Fernzugriff auf die Brandmeldeanlage

Anzeige und Bedienung mittels Smartphone, Tablet oder PC

Ing. Mag. Andreas Kurzweil

Labor Strauss Sicherungsanlagenbau GmbH

A-1231 Wien · Wiegelestraße 36

Tel.: 01 521 14-0 · Fax: 01 521 14-27 · office@lst.at · www.lst.at

Mobile Geräte für die Telekommunikation sind alltägliche Begleiter unseres Lebens geworden. Große Teile der Bevölkerung besitzen Smartphones und verwenden regelmäßig das eine oder andere Anwenderprogramm – kurz „App" genannt. Die unzähligen angebotenen Apps umfassen alle Bereiche des täglichen Lebens wie Unterhaltung, Informationsdienste, Spiele und Sport. Aber auch gewerbliche oder industrielle Anwendungen sind häufig zu finden.

Über Apps können heute auch viele technische Produkte über die Ferne gesteuert werden. Von der Einstellung des Videorecorders über die Fernsteuerung eines Spielzeugautos bis hin zur Programmierung des Rasenmähers lassen sich viele Geräte über eine mobile Applikation aus der Ferne bedienen. Daher liegt es nahe, auch industrielle Anlagen mit einem Fernzugriff auszustatten und eine Bedienung mittels Mobiltelefon oder PC zu ermöglichen. Im Bereich der Brandmeldeanlagen bieten hierfür wenige Hersteller spezielle „Brandmelde-Apps" an.

Nutzen für Endkunden, Servicedienste und Einsatzkräfte

Ein mobiler Zugriff auf die Brandmeldeanlage bietet viele Vorteile gegenüber der Bedienung der Brandmelderzentrale vor Ort. Hier ist zuerst der zeitlich und räumlich unabhängige Überblick über alle Anlagenzustände zu nennen. Die mobile Applikation gibt jederzeit und an jedem Ort Auskunft über die momentan anstehenden Alarme, Störungen, Abschaltungen oder aktivierten Brandfallsteuerungen.

Bei Eintreffen eines wichtigen Ereignisses – zum Beispiel eines Brandalarms – kann eine Nachricht an den Anlagenbetreiber ausgelöst werden. Ist die mobile Applikation in der Lage, detaillierte Informationen über den Einsatzort zu geben oder sogar einen Gebäudeplan darzustellen, können sich die Einsatzkräfte bereits am Weg zum betreffenden Objekt umfassend auf den Einsatz vorbereiten. Gleichermaßen kann ein Brandwart vor Ort – nach Abstellen der Sirenen und Start der Interventionsschaltung – den betroffenen Bereich erkunden und die Zentrale im Falle eines Fehlalarms direkt per Smartphone rückstellen. Dadurch wird nicht nur Zeit gespart, für diesen Vorgang ist auch nur eine Person erforderlich.

Im Zuge der Inbetriebnahme kann der Anlagenerrichter über die mobile Applikation eine komfortable Melderprüfung vornehmen. Eine Meldergruppe nach der anderen wird per Fernbedienung in den Prüfzustand geschaltet. Nach Auslösen des Melders wird das Eintreffen des Prüfalarms am mobilen Gerät des Technikers angezeigt. In gleicher Weise kann ein Wartungstechniker eine Einmann-Revision oder Störungsbehebung durchführen. Ohne Sichtkontakt oder Sprechverbindung zum Personal an der Zentrale können die Brandmelder bequem geprüft werden. Das spart Zeit und senkt die Kosten für den Einsatz.

Risiken und Sicherheit beim Fernzugriff

Ein Brandmeldesystem erfordert – im Gegensatz zu Anwendungen im Privatbereich – ein sehr hohes Maß an Sicherheit gegen unberechtigten Zugriff. Ist diese Sicherheit nicht gegeben, könnte sich ein Unbefugter Zugang zur Brandmeldeanlage verschaffen. Das Auslesen des aktuellen Zustands einer Brandmeldeanlage – etwa, wieviele Abschaltungen gerade anstehen – mag noch relativ harmlos erscheinen. Wenn es aber darum geht, dass ein Unbekannter selbst eine Abschaltung vornimmt und anschließend ein Brandereignis nicht erkannt wird, wird das Ausmaß des Schadens schnell sichtbar. Deshalb gilt es hier, geeignete technische und organisatorische Schutzmaßnahmen vorzusehen und umzusetzen. Die Verantwortung hierfür liegt einerseits beim Hersteller der Brandmelderzentrale und des Fernzugriff-Systems sowie

andererseits beim Planer, Errichter und Betreiber der Brandmeldeanlage.

Der ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e. V. – hat in Deutschland hierfür die Empfehlung 33010 „Merkblatt für die Interaktion mobiler Endgeräte mit Brandmelderzentralen über IP-Netze“ herausgegeben. In Österreich unterliegt der Fernzugriff und die mobile Applikation – genauso wie ein stationäres Einsatzleitsystem – der ÖNORM F 3003 „Brandmelde-Einsatzleitsysteme“. Diese Norm regelt die Darstellung des Zustandes und die Bedienung von Brandmelderzentralen. Die ÖNORM F 3003 wird derzeit überarbeitet, die endgültige Fassung wird voraussichtlich im Laufe des Jahres 2016 erscheinen.

Im Bereich der technischen Maßnahmen ist die **Informationssicherheit** durch geeignete Technologien wie Kryptografie zu gewährleisten. Dies gilt umso mehr, als sich Smartphones, Tablets und PCs mit mobilen Applikationen öffentlicher IP-Netze bedienen. Dabei sind insbesondere die Vertraulichkeit, die Authentizität, die Integrität und die Verfügbarkeit der Daten sicherzustellen. Diese untereinander eng verbundenen Konzepte sollen nachfolgend kurz erläutert werden:

- Die **Vertraulichkeit** der Daten – also ihre Nicht-Einsehbarkeit durch Dritte – kann durch Verschlüsselung der Verbindung erreicht werden. Weder der Zustand der Brandmeldeanlage noch eine Bedienung durch den Benutzer soll einem Unbefugten bekannt werden. Für die Verschlüsselung gibt es zahlreiche erprobte Technologien – asymmetrische, symmetrische und kombinierte kryptografische Verfahren.
- Bei der **Authentizität** der Daten gilt es, den Benutzer des Fernzugriff-Systems zu identifizieren und anhand seiner Berechtigung zu authentifizieren. Somit besteht kein Zweifel an der Urheberschaft des Fernzugriffs – sei es zur Informationsabfrage oder für einen Bedienvorgang. Die Identifizierung eines Benutzers wird meist durch Überprüfung des Benutzernamens und Passworts beim Verbindungsaufbau geregelt. Dies setzt eine personalisierte Registrierung der Benutzer beim Betreiber des Systems voraus.
- Die **Integrität** der Daten muss gewährleistet werden, um sicherzugehen, dass Daten nicht unterwegs verändert wurden – sei es ungewollt, etwa durch eine fehlerhafte Datenübertragung oder durch bewusste Manipulation. Die Integrität der Datenübertragung kann ebenfalls durch kryptografische Techniken – mittels Signatur – sichergestellt werden.
- **Verfügbarkeit** bedeutet, dass das Fernzugriff-System jederzeit zur Verfügung steht. Die Verantwortung dafür liegt hauptsächlich im Bereich der IT-Infrastruktur. Hier ist auf eine funktionierende Hardware, aktuelle Software und Schutzmaßnahmen gegen Cyberangriffe – zum Beispiel Installation von Antivirus-Software und einer Firewall – zu achten. Beim Fernzugriff über ein Mobilfunknetz ist natürlich auch dessen Verfügbarkeit maßgeblich.

Abgesehen von den beschriebenen Sicherheitsmaßnahmen ist natürlich auch darauf zu achten, dass ein Fernzugriff-System keinerlei negative Auswirkungen auf die Brandmeldeanlage hat. Die Funktion der Brandmelderzentrale gemäß EN 54-2 muss in jedem Fall gegeben sein. Neben den technischen Maßnahmen sind auch **organisatorische Regelungen** von großer Bedeutung. Die Geheimhaltung von Zugangsdaten, der Schutz von mobilen Geräten gegen Verlust oder Diebstahl sowie eine restriktive Vergabe von Berechtigungen sind hier ebenso wichtig wie die regelmäßige Wartung der Hard- und Software der gesamten IT-Infrastruktur. Auch die Schulung der Benutzer und Sensibilisierung hinsichtlich sicherheitskritischer Applikationen sind ein wesentlicher Beitrag zur Sicherheit.

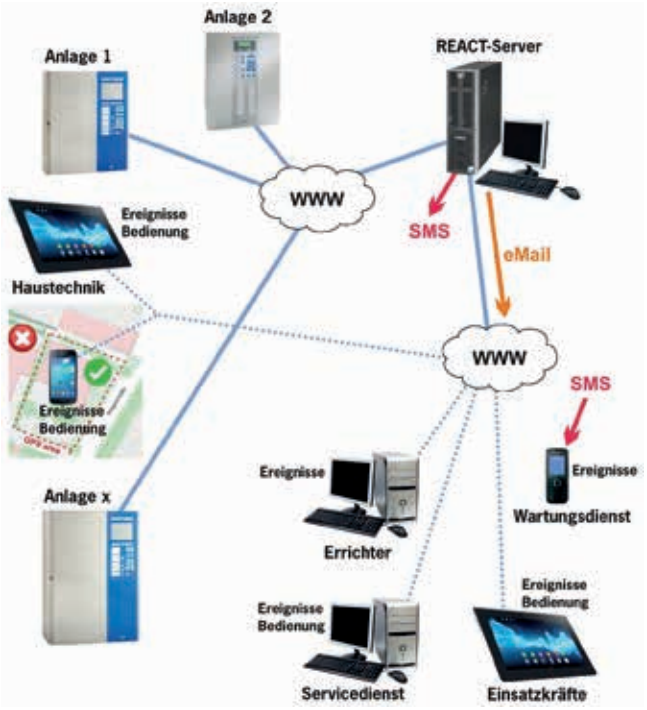

Abb. 1: Übersicht über das Fernzugriff-System REACT

Fernzugriff am Beispiel des REACT-Systems

Mit dem „**RE**mote **AC**cess **T**ool“ können die Brandmelderzentralen Serie BC600 und Serie BC216 von Labor Strauss über die Ferne bedient und alle Betriebszustände abgefragt werden. Der Zugriff ist mittels Smartphone, Tablet oder PC möglich. Die Verbindung zur Zentrale wird immer über einen für diese Applikation konfigurierten Server abgewickelt, der die Kommunikation entkoppelt. Eine direkte Datenverbindung zwischen dem mobilen Gerät mit der REACT-Applikation und der Brandmelderzentrale ist aus Sicherheitsgründen nicht möglich.