25. Mai 2018

Datenschutz-Grundverordnung

Interlogix Advisor Advanced: Produkte und Datenschutz

DSGVO

Die am 25. Mai 2018 in Kraft getretene Datenschutz-Grundverordnung („DSGVO“) ist eine Verordnung der Europäischen Union zum Schutz personenbezogener Daten. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar gilt eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennnummer oder besonderen Merkmalen identifiziert werden kann, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Weitere Informationen zur DSGVO finden Sie unter: **http://www.eugdpr.org**

Eine der bedeutsamsten Änderungen des EU-Datenschutzrechts ist der erweiterte Geltungsbereich der DSGVO. Sie gilt für sämtliche in der EU niedergelassenen Unternehmen, unabhängig davon, ob die Datenverarbeitung in der EU stattfindet oder nicht, ebenso wie für Unternehmen außerhalb der EU, die personenbezogene Daten von in der EU ansässigen Personen verarbeiten.

United Technologies Corporation ist sich der Bedeutung der DSGVO bewusst und hat weltweit verbindliche unternehmensinterne Regeln (Binding Corporate Rules, BCRs) eingeführt, die unsere Datenschutzrichtlinie sowie unser internes datenschutzbezogenes Governance-System umfassen. BCRs gelten als der Goldstandard für den Datenschutz. Unsere BCRs sind in mehreren Sprachen öffentlich einsehbar (**http://www.utc.com/Pages/Privacy.aspx**).

Wie sehen die Folgen für Advisor Advanced-Produkte aus?

Advisor Advanced wird von der UTC Fire & Security Americas Corporation, Inc. (als „Interlogix“ tätig) entwickelt und umfasst eine Reihe von Produkten mit Funktionen zur Einbruchserkennung sowie zur Zutrittskontrolle für die Sicherheit von Gebäuden und Grundstücken. Zu unseren Produkten gehören Hardware wie Einbruchmeldezentralen, Erweiterungsmodule, Bedienteile und Lesegeräte sowie Softwareanwendungen zur Konfiguration und Bedienung von Lösungen. Die unterschiedlichen Systeme benötigen für deren Funktion personenbezogene Daten. Im Rahmen von Installation und Inbetriebnahme legen Sie gemeinsam mit dem beauftragten Unternehmen fest, welche personenbezogenen Daten hierbei eingegeben werden. Da Interlogix nicht an Installation und Inbetriebnahme der Advisor Advanced-Produkte beteiligt ist, obliegt es der Verantwortung des beauftragten Unternehmens sowie des Endanwenders zu gewährleisten, dass die Erfassung und Verwendung personenbezogener Daten den Bestimmungen der DSGVO entspricht.

Interlogix unterstützt den Endanwender bei der Einhaltung der Datenschutzbestimmungen, indem entsprechende Anforderungen bei der Produktentwicklung berücksichtigt werden. Trotzdem liegt die Verantwortung für die Eingabe, Verarbeitung und Pflege personenbezogener Daten in Advisor Advanced-Produkten letztlich beim Endanwender. Interlogix ist dem Prinzip „Privacy by Design“ verpflichtet.

Es unterstützt den Endanwender dadurch, dass dieser festlegen kann, welche personenbezogenen Daten in das System eingegeben werden. Interlogix-Produkte schützen personenbezogene Daten von Personen, die Zugang zu Gebäuden bzw. Grundstücken des Endanwenders haben, auf mehreren Ebenen. Verschlüsselungsmethoden gemäß anerkannter Branchenstandards und ISO lassen sich im System konfigurieren bzw. installieren, beispielsweise 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 dem Endanwender. Darüber hinaus ermöglicht die Anwendung umfassende Systemeinschränkungen, mit denen sich der Zugriff auf autorisierte Benutzer begrenzen lässt.

Zusätzlich zur Auslegung des Produkts kann auch das mit der Installation beauftragte Unternehmen den Endanwender hinsichtlich des richtigen Umgangs mit obligatorischen und optionalen Feldern in unseren Produkten unterstützen. Außerdem kann das Unternehmen zusätzliche Informationen darüber bereitstellen, welche Daten und Protokolle angezeigt werden und welche Backups während der Installation, der Inbetriebnahme und der Produktwartung erstellt werden.

Identifizieren

Den Speicherort personenbezogener Daten bestimmen.

Anwenden

Verarbeitung, Zugriff und Löschung personenbezogener Daten verwalten und Anfragen betroffener Personen beantworten.

Schützen

Sicherheitsverfahren zum Schutz personenbezogener Daten festlegen.

Dokumentieren

Unterlagen zu Verfahren speichern.

Überwachen

Datenschutzverletzungen verhindern und melden.

Datenschutz-Grundverordnung

Interlogix Advisor Advanced: Produkte und Datenschutz

Cybersicherheit

Die Cybersicherheit in Bezug auf die unter der Marke Advisor Advanced angebotenen Produkte und Dienstleistungen sowie der Schutz personenbezogener Daten haben bei Interlogix oberste Priorität. Interlogix arbeitet fortlaufend an der diesbezüglichen Verbesserung seiner Produkte. Hierzu hat United Technologies Corporation (UTC), die Muttergesellschaft von Interlogix, die Position eines Produktsicherheitsbeauftragten geschaffen.

Endanwender von Advisor Advanced-Produkten haben die Möglichkeit, personenbezogene Daten im Produkt zu speichern. Über die Bedieneinheiten besteht direkter Zugriff auf die eindeutige Anmeldeidentifikation (ID) und die damit verbundenen Zugriffsrechte. Angegebene Anmelde-IDs (PIN-Code oder Karte) werden mit den im System gespeicherten Anmelde-IDs abgeglichen. Anschließend wird der Zugang zu den gewünschten Funktionen bzw. Türen/Aufzügen abhängig von den Sicherheitsregeln gewährt oder verweigert, die während der Installation des Systems beim Endanwender konfiguriert wurden.

Die Verwendung personenbezogener Daten ist für das Einbruchmeldesystem von Endanwendern zwingend erforderlich, um die Bewegungen von Mitarbeitern und Besuchern sowie deren Zugang zu gewünschten Funktionen steuern zu können. Die einzigen Datenfelder, die in Advisor Management eingegeben werden müssen, sind der Name und ggf. ein Berechtigungsnachweis (Ausweisnummer, PIN). Mit der Zuordnung des Berechtigungsnachweises zu einer Person lassen sich Berechtigungen festlegen, die abhängig von Ort und Zeit Zugang zu bestimmten Funktionen bzw. Bereichen gewähren.

Daneben stehen in Advisor Management weitere Felder zur Verfügung, mit denen sich die Gewährleistung der Sicherheit optimieren lässt, darunter: interne und externe Nummer (wird häufig zur Erfassung interner Personal- bzw. Identifikationsnummern verwendet), E-Mail-Adresse, Geschlecht, Foto und Zugriffsebenen. Diese Daten können beispielsweise in regelmäßigen Abständen durch einen sicheren Datenabgleich mit einer Personaldatenbank aktualisiert werden. Der Endanwender legt anhand der Vergabe von Berechtigungen fest, welche Benutzer Zugriff auf Datenfelder erhalten und welche Benutzer Datenfelder hinzufügen bzw. ändern können.

In den Ereignisverlaufsprotokollen der Bedieneinheiten werden detaillierte Daten gespeichert. Die Einträge der Ereignisverlaufsprotokolle enthalten eine Ereignisbeschreibung mit Uhrzeit und Datum des Auftretens. Endanwender haben außerdem die Möglichkeit, zusätzliche Angaben in den Protokollen zu speichern, beispielsweise zum Ort des Ereignisses sowie zur beteiligten Person. Zusätzlich lässt sich der Name einer Person auch an einen Wachdienst senden, damit dieser die an einem Ereignis beteiligte Person identifizieren und entsprechende Maßnahmen einleiten kann. Bei Einbruchmeldungen entspricht die Speicherung von Ereignissen und Alarmberichten Sicherheitsnormen wie EN50131.

Unterstützung bei Datenschutzmaßnahmen

Mit Advisor Management können Sicherheitsadministratoren des Endanwenders Berechtigungen festlegen, die gewährleisten, dass einzelne Benutzer entsprechende Zugriffsrechte für Funktionen und Daten der Anwendung erhalten, die sie für ihre Aufgaben benötigen. Außerdem lässt sich der gewünschte Zugriffstyp festlegen.

Nur bestimmte Personen (z. B. Installationstechniker) erhalten über die Advisor-Bedieneinheiten Zugriff auf das System. Der Zugriff ist dabei auf die Funktionen und Konfigurationsoptionen beschränkt, die zu den von Endanwendern zugewiesenen Berechtigungen gehören.

Bereiche mit Zutrittskontrolle und Einbruchmeldung sowie Alarmüberwachung lassen sich einschließlich entsprechender Benutzerzugriffsberechtigungen über Advisor Management konfigurieren. Dabei ist ein Schutz über ein Kennwort oder Single Sign-On möglich. Der Systemzugriff kann anhand von Hardware, Standort, Anwendung und Funktionen sowie anhand von Lese- sowie Bearbeitungsrechten eingeschränkt und auf den jeweiligen Tätigkeitsbereich einer Person beschränkt werden.

Alle von Meldern erfassten Ereignisse werden an die Bedieneinheit gesendet und anschließend an eine Sicherheitsmanagement-Anwendung wie Advisor Management oder Konfigurations- und Diagnosetools übertragen, in denen die Ereignisse gespeichert bzw. ausgewertet werden. Auf Wunsch kann der Endanwender weitere personenbezogene Daten zwecks einer angemessenen Reaktion an Wachdienste senden.

Für sämtliche Ereignisse in Zusammenhang mit einem Zutritt durch Türen bzw. dem Eindringen in geschützte Bereiche werden eine Ereignisbeschreibung sowie weitere Details unter Einhaltung entsprechender gesetzlicher Vorgaben zunächst in der Hardware erfasst sowie gespeichert und sobald eine Verbindung besteht an die Advisor Management-Anwendung übertragen und auch in dieser gespeichert. Dadurch lassen sich Ereignisse, wenn erforderlich, auch nachträglich durch autorisiertes Personal prüfen. Wie lange die Daten aufbewahrt werden, bestimmt der Endanwender. In Advisor Advanced-Produkten ist keine unveränderliche Standardspeicherdauer festgelegt.

Ref. 1543 – Advisor DE – 0401