf ihre physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Merkmale beziehen. Viele Datenschutzgesetze enthalten eine erweiterte Zuständigkeit, was bedeutet, dass sie für Einrichtungen gelten, die außerhalb der Region ansässig sind, aber in dieser Region Geschäfte machen oder sich auch auf dort ansässige Betroffene konzentrieren. Carrier ist sich der Bedeutung dieser Datenschutzgesetze bewusst und hat auf globaler Ebene ein internes datenschutzbezogenes Prozesssystem und eine Datenschutzrichtlinie eingeführt.

Carrier hat auch die BCR (Binding Corporate Rules) der EU erhalten, die als der goldene Standard in Bezug auf den Datenschutz gelten (Approved Binding Corporate Rules | European Data Protection Board (europa.eu)) und hier veröffentlicht werden: link. Darüber hinaus verfügt Carrier über ein globales Datenschutzteam.

Wie wirkt sich dies auf das Axon-Portfolio aus?

Axon, entwickelt von der Carrier Corporation (firmierend als "Aritech"), besteht aus einer Reihe von Produkten und Lösungen, die durch die Installation von Einbruchmelde- und Zutrittskontrollfunktionen für die Sicherheit von Immobilien sorgen. Axon und die davon abgeleiteten Produkte umfassen Hardware wie Sicherheitszentralen, Erweiterungen, Tastaturen und Leser sowie Softwareanwendungen zur Konfiguration und Verwaltung dieser Lösungen.

Axon verwendet die Advisor Management Software als Schnittstelle zur Verwaltung und Kontrolle von Sicherheitssystemen vor Ort oder aus der Ferne. Die Verwendung personenbezogener Daten ist von zentraler Bedeutung für das Sicherheitssystem eines Endnutzers, um die Bewegungen und den Zugang zu gewünschten Funktionen seiner Mitarbeiter und Besucher zu verwalten. Die einzigen Datenfelder, die in Advisor Management obligatorisch sind, sind ein Name und - falls erforderlich - ein Berechtigungsnachweis (Ausweisnummer, PIN), der dazu dient, einen Berechtigungsnachweis mit einer Person zu verknüpfen und Berechtigungen festzulegen, wo und wann der Benutzer Zugang zu der gewünschten Funktion oder dem gewünschten Zutritt erhalten kann.

Das Errichterunternehmen, das die Axon-Sicherheitslösung installiert, arbeitet mit dem Endbenutzer zusammen, um zu definieren, welche persönlichen Datenelemente als Teil des Installations- und Inbetriebnahmeprozesses eingegeben werden. Da Aritech die Axon-Lösung nicht installiert oder in Betrieb nimmt, sind der Errichter und der Endbenutzer dafür verantwortlich, dass die Sammlung und Verwendung von persönlichen Daten konsistent sind, um den Datenschutz einzuhalten.

Die eindeutige Identifikation des Ausweises (ID) und die damit verbundenen Zutrittsrechte sind über die Einbruchmeldezentrale für eine sofortige Entscheidungsfindung verfügbar. Die Vorlage einer Identifikationsnummer (Pin-Code oder Karte) an einem Leser wird mit der im System registrierten Identifikationsnummer abgeglichen, und der Zugang zu den angeforderten Funktionen oder der Zutritt zu Türen/Aufzügen wird je nach den vom Errichter des Systems in den Räumlichkeiten des Endnutzers konfigurierten Sicherheitsregeln gewährt oder verweigert.

Beispiele für Datenfelder, die zur Optimierung des Sicherheitsmanagements in Advisor Management konfiguriert werden können, sind interne und externe Nummern (häufig zur Erfassung interner HR-Nummern oder interner ID-Nummern), E-Mail-Adresse, Geschlecht, Foto und Zutrittsebenen. Diese Daten können über einen gesicherten Datenaustausch in regelmäßigen Abständen aus einer Personaldatenbank abgefragt werden. Der Zugang zu den Datenfeldern und die Möglichkeit, sie hinzuzufügen oder zu ändern, beruhen auf den Entscheidungen der Endnutzer und werden durch vom Endnutzer konfigurierbare Berechtigungen gesteuert.

Die Einbruchmeldezentrale speichert Details als Ereignisse in den Ereignisprotokollen. Die Einträge in den Ereignisprotokollen enthalten eine Beschreibung der Ereignisse mit Uhrzeit und Datum des Auftretens. Der Endbenutzer kann die Protokolle auch so konfigurieren, dass sie zusätzliche Informationen zur Identifizierung der beteiligten Person und des Ortes des Ereignisses enthalten. Der Name einer Person kann auch an eine Einbruchmeldezentrale gesendet werden, um zu ermitteln, wer an einem Ereignis beteiligt ist, und die entsprechenden Maßnahmen einzuleiten. Bei Einbruchsalarmen entspricht die Speicherung von Ereignissen und die Alarmberichterstattung den Sicherheitszulassungen wie EN50131.

- **Identifizieren** Vergewissern Sie sich, dass Sie wissen, wo Ihre persönlichen Daten gespeichert werden.
- **Übereinstimmen** Verwaltung der Verarbeitung, des Zugriffs auf und der Löschung von personenbezogenen Daten und Beantwortung von Anfragen der betroffenen Personen.
- **Schützen** Einführung von Sicherheitsverfahren zum Schutz personenbezogener Daten.
- **- Aufzeichnen** Führen Sie ein Protokoll über Ihre Verfahren.
- **Überwachen** Verhinderung von Datenschutzverletzungen und deren Meldung.

Datenschutz durch Design

Carrier hält sich an die "Privacy by Design"-Prinzipien, die inzwischen in vielen Datenschutzgesetzen gesetzlich vorgeschrieben sind. Im Kern fordert "Privacy by Design" die Einbeziehung des Datenschutzes als integralen Bestandteil in die Gestaltung von Systemen.

Während der Endbenutzer letztendlich für die Eingabe, Verarbeitung und Verwaltung persönlicher Daten in Axon-Produkten verantwortlich ist, unterstützt Aritech den Endbenutzer bei der Einhaltung des Datenschutzes, indem es die Datenschutzanforderungen in das Produktdesign einbezieht. Aritech verpflichtet sich zu "Privacy by Design.

Unsere Produkte sind so konzipiert, dass sie den Endbenutzer unterstützen, da dieser bestimmt, welche persönlichen Daten er in das System eingibt. Die Produkte von Aritech bieten verschiedene Sicherheitsstufen, um die persönlichen Daten von Personen zu schützen, die Zutritt zu den Räumlichkeiten des Endbenutzers haben. Anerkannte Industriestandards und ISO-konforme Verschlüsselungsmethoden können im System konfiguriert oder installiert werden, wie z.B. DESFire EV1 zwischen Karte und Leser, Verschlüsselung zwischen Controller und Server und HTTPS für eine sichere Verbindung zwischen dem Server der Advisor Management-Anwendung und den Endbenutzern. Darüber hinaus unterstützt die Anwendung umfassende Systembeschränkungen, um den Zugriff auf diejenigen zu beschränken, die dazu berechtigt sind.

Zusätzlich zur Produktgestaltung kann der Errichter den Endbenutzer bei der Festlegung des Umgangs mit Pflichtfeldern und optionalen Feldern in unseren Produkten unterstützen. Der Errichter kann zusätzliche Informationen darüber liefern, welche Daten und Protokolle er einsehen kann und welche Sicherungen während der Installation, Inbetriebnahme und Produktwartung erstellt werden.

Unterstützung bei Aufgaben im Bereich des Datenschutzes

Advisor Management bietet den Sicherheitsadministratoren eines Endanwenders die Möglichkeit, Berechtigungen zu definieren, um sicherzustellen, dass Einzelpersonen Zugriffsrechte auf die Funktionen und Daten in der Anwendung haben, die sie zur Erfüllung ihrer Aufgaben benötigen, und um zu definieren, welche Art von Zugriff angemessen ist.

Axon Einbruchmeldezentralen sind nur für privilegierte Personen (Errichter usw.) zugänglich, die nur Zugriff auf Funktionen und Konfigurationsdetails haben, die ihnen vom Endbenutzer zugewiesen wurden.

Advisor Management kann zur Konfiguration der Umgebungen für Zutritt, Einbruchschutz und Alarmüberwachung verwendet werden, einschließlich der Zugriffsrechte für Endbenutzer. Es ermöglicht die Durchsetzung von Passwörtern und kann Single Sign-On unterstützen. Der Systemzugang kann durch die Segmentierung von Hardware, Standort, Anwendung und Funktion sowie durch Lese- und Bearbeitungsrechte eingeschränkt und auf die funktionale Verantwortung einer Person begrenzt werden.

Jedes von einem Sensor erfasste Ereignis wird an die Einbruchmeldezentrale gesendet und dann an eine angeschlossene Sicherheitsmanagement-Anwendung wie Advisor Management oder an Konfigurations- und Diagnosetools zur Aufzeichnung und Diagnose übertragen. Zusätzliche persönliche Daten können auch an eine zentrale Wachdienststelle gesendet werden, um Alarme weiterzuverfolgen, je nach der vom Endbenutzer gewählten Konfiguration.

Für jedes Ereignis, das sich auf den Zutritt durch Türen oder Einbruchsbereiche bezieht, werden die Beschreibung des Ereignisses und die zugehörigen Details zunächst in der Hardware in Übereinstimmung mit den Sicherheitsvorschriften erfasst und aufbewahrt, und wenn sie mit der Advisor Management-Anwendung verbunden sind, werden diese Ereignisse auch übertragen und in der Anwendung gespeichert. Dies ermöglicht eine spätere Überprüfung der Ereignisse durch autorisiertes Personal - falls und wie erforderlich - und so lange wie nötig. Die Datenaufbewahrung wird vom Endbenutzer

bestimmt; Axon-Produkte sehen keine Standard-Löschperiode vor, sondern erlauben es dem Endbenutzer, diese zu definieren.

Den Menschen das Recht geben, ihre Daten zu kontrollieren

Advisor Management stellt eine Reihe von Datenfeldern zur Verfügung, in denen personenbezogene Daten gespeichert werden, um die Zuweisung von Zutrittsrechten zu identifizieren und die ordnungsgemäße Verwendung von PIN-Codes, Zutrittskarten, Nummernschildern oder gleichwertigen Ausweisarten zu überwachen. Diese werden von den Betreibern der Advisor Management Anwendung kontrolliert.

Die Advisor Management-Anwendung speichert benutzerbezogene Details in Protokollen, um die ordnungsgemäße Nutzung des Zugangsrechts in der Anwendung als physischen Zutritt durch Sicherheitselemente wie Türen, Aufzüge oder Einbruchsbereiche zu überprüfen. Advisor Management bietet die Möglichkeit, die Speicherdauer zu begrenzen und einen Bericht über die gespeicherten personenbezogenen Daten einer Person zu erstellen oder zu visualisieren, welche Mitarbeiter mit personenbezogenen Daten arbeiten.

Die Axon Einbruchmeldezentralen erstellen auch Protokolle, wie sie von den Vorschriften gefordert werden, sowie für Audit-Zwecke. Die Axon Einbruchmeldezentralen bieten die Möglichkeit, die personenbezogenen Daten nach einer konfigurierbaren Zeitspanne zu anonymisieren, da die Protokolleinträge nicht gelöscht werden dürfen.

Über Aritech

Aritech bietet führende Sicherheits- und Lösungen zum Schutz von Personen für kommerzielle Anwendungen in den Bereichen Einbruchschutz, Video, Übertragung und Zutritt. Aritech bietet einige der vertrauenswürdigsten Produktnamen in der Branche und wird durch kontinuierliche Partnerdienste unterstützt, damit Kunden das sichern und schützen können, was ihnen am wichtigsten ist. Aritech ist Teil der Carrier Global Corporation, einem weltweit führenden Anbieter von gesunden, sicheren und nachhaltigen Gebäude- und Kühlkettenlösungen. Für weitere Informationen besuchen Sie aritech.com oder folgen Sie uns auf LinkedIn @Aritech.

Die maßgebliche Ausführung dieses Merkblatts ist Englisch: link. Sollte diese Übersetzung im Widerspruch zur englischen Version des Merkblatts stehen, ist die englische Version maßgebend.