ZVEI | MERKBLATT

ZVEI Merkblatt für die Interaktion mobiler Endgeräte mit Brandmelderzentralen über IP-Netze

33010:2014-02

INHALT

1. VORWORT

Eine Applikation für den Fernzugriff (AFFZ) dient zur Interaktion mobiler Geräte mit Brandmelderzentralen über nicht vertrauenswürdige Netze wie z. B. das Internet. In solchen Netzen sind zusätzliche Maßnahmen erforderlich, um die Grundsätze der Authentizität, Vertraulichkeit und Verfügbarkeit der Daten zu gewährleisten und die uneingeschränkte Funktion der Brandmelderzentrale (BMZ) sicherzustellen. Hieraus ergibt sich die Notwendigkeit, Themen wie Informationssicherheit bezogen auf das Anwendungsgebiet zu berücksichtigen.

Durch den Einsatz mobiler Geräte entstehen zusätzliche Gefahren (z. B. Verlust, Diebstahl, Weitergabe an unbefugte Dritte). Diese müssen dem Benutzer aufgezeigt werden und bedürfen besonderer organisatorischer Regelungen und technischer Maßnahmen. Dieser Leitfaden gibt unverbindliche Empfehlungen für die Umsetzung der vorgenannten Grundsätze.

Die Anwendung dieses Leitfadens darf unter Berücksichtigung weiterer Anforderungen auch in anderen Anwendungsszenarien zum Einsatz kommen. Es werden Anforderungen und nicht konkrete Lösungen spezifiziert um insbesondere die Sicherheitsanforderungen optimal mit dem neusten Stand der Technik umsetzen zu können.

2. ANWENDUNGSBEREICH

Eine AFFZ dient zur Interaktion zwischen mobilen Geräten und Brandmelderzentralen über IP-Netze. Eine AFFZ wird beispielsweise auf einem mobilen Smart Device, Laptop oder auf einem anderen rechnergestützten mobilen System betrieben. Die möglichen Benutzer einer AFFZ sind Betreiber, Installations-, Wartungs- und Instandhaltungspersonal sowie Feuerwehr bzw. andere gefahrenabwehrende Einrichtungen.

Dieser Leitfaden berücksichtigt sicherheitsrelevante Aspekte, die sich für Brandmeldezentralen im Zusammenhang in der Verbindung mit dem Internet ergeben. Die Aufgabe der vollständigen Beurteilung der Informationssicherheit liegt über diesen Leitfaden hinaus bei dem Hersteller der Brandmelderzentrale / AFFZ und weiteren beteiligten Parteien (z. B. Planer und Betreiber) des Gesamtsystems.

Die Verwendung von Technologien, die nicht im Verantwortungsbereich des Herstellers der AFFZ liegen, kann unabhängig von der Einhaltung dieses Leitfadens Einfluss auf die Verfügbarkeit haben.

Dieser Leitfaden beschreibt keine Anforderungen:

- an die Verfügbarkeit der IT-Infrastruktur oder der rechnergestützten mobilen Systeme. Die Verfügbarkeit ist durch den Hersteller und den weiteren beteiligten Parteien je nach Anwendungsgebiet sicherzustellen.
- an die Hardware der in diesem Zusammenhang erwähnten rechnergestützten mobilen Systeme sowie deren Infrastruktur (z. B. Switches, Server)
- für Benutzeroberflächen der AFFZ
- an Verbindungen durch Servicelaptops zur Brandmelderzentrale, die einen anderen Kommunikationskanal nutzen (z. B. Direktanschluß)

3. BEGRIFFE

3.1 Applikation für den Fernzugriff (AFFZ)

Anwendung (Programm) für ein mobiles Gerät zur Kommunikation mit der BMZ.

3.2 Authentifizierung

Überprüfen einer im Rahmen der Authentisierung erhaltenen Information.

3.3 Authentisierung

Vorlage eines Nachweises eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

3.4 Authentizität

Authentizität ist die Eigenschaft, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden..

3.5 Brandmelderzentrale (BMZ)

Einrichtung gemäß EN54-2 für die Aufnahme, Auswertung, Anzeige und Weiterleitung von Meldungen und Informationen (z. B. Feueralarm- und Störungsmeldungen).

3.6 Brute Force Angriff

Im Bereich der Kryptoanalyse verwendete Methode zur Entschlüsselung durch Ausprobieren aller möglichen Schlüssel.

3.7 Denial-of-Service

Bezeichnet die Nichtverfügbarkeit von Diensten, welche meist in Folge einer Überlast durch Angriffe auf die zugrundeliegenden Infrastruktur auftritt.

3.8 Integrität

Korrektheit (Unversehrtheit) von Daten, d.h. sie sind vollständig und unverändert

3.9 Secure Development LifeCycle (SDL)

Entwicklungszyklus für vertrauenswürdigen Computereinsatz

3.10 Service Applikation

Anwendung (Programm) für die Kommunikation der Brandmelderzentrale mit der AFFZ. Die Serviceapplikation stellt den Zugangspunkt für AFFZ zur BMZ zur Verfügung und kann weitergehende Dienste (z. B. Webdienste) anbieten.

Hinweis: Diese kann in die BMZ integriert oder auf einem eigenständigen System sein.

3.11 Smart Device

Mobiles Gerät, typischerweise Smartphone, Tablet oder ähnliches, auf dem die AFFZ läuft.

3.12 Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen.

Hinweis: Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

4. SYSTEMANFORDERUNGEN

4.1 Bezug zu den Regelwerken

In diesem Leitfaden wird die Anwendung für die Interaktion über IP Netze (AFFZ) behandelt. Die AFFZ ist kein Ersatz für die nach EN54-2 verpflichtenden Anzeige- und Bedienelemente, vielmehr eine Ergänzung. Die AFFZ ist kein Bestandteil der Brandmelderzentrale.

Für weitere Informationen siehe Anhang A.

4.2 Zugangsebenen

Es gelten die Zugangsebenen nach EN 54-2.

Für alle Zugangsebenen ist eine Authentifizierung erforderlich (siehe 5.3.3). Diese sollte personalisiert sein. Die Nutzung von unspezifischen Authentifizierungen (z.B. Person 1, Zugang A), bei denen Nutzer nicht eindeutig identifiziert werden können oder sich einen Zugang teilen, sollten vermieden werden. Sollte dies nicht praktikabel sein, muss eine organisatorische Lösung sicherstellen, dass die Nutzer auch nachträglich identifiziert werden können.

Zugang und Berechtigungen sollten entzogen werden können.

Einschränkungen innerhalb der Zugangsebenen können sich abhängig vom geographischen Ort des Benutzers hinsichtlich der erlaubten Funktionen ergeben.

Es werden 3 Interaktionskategorien unterschieden:

1. Visualisierung ohne funktionales Einwirken (z. B. mit Zusatzinformationen z. B.Laufkarten, Ortsinformationen)
2. Visualisierung mit eingeschränktem funktionalen Einwirken (z. B. Abschalten)
3. Visualisierung mit uneingeschränktem Einwirken (z. B. Fernunterstützung) insbesondere unter Berücksichtigung von Anhang A

Zugangsebene nach EN54-2	**Interaktions-kategorie der AFFZ**		
	1	**2**	**3**
Informationen aus Zugangsebene 1	●	●	●
Informationen welche über Zugangsebene 1 hinausgehen	●	●	●
Einwirken auf die Zentrale durch Bedienfunktionen Zugangsebene 1		●	●
Einwirken auf die Zentrale durch Bedienfunktionen Zugangsebene 2		●	●
Einwirken auf die Zentrale durch Bedienfunktionen Zugangsebene 3			●
Einwirken auf die Zentrale durch Bedienfunktionen Zugangsebene 4 (unter Berücksichtigung von Anhang A)			●

4.3 Anzeige- und Bedienfunktionen an der AFFZ

Die Anzeigen an der AFFZ müssen konsistent mit denen an der BMZ sein. Die Anordnung, der Umfang und die Darstellung müssen nicht der an der BMZ entsprechen.

Die möglichen und erlaubten Anzeige- und Bedienfunktionen der AFFZ müssen nutzungsbezogen zwischen den beteiligten Parteien vereinbart werden.

Die Bedienung zusätzlicher Funktionen über die AFFZ, welche nicht zu den verbindlichen Funktionen einer BMZ gehören (z.B. technische Steuerungen), sind jederzeit möglich, soweit die Verfügbarkeit der verbindlichen Funktionen nach EN54-2 sichergestellt ist.

4.4 Verbindung AFFZ - BMZ

Die AFFZ baut eine Verbindung über einen definierten Zugangspunkt (Service-Applikation) zu einer BMZ auf. Diese Verbindung muss die in diesem Kapitel nachfolgend definierten Anforderungen erfüllen. Im Folgenden werden Möglichkeiten beschrieben, bei denen der Zugangspunkt in verschiedenen Netzen liegen kann.

4.4.1 Systemaufbau

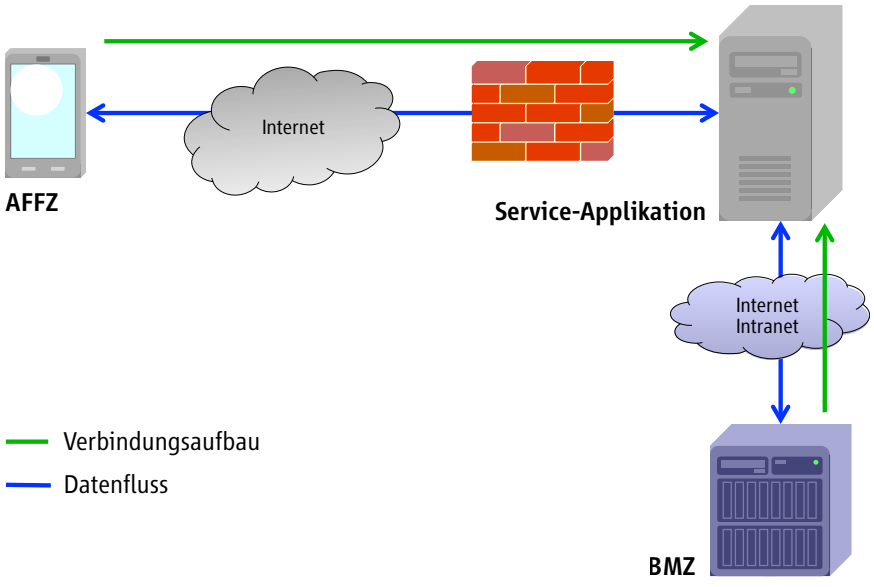
Das System besteht aus den folgenden Systemkomponenten

- AFFZ
- Serviceapplikation
- BMZ-Applikation

die an der Verbindung beteiligt sind.

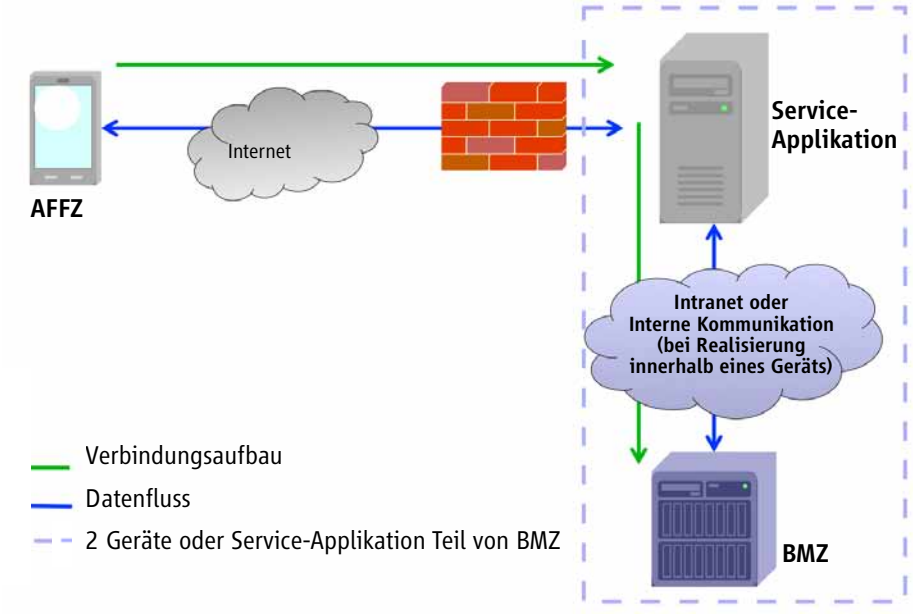
4.4.2 Direkte Verbindung in einem internen Netz

Die AFFZ und die Serviceapplikation befinden sich in einem internen Netzwerk das gegen einen unberechtigten Zugriff möglichst gut geschützt ist, z. B. Firmennetzwerk, eigenes Netz der Brandmeldetechnik. Die AFFZ baut eine direkte Verbindung zur Serviceapplikation auf. Es findet keine Verbindung über das Internet oder andere unsichere Netze statt.



4.4.3 Direkte Verbindung über Internet

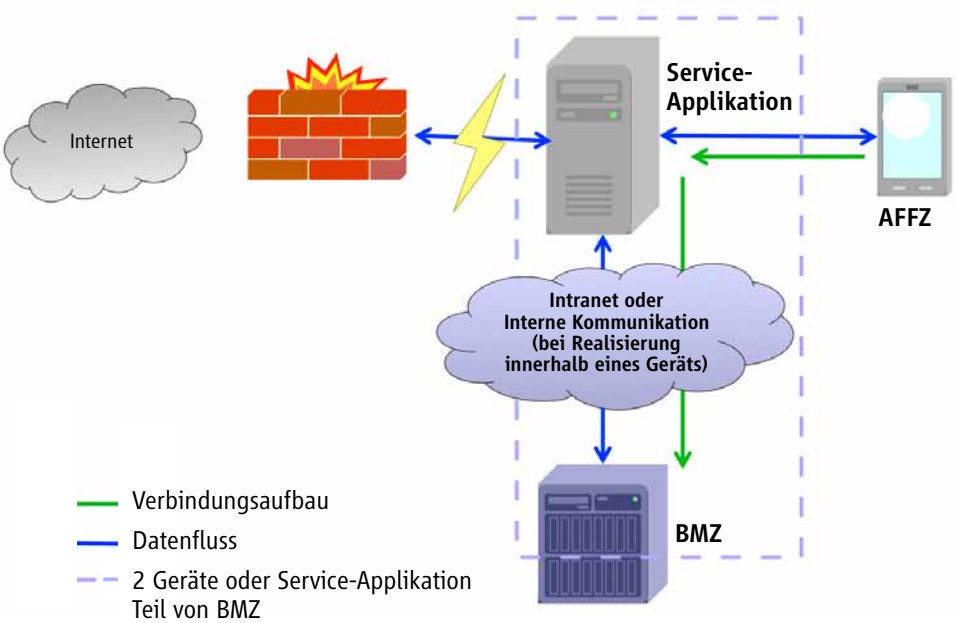
Die Service-Applikation ist direkt aus dem Internet erreichbar und in die BMZ integriert oder mit ihr direkt verbunden. Aufgrund der möglichen direkten Erreichbarkeit der BMZ ist diese Variante einer höheren Gefährdung durch Cyberangriffe ausgesetzt und ihr Einsatz sollte einer vorherigen Risikoabwägung unterzogen werden



4.4.4 Indirekte Verbindung über Internet

Die AFFZ auf dem Smart Device hat eine Verbindung zu einer Service-Applikation. Die BMZ hat ihrerseits eine Verbindung zu der Service-Applikation.

Die BMZ ist in diesem Fall aus dem Internet nicht zugreifbar.



5. ANFORDERUNGEN AN DIE INFORMATIONSSICHERHEIT

Da die AFFZ sicherheitskritische Funktionen steuert, sind an ein Informationssicherheitskonzept hohe Anforderungen zu stellen.

Neben technischen sollten auch organisatorische Maßnahmen durch die Beteiligten über eine Risikobeurteilung bewertet werden.[1]

5.1 Verfügbarkeit der BMZ

Funktionen der AFFZ dürfen keine negativen Auswirkungen auf die Verfügbarkeit des Brandmeldesystems haben.

Es sind geeignete Maßnahmen vorzusehen, um die Rückwirkungsfreiheit aus dem Netzwerk auf die BMZ zu gewährleisten. In diesem Zusammenhang bedeutet Rückwirkungsfreiheit, dass die zur Bearbeitung der AFFZ-Anbindung notwendigen Funktionen keinen Einfluss auf die verbindlichen Funktionen der BMZ nach EN54-2 haben.

5.2 Anforderungen an den Entwicklungsprozess

Bei der Erstellung der AFFZ und der Serviceapplikation auf dem Zugangspunkt sollte ein SDL eingehalten werden. Dazu gehört auch die grundsätzliche Unterziehung der Produkte einer technischen Sicherheitsanalyse (Penetrations- oder Schwachstellentests), bei denen nicht nur auf bekannte Schwachstellen, sondern auch auf neue, unbekannte Verwundbarkeiten getestet wird.

Es sollten bei Sicherheitsfunktionen möglichst die Standardfunktionen des Smart Devices sowie des jeweiligen Betriebssystems verwendet und eigene Implementierungen vermieden werden. Es wird zusätzlich die Verwendung von Sicherheitsbibliotheken empfohlen.

5.3 Anforderungen an die AFFZ

Für die sichere Verwendung der AFFZ ist die Sicherheit des mobilen Gerätes zu gewährleisten.[2]

Wenn keine Verbindung zur BMZ besteht, darf die AFFZ keine Statusinformationen ausgeben oder BMZ relevante Bedienschritte entgegennehmen und zwischenspeichern.

Sämtliche auf dem Gerät der AFFZ gespeicherten kritischen Daten müssen verschlüsselt werden.

Eine AFFZ sollte mit minimal möglichen Rechten auf dem Smart Device funktionieren. Ein Zugriff beispielsweise auf das Adressbuch sollte nicht erfolgen.

[1] Eine vertragliche Fixierung folgender Punkte ist zu empfehlen:
- Mögliche und erlaubte Anzeige- und Bedienfunktionen der AFFZ
- Verfügbarkeit der Infrastruktur / des IP-Netzes
- Zugriffs- und Verwendungsrechte

[2] Es sind die Empfehlungen des BSI zu berücksichtigen.

5.3.1 Anforderungen an die Integrität

Die AFFZ muss gegen Manipulation geschützt werden. Dazu gehören die Erkennung von Manipulation der AFFZ sowie die Verweigerung der Ausführung der AFFZ auf einem unsicheren Smart Device (beispielsweise gerootet/gejailbreaked, debugger aktiv). Die verwendete Lösung muss dem aktuellen Stand der Technik entsprechen und sämtliche kritische Daten müssen verschlüsselt gespeichert werden.

5.3.2 Registrierung der AFFZ

Jedes mobile Gerät, das die AFFZ nutzt, sollte an der Service-Applikation individuell registriert werden. Es muss innerhalb der Service Applikation die Möglichkeit zur Verwaltung verschiedener Smart Devices oder zugeordnete Benutzer geben, damit zuvor berechtigte Geräte oder Benutzer gesperrt werden können.

5.3.3 Anforderungen an die Authentizität

Jeder Benutzer muss sich über die AFFZ am Zugangspunkt authentifizieren. Dies gilt für alle Interaktionsebenen.

Nach einer definierten Zeit der Inaktivität muss man sich neu authentifizieren.

5.4 Anforderungen an die Kommunikation

5.4.1 Anforderungen an die Integrität und Authentizität

Die Integrität und Authentizität des Datenaustausches muss durch ein geeignetes Verfahren sichergestellt werden.

5.4.2 Verschlüsselung

Da sensible Daten übertragen werden, muss die Übertragung verschlüsselt erfolgen. Dies gilt für alle Interaktionsebenen.

5.5 Anforderungen an den Zugangspunkt im Internet (Serviceapplikation)

Aufgrund der Zugänglichkeit des Zugangspunkts durch das Internet sind Verfahren zu dessen Absicherung erforderlich. Die Applikation innerhalb des Zugangspunkts, mit der die AFFZ kommuniziert, muss durch angemessene Verfahren abgesichert sein.

5.5.1 Webanwendung

Sollte auf dem Zugangspunkt eine Internetanwendung mit Weboberfläche laufen, so muss diese entsprechend dem Stand der Technik abgesichert sein.

5.5.2 Login / Authentisierung

Allgemeine Best Practices sind anzuwenden. Siehe BSI Empfehlungen.

5.5.3 Logging

Wichtige Vorgänge, wie z. B. Verbindungen, Logins, fehlgeschlagene Logins oder Änderungen der Konfigurationsdaten, müssen protokolliert werden.

5.5.4 Netzwerkdienste

Im Bereich der Netzwerkdienste sind die entsprechenden Maßnahmen zur Systemhärtung anzuwenden wie z. B. Abschalten unbenutzter Dienste.
Es sollten Vorkehrungen gegen Angriffe (z. B. Denial of Service oder Brute Force-Angriffe) vorgesehen sein.

5.6 Dokumentation

Hersteller sollten die nachfolgend genannten Punkte bei der Dokumentation berücksichtigen, um einen sicheren Einsatz beim Kunden zu gewährleisten.

- Zielgruppen seitens eines Integrators oder Anwenders sind zu definieren, die aus sicherheitsspezifischen Überlegungen über die in der Dokumentation enthaltenen Informationen informiert werden müssen
- Sicherheitseigenschaften bzw. -funktionen der Komponente
- Risiken / Bedrohungen die durch die Komponente selbst abgedeckt werden
- Bedrohungen die im Rahmen einer Sicherheitsbewertung bzw. eines Sicherheitsmanagements vorhanden sind
- Welche Maßnahmen wurden getroffen, um das Produkt gegen diese Bedrohungen abzusichern
- Dienste, die (mit den im Produkt integrierten Mechanismen) nicht abgesichert werden können und daher ergänzenden technischen oder organisatorischen Sicherheitsmaßnahmen bedürfen
- Sämtliche Schnittstellen und Funktionen dokumentiert
- Verzicht auf Hintertüren oder versteckte Funktionen
- Empfehlungen bzgl. der Konfiguration für einen sicheren Betrieb
  - Ausreichende Hinweise für die Änderung von Standardpasswörtern und zum Deaktivieren von nicht benötigten Accounts
  - Konfigurationsoptionen / -alternativen mit den entsprechenden Konsequenzen
  - Einstellungen die als kritisch sind bzw. zu einer erhöhten Gefährdung führen können.
- Checkliste zur Übersicht über die Konfiguration und deren sicherheitsspezifische Implikationen
  Angabe der Konfiguration für andere Komponenten der eingesetzten Infrastruktur (z. B. Router & Switches)
- Referenzen auf weiterführende Informationen zur Absicherung bzw. zum sicheren Betrieb

6. ANHANG A IT-EMPFEHLUNGEN

A.1 BSI-Empfehlungen

- BSI IT-Grundschutz
- Sicherer Fernzugriff auf das interne Netz (ISi-Fern)
- Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)
- Anforderungen an netzwerkfähige Industriekomponenten
- Sichere Passwörter in Embedded Devices
- Entwicklung sicherer Webanwendungen
- Sichere Softwareentwicklung unter Android
- Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen

A.2 IEC 62443

Internationale Normenreihe über die „IT-Sicherheit für industrielle Leitsysteme – Netz- und Systemschutz".

- Teil 1-1: Terminology, concepts and models
- Teil 2-1: Establishing an industrial automation and control system security program
- Teil 3-1: Security technologies for industrial automation and control systems
- Teil 3-3: Security for industrial process measurement and control Network and
- system security

A.3 VDI Richtlinie 2182

Informationssicherheit in der industriellen Automatisierung

A.4 BDEW-Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

Grundsätzliche Sicherheitsmaßnahmen für Steuerungs- und Telekommunikationssysteme für Unternehmen der Energiewirtschaft

7. ANHANG B
NATIONALE ANWENDUNGSVORSCHRIFTEN

Referenzliste zu Anwendungsrichtlinien. Diese erhebt keinen Anspruch auf Vollständigkeit.

B.1 Deutschland

VDE 0833-1 Absatz 5.1.4

B.2 Niederlande

NEN 2654-1 Anhang F

B.3 Österreich

Zusätzliche spezielle Anforderungen in Österreich zu GPS aus Sicht der Prüfstelle:

- Ist zum Betrieb der AFFZ an der Brandmelderzentrale eine spezielle Hardware (z. B. ein PC) erforderlich, so muss sich diese entweder in einem ständig versperrten Raum mit Zutritt nur für geschultes Personal oder in einem versperrten Zentralenschrank befinden.

- Für den Einsatz in Bedienebene 2 gemäß ÖNORM EN 54-2 sind folgende Auflagen einzuhalten:

  - Die Bedienung darf nur möglich sein, wenn sich das Gerät auf dem Betriebsgelände oder in unmittelbarer Nähe zu diesem befindet: dies ist durch Eingabe von GPS-Daten zu realisieren. Die Objektstrukturen (Betriebsgelände) sind mittels Polygonen nachzubilden.

  - Es muss für Inspektoren der Prüfstelle f. Brandschutztechnik jederzeit möglich sein, auf einfache Art und Weise die einprogrammierten GPS Daten für ein konkretes Objekt (Funktionsgrenzen auf einem Plan) abzufragen.

  - Es muss sichergestellt sein, dass alle Schaltvorgänge wie Ab- und Einschaltungen, Alarmrückstellungen etc., die über das Gerät vorgenommen werden, elektronisch protokolliert werden und bei Bedarf ausgedruckt werden können. Dies kann durch folgende technische oder organisatorische Maßnahmen erreicht werden:
    – Erinnerungsfunktion direkt am mobilen Endgerät, falls Eintragungen per Hand im Kontrollbuch durchzuführen sind
    – ein Web/Cloud-Kontrollbuch ist zulässig, falls ein Ausdrucken dieses Kontrollbuches in regelmäßigen Abständen (mindestens einmal wöchentlich) erfolgt und dies durch Anweisungen im Betrieb geregelt ist

  - Es muss sichergestellt sein, dass sich bei Vorhandensein mehrerer Geräte in einem Objekt zu einem Zeitpunkt immer nur ein Benutzer in Bedienebene 2 befinden kann.

Das Merkblatt entstand durch die Mitglieder des ad hoc Arbeitskreis APP im Fachverband Sicherheit

Claus Caspari, Bosch Sicherheitssysteme
Philip Dürringer, Bosch Sicherheitssysteme
Frank Herstix, Novar GmbH a Honeywell Company
Markus Ibba, Bosch Sicherheitssysteme
Michael Jäntsch, Siemens
Andreas Kahl, Bosch Sicherheitssysteme
Thomas Kern, Schrack Seconet
Christian Kühn, Schlentzek & Kühn
Christian Lais, Siemens
Oliver Lenz, Siemens
Lukas Linke, ZVEI
Andreas Schneckener, Hekatron

Wir danken für die inhaltliche Unterstützung und Kommentierung von Jens Wiesner, Bundesamt für Sicherheit in der Informationstechnik (BSI)

ZVEI
Die Elektroindustrie

Impressum

Merkblatt
ZVEI Merkblatt für die Interaktion mobiler Endgeräte mit Brandmelderzentralen über IP-Netze

Herausgeber:
ZVEI - Zentralverband Elektrotechnikund
Elektronikindustrie e. V.
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: 069 6302-245
Fax: 069 6302-1245
E-Mail: krapp@zvei.org
www.zvei.org

Verantwortlich:
Peter Krapp
Geschäftsführer Fachverband Sicherheit
und Arge Errichter und Planer

Februar 2014