15. Fernzugriff auf Brandmeldeanlagen

Mit zunehmendem Einzug in die Brandschutzpraxis zeigt sich, dass in der Digitalisierung tatsächlich ein enormes Potenzial für mehr Effizienz, höhere Sicherheit und Wachstum steckt. Gerade mit Blick auf den Fachkräftemangel bieten digitale Tools mit Fernzugriffsoption einen hohen Mehrwert und spürbare Entlastung im Arbeitsalltag.

15.1 Vorteile dieser Technologie und deren Anwendung

Mit der Internet-Technologie und entsprechenden mobilen Endgeräten (Smart Devices) können wichtige Informationen aus Brandmeldeanlagen (BMA) an hilfeleistende Stellen, Technikabteilungen oder mobil direkt an einen zuständigen Service-Techniker weitergeleitet werden. Diese Technik kann auch zur zusätzlichen Weiterleitung von Alarmmeldungen an die Feuerwehr genutzt werden, sofern diese nicht als Erstinformationen dienen!

Auch Betreibern von Objekten (Nutzern) stehen zeitnahe und aktuelle Informationen über den Zustand ihrer BMA zur Verfügung. Gerade für den organisatorischen Brandschutz und sich daraus ergebenden Folgemaßnahmen ist diese Form der Informationen von Bedeutung, insbesondere für das Handeln verantwortlicher Personen im Ereignisfall (z. B. stiller Alarm in einem Krankenhaus, personelle Maßnahmen zur Vermeidung von Falschalarmen nach VDE 0833-2), bei einer Evakuierung oder die Vorgehensweise einer vor Ort befindlichen Werkfeuerwehr. Ausgehend von dem genehmigten Brandschutzkonzept und der Alarmorganisation können so zusätzlich Lösungen geschaffen werden, die zur Sicherstellung des Betriebsablaufs und der Schutzziele beitragen.

Auch für Errichter von BMA ist die Nutzung dieser Lösungen von Vorteil. Alarme, Störungen und Abschaltungen können genau analysiert werden. Auch im Hinblick auf die nach der DIN 14675-1 und VDE 0833-2 geforderte Instandhaltung können Programme für mobile Endgeräte, wie Tablet-PCs genutzt werden und unterstützen die Organisation sowie die Dokumentation und Nachweisführung. Weiterhin übernehmen Programme auch den Zugriff auf die BMA, um umfangreiche Servicemaßnahmen und Analysen zu unterstützen. Zusätzlich dienen diese Lösungen bei Betreibern und Errichtern zur Personal- und Kostenoptimierung, insbesondere unter den Herausforderungen des Fachkräftemangels.

15.2 Lösungen

Für die technische Umsetzung von Marktanforderungen (wie z.B. Serviceeinsätze und Unterstützung der Betreiber aus der Ferne) wird u. a. die Internet-Technologie genutzt. Hierbei unterscheidet man grundsätzlich den Ort von Kunden-Daten und Anwendungs-Software (Programm).

15.2.1 Cloud-basierende Lösungen

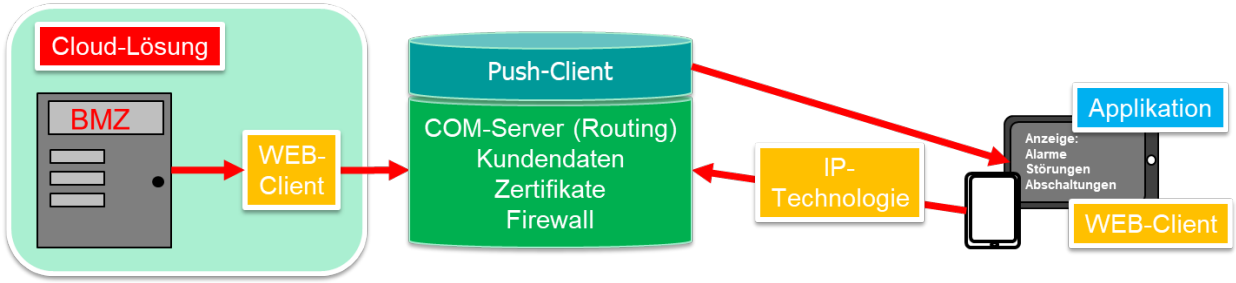
Die Cloud-basierende Lösung nutzt Kommunikationsserver (COM-Server) professioneller Anbieter, die das Routing (IP) und Authentifizierung (ID) der mobilen Endgeräte, das Übertragungsverfahren (Verschlüsselung, z. B. SSL (Secure Socket Layer) mittels Zertifikat) sowie das Speichern aller Daten (Verbindungsdaten, Kundendaten) und die dazu notwendigen Schutzmaßnahmen (Firewall) übernehmen.

Die Programme (Apps) auf den mobilen Endgeräten nutzen das Leistungsvermögen des jeweiligen Betriebssystems. Der an der BMZ befindliche Client-Server sendet bei einer Zustandsänderung der BMA das entsprechende Ereignis an den COM-Server. Das registrierte Endgerät (Client) kommuniziert mit dem COM-Server und erhält bei Zustandsänderungen die aktuelle Information.

Bestimmte Ereignisse (Alarme, Serviceinformationen) können über ein WEB-Portal eingesehen werden. In Abhängigkeit von verschlüsselten Protokollen können Möglichkeiten einer Bedienung (BMZ-Bedienfeld) zur Verfügung gestellt werden. Die Zugänge zu diesen Daten sind nach heutigem Stand der Technik über entsprechende Schutzmaßnahmen geregelt.

Vorteil:	Nachteil:
Das Programm wird ausschließlich durch Hersteller auf dem COM-Server aktualisiert. Nötige Zertifikate (z. B. Push-Notifikation) werden am COM-Server bereitgestellt und müssen nicht vom Nutzer kontrolliert werden. Eine Anbindung an das IT-Netzwerk vor Ort ist nicht erforderlich. Die Sicherheit und die Infrastruktur werden vom Hersteller (Anbieter)gestellt.	Die Sicherheit der Daten und die Verfügbarkeit der Dienste ist vom Anbieter des WEB-Servers abhängig. Die Anzahl der mobilen Endgeräte und Menge der Daten (Speicherbedarf) können von technischer Seite her begrenzt sein. Die Anwendungen lassen sich bei Hinzunahme oder Tausch von mobilen Endgeräten aufgrund der Authentifizierung nur mit Aufwand portieren. Um die Unabhängigkeit vom IT-Netzwerk des Kunden zu gewährleisten, sind laufende Kosten für Mobilfunk-Verträge notwendig.

Schema:

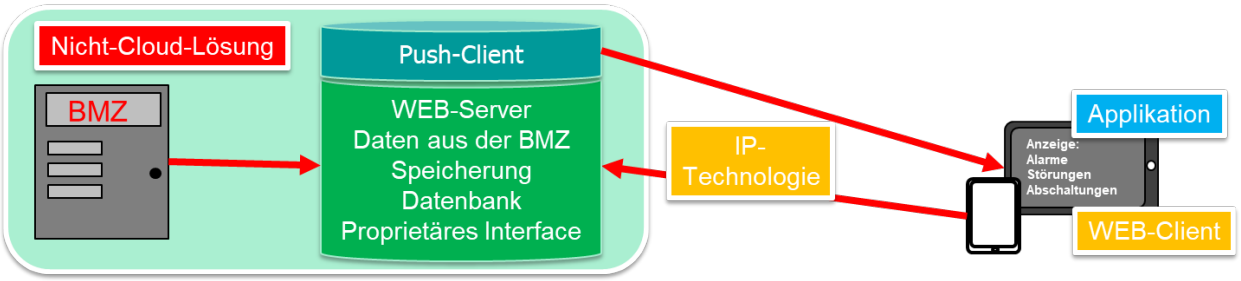


15.2.2 Nicht-Cloud-basierende Lösungen

Die Nicht-Cloud-basierende Lösung benötigt keinen COM-Server im eigentlichen Sinne, da die mobilen Endgeräte eine eigene Kommunikation mit dem an der BMA befindlichen WEB-Server aufbauen. Das Übertragungsverfahren kann mittels Verschlüsselung gesichert werden. Der Programm- und Datenspeicher befindet sich in unmittelbarer Nähe der BMZ und verfügt über entsprechende Schutzmaßnahmen.

Die Programme (Apps) auf den mobilen Endgeräten nutzen das Leistungsvermögen des jeweiligen Betriebssystems. Mit den Zugangsdaten des mobilen Endgerätes wird das zyklische Abfragen (Polling) des WEB-Clients autorisiert. Nach Zustandsänderung der BMA (Ereignis) empfängt der WEB-Client (Endgerät) die entsprechenden Daten. In Abhängigkeit von verschlüsselten Protokollen können Möglichkeiten einer Bedienung (BMZ-Bedienfeld) zur Verfügung gestellt werden.

Vorteil:	Nachteil:
Das Programm sowie die gespeicherten Daten stehen ausschließlich vor Ort dem Kunden zur Verfügung. Der Kunde hat Rechte eines Administrators und vollen Zugriff auf das System. Durch die Einbindung in das IT-Netzwerk des Kunden entstehen keine laufenden Kosten. Die Größe des Speicherbedarfs sowie die Anzahl der mobilen Endgeräte sind nahezu unbegrenzt.	Um Zustandsänderungen den Endgeräten mitzuteilen, muss der Client-Server „immer von außen“ erreichbar sein. Sofern keine andere Anschlussmöglichkeit gewählt wurde (separater DSL-Anschluss, LTE-Router), ist die Abstimmung mit der örtlichen IT-Abteilung zwingend erforderlich. Aktualisierungen entsprechender Software müssen dem WEB-Server ermöglicht und können mittels eines automatischen Updates bereitgestellt werden. Das bedeutet, das Netzwerk des Kunden für Zugriffe von außen passend zu paramerieren und erfordert besondere Schutzmaßnahmen durch den Kunden (z. B. Subnetz). Zertifikate sind auf dem WEB-Server hinterlegt. Um der Kunden IT dies zu übermitteln werden IT-Fachkenntnisse benötigt.

Schema:


15.2.3 Remote-Services

Für den Remote-Service sind PC-Programme, APPs oder Web-Applikationen notwendig, die von Herstellern der BMZ zur Verfügung gestellt werden, um aus der Ferne auf eine BMZ zuzugreifen. Diese Lösungen (Programme) besitzen umfangreiche Leistungsmerkmale (Programmierung der BMZ), die mittels besonders geschützter Übertragungsverfahren, wie Virtual Private Network (VPN) einen direkten Zugriff auf eine BMZ besitzen und somit umfassende Änderungen vornehmen können.

Eine ständige Zustandsanzeige im eigentlichen Sinn (Ereignisse der BMZ) ist prinzipiell möglich, spielt aber bei diesen Anwendungen eine untergeordnete Rolle. Die Anschaltung eines Service-PCs via VPN an eine BMZ ermöglicht eine zuverlässige und sichere Verbindung und integriert Teile der BMZ in ein geschlossenes Netzwerk. Neben dem PC-Programm für den Service der BMZ können auch Möglichkeiten einer Bedienung (BMZ-Bedienfeld) zur Verfügung gestellt werden.

Neben den eigentlichen Informationen (z.B. für die Instandhaltung) können unter Berücksichtigung des Datenschutzes auch alle Betriebszustände der BMZ übertragen und ausgewertet werden (Meta-Daten).

Vorteil:	Nachteil:
Die Anschaltung eines Service-PCs via VPN an eine BMZ ermöglicht eine zuverlässige und sichere Verbindung und integriert Teile der BMZ in ein geschlossenes Netzwerk.	Es müssen Verfahren zur Authentifizierung (Schlüssel) bereitgestellt werden. Die VPN-Server und das Netzwerk benötigen eine hohe Verfügbarkeit und administrative Kenntnisse in Sachen IT-Technologie. Die Programme werden meist dem Endkunden nicht zur Verfügung gestellt und sind häufig nur Bestandteil von Instandhaltungsverträgen durch den Lieferanten.
Schema: