BRANDMELDETECHNIK

Brandschutz digital ...

... aber inklusive Datensicherheit und Schutz vor Cyberangriffen

Unternehmen und Organisationen setzen zunehmend auf digitale Lösungen, um ihre Brandmeldetechnik zu optimieren und u. a. von den Möglichkeiten der standortübergreifenden Steuerung und Überwachung sowie dem Fernzugriff für eine effiziente Wartung und Instandhaltung zu profitieren. Allerdings bringt die Digitalisierung des Brandschutzes auch Herausforderungen mit sich, insbesondere in Bezug auf die Datensicherheit und den Schutz vor Cyberangriffen. Für den sicheren Zugriff auf die Alarm- und Sicherheitssysteme nutzt Securiton Deutschland die firmeneigene Cloud-Lösung der Securitas Gruppe Schweiz.

Das Herzstück aller ortsunabhängigen, digitalen Dienste ist die Cloud, denn sie bildet das Bindeglied zwischen Brandmeldeanlage und Fernzugriffsmöglichkeiten. Auch andere Sicherheitssysteme wie Einbruchmeldeanlagen oder Videoüberwachungssysteme können auf diese Weise mit der Brandmeldeanlage zu einer Gesamtlösung vernetzt werden.

Ein sicherer Cloud-Service erfordert eine Reihe von Voraussetzungen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten. Eine starke Verschlüsselung und solide Zugriffskontrolle sind hierfür unerlässlich. Alle gespeicherten Daten sollten mit einer starken Verschlüsselungstechnologie geschützt sein, um sicherzustellen, dass sie nur von autorisierten Benutzern gelesen werden können. Darüber hinaus sind eine regelmäßige Überwachung und Aktualisierungen der Sicherheitsmaßnahmen erforderlich. Sicherheitslücken müssen umgehend mit Patches oder Updates geschlossen werden, um potenzielle Schwachstellen sofort zu beheben.

Sicherheits-Standard für Rechenzentren

Ein sicherer Cloud-Service muss über eine zuverlässige Datensicherung und Wiederherstellungsfunktion verfügen. Das amerikanische Uptime Institute, das einen weltweiten Standard für die Sicherheit von Rechenzentren definiert hat, klassifiziert vier sogenannten Tiers (englisch für Rang, Stufe). Die vier Tier-Klassen, die in der TIA-942 (Telecommunications Infrastructure Standard für Data Centers) vorgenommen wurden, legen die Ausfallsicherheit und die Verfügbarkeit eines Rechenzentrums fest.

Tier 1-Rechenzentren weisen meist eine einfache Infrastruktur auf und sind am wenigsten zuverlässig, während Tier 4-Datacenter im Aufbau die komplexesten sind und über die meisten redundanten Komponenten verfügen. Anwender können dadurch mit einer maximalen Ausfallzeit von lediglich 0,8 Stunden pro Jahr rechnen, womit die Verfügbarkeit bei 99,99 Prozent liegt. Allerdings ist der technische Aufbau hier sehr komplex und anspruchsvoll. Das bedeutet dementsprechend hohe Kosten für die Realisierung.

Brandschutzexperten müssen auch IT-Sicherheitsexperten sein

Mit dem Angebot einer digitalen Anwendung geht die Verantwortlichkeit der Brandschutzexperten über den reinen Brandschutz hinaus. Sie umfasst zusätzlich die Vermeidung vor Cyberangriffen auf das Brandmeldesystem und die Kundendaten sowie den verantwortungsvollen Umgang mit sensiblen Informationen.

Es ist von entscheidender Bedeutung, dass Hersteller von Brandmeldeanlagen in der Lage sind, potenzielle Schwachstellen in den digitalen Brandschutzsystemen zu identifizieren und geeignete Sicherheitsmaßnahmen zu ergreifen. Dazu gehört beispielsweise die regelmäßige Aktualisierung von Sicherheitssoftware, die Implementierung von Firewalls und Verschlüsselungstechnologien wie die Schulung der Mitarbeiter im Umgang mit sensiblen Daten. Nur durch eine umfassende Sicherheitsstrategie können Hersteller diese Verantwortung wahrnehmen und das Vertrauen ihrer Kunden in ihre digitalen Lösungen stärken.

Eigene Cloud-Lösungen schaffen Sicherheit

Für den sicheren Zugriff auf die Alarm- und Sicherheitssysteme nutzt Securiton Deutschland die firmeneigene Cloud-Lösung der Securitas Gruppe Schweiz. „Damit haben wir die komplette Kette vom Sensor bis zur Private Cloud in der eigenen Hand und die volle Kontrolle über alle Sicherheitsaspekte“, berichtet Volker Benz, Produktmanager Digitale Applikationen bei Securiton Deutschland. Die beiden georedundanten Rechenzentren entsprechen der Tier-Klasse 4 und weisen damit eine Höchstverfügbarkeit auf höchstem Sicherheitsstandard auf.

Um Zugriffe Dritter zu minimieren, wird die eigens beschaffte Hardware selbstständig gewartet und viele Prozesse möglichst automatisiert abgebildet. Dazu gehört beispielsweise auch die Konfiguration der Router für die Brandmeldezentralen. Die Router selbst werden regelmäßig mit Sicherheitsupdates versorgt und der Datenaustausch zwischen Router und Cloud wird auf ein Minimum reduziert, um möglichst wenig Angriffsfläche zu bieten. Die Datenhoheit wird zusätzlich durch stark eingeschränkte Zugriffsrechte der Systempartner gesichert.

So verhindert Securiton zuverlässig den Zugriff Dritter und damit den Missbrauch von sicherheitsrelevanten und kundenspezifischen Daten. Die Server werden nebst umfassender Sicherheitstechnik vor Ort sogar vom eigenem Sicherheitspersonal der Securitas Gruppe Schweiz bewacht, um physische Manipulation oder Diebstahl zu verhindern.

Die Digitalisierung des Brandschutzes bietet zweifellos viele Vorteile. Aber es ist wichtig, dass die Sicherheit der Daten dabei nicht vernachlässigt wird. Nur durch eine umfassende und proaktive Herangehensweise an die Datensicherheit kann gewährleistet werden, dass die digitalen Lösungen im Brandschutz effektiv und sicher eingesetzt werden können. GIT

Securiton Deutschland
www.securiton.de