VdS greift den Wunsch des Marktes auf

Mobile Applikationen in der Einbruchmeldetechnik

AUTOR: DIPL.-WIRTSCHAFTSJURIST (FH) SEBASTIAN BROSE

Wandel in der Übertragungstechnik als Auslöser eines Trends

Als sich abzeichnete, dass Netze wie X.31 und ISDN aussterben und das Internet/IP die Nachfolge antreten sollte, herrschte zunächst eine gewisse Skepsis. Die große Bandbreite, die IP zu Verfügung stellt, war für Sicherheitsanwendungen völlig überdimensioniert, stattdessen sah man sich mit einer stärkeren Unzuverlässigkeit von Verbindungen (z. B. Zwangstrennung) gegenüber. Auch war die Übertragungstechnik nicht mehr alleiniger „Herr der Leitung", sondern wurde Teil eines Netzes, das von unterschiedlichsten Akteuren/Systemen genutzt wird.

Nachdem aber die allermeisten Herausforderungen gemeistert waren, wurde schnell klar, welchen Zusatznutzen die Verwendung der IP-Netze bietet: Plötzlich war die EMZ bzw. ÜE rund um die Uhr online und konnte damit auch erreicht werden. Unabhängig davon fand parallel eine rasante Verbreitung von Smartphones statt, sodass sich ein neuer Trend entwickelte: Nach den Aussagen unserer Errichter und Hersteller von Einbruchmeldeanlagen ist derzeit das zentrale Verkaufsargument bei vielen Kundengesprächen die „App-ability", also die Tatsache, dass der Nutzer mittels App auf seine Einbruchmeldeanlage zugreifen und z. B. Statusanzeigen prüfen und Bedienungen vornehmen kann.

App oder Attest?

Nach bisherigem Stand der VdS-Richtlinien waren derartige Anwendungen leider unzulässig. Die Richtlinien für Einbruchmeldeanlagen – Planung und Einbau, VdS 2311 forderten für eine „Fernabfrage" u. a. die aktive Freigabe durch den Betreiber vor Ort und gestatten den Zugriff auch nur im unscharfen Zustand. Das führte dazu, dass der richtlinienkonforme Einsatz von „EMA-Apps" nicht möglich war und es zur Frage kam: „App oder Attest?" Oft entschieden sich die neuen Techniken besonders aufgeschlossenen Endkunden für die App und damit gegen eine VdS-anerkannte und attestierte EMA.

VdS hat das Problem erkannt und sich der Aufgabe gestellt, eine Lösung zu entwickeln, denn grundsätzlich sind alle – Versicherer, Errichter, Hersteller, Endkunden und VdS – davon überzeugt, dass auch VdS-Anlagen mit App möglich sein sollten. Die Frage war also „nur noch", auf welchem Sicherheitsniveau. Anders ausgedrückt: Welche Anforderungen muss eine App und die zugehörige EMA mindestens erfüllen, damit VdS die App akzeptieren kann?

Grundsatz der Richtlinien VdS 3169

Die Anforderungen und Prüfmethoden für solche „EMA-Apps" sind in den Richtlinien „Fernzugriff auf Einbruchmeldeanlagen mittels Smart Device-Applikation", VdS 3169, fixiert worden. Der Erstellung lag die Überlegung zugrunde, dass Smart Devices mit entsprechenden Applikationen zur Zustandsabfrage und Fernsteuerung von Einbruchmeldeanlagen als abgesetztes Bedienteil begriffen werden können. Da sich dieses jedoch nicht im (überwachten) Sicherungsbereich befindet, entstehen zusätzliche Angriffsflächen im Sicherheitssystem EMA.

Die neuen Richtlinien beschreiben nun Anforderungen und Prüfmethoden für Maßnahmen, um diesem Risiko zu begegnen, mögliche neue Angriffsflächen zu eliminieren und die Smartphone-Applikation auf ein vergleichbares Sicherheitsniveau zu heben, wie es bei einem abgesetzten Anzeige- und Bedienfeld im Sicherungsbereich gegeben ist. Sie gelten für Applikationen, die auf Smart Devices zum Einsatz kommen und zur Kommunikation mit VdS-anerkannten Einbruchmeldesystemen oder VdS-Home-Gefahrenwarnanlagen bestimmt sind.

Drei Grundsätze der IT-Sicherheit

Bei der Festlegung der Anforderungen an jede App spielen die drei Grundsätze der IT-Sicherheit eine wichtige Rolle: Authentizität, Integrität und Vertraulichkeit.

Die Authentizität der Daten wird sichergestellt durch ein so genanntes Pairing-Verfahren (s. u.) und die Ermittlung von Hashcodes, damit die App als solche nicht kompromittiert werden kann (nach einem erfolgten Pairing kommuniziert die EMA nur mit den konkreten Smart-Devices).

Die Integrität der Daten wird durch verschiedene Mechanismen gewährleistet: Daten werden möglichst nur in speziell geschützten Speicherbereichen abgelegt; nur die Daten werden auf dem Smartphone abgespeichert, die nicht auch aus dem Master (der EMZ) geladen werden können; durch Checksummen usw. Außerdem dürfen Anzeigen

Der Autor dieses Beitrags, ***Dipl.-Wirtschaftsjurist (FH) Sebastian Brose***, ist Mitarbeiter des Bereichs Security bei VdS Schadenverhütung.

Kontakt:
sbrose@vds.de

und Bedienfunktionen nur „live" durchgeführt werden, also während eine Verbindung zwischen Client und Master besteht.

Um die Vertraulichkeit der Daten zu wahren, muss eine AES-Verschlüsselung mit 128 Bit mit CBC (Cipher Block Chaining Mode; gleiche Inhalte sehen nicht gleich aus) eingesetzt werden, wie es auch das Protokoll VdS 2465 vorsieht. Schließlich sorgt ein Timeout dafür, dass Verbindungen abgebaut werden, die nicht aktiv genutzt werden.

Pairing-Verfahren

Um die Sicherheit der App-Anwendung in EMA zu gewährleisten, muss ein Pairing-Verfahren eingesetzt werden, mittels dessen die Authentizität sichergestellt wird. Es bietet zudem die Möglichkeit, einzelne Clients zu sperren, etwa nach Verlust oder Diebstahl. Im Master wird eine Liste der zulässigen Clients geführt, die z.B. anhand ihrer MAC-Adresse oder IMEI-Nummer identifiziert werden. Nur die dem Master (EMZ/ÜE) bekannten Clients (Apps/Smartphones) können Zugriff auf die EMA erlangen. Das erstmalige Anlegen (Initial Pairing) muss durch den Errichter erfolgen.

Greift ein Client über einen einstellbaren Zeitraum nicht auf den Master zu oder gibt er dreimal hintereinander einen falschen Nutzercode ein, wird er temporär gesperrt. Der Betreiber muss dann vor Ort den betreffenden Client wieder freischalten. Alternativ kann dies auch aus der Ferne durch Eingabe eines PUK (Personal Unblocking Key) möglich sein.

Für Applikationen, die zum ausschließlichen Einsatz mit VdS-Home-Gefahrenwarnanlagen bestimmt sind, sind die Regelungen zum Pairing optional. Es wird jedoch ausdrücklich empfohlen, auch bei VdS-Home-Gefahrenwarnanlagen ein entsprechendes Verfahren umzusetzen.

Nutzercode

Der Nutzer der App muss zum Starten derselben zunächst einen persönlichen Nutzercode („Passwort") eingeben, damit nicht jeder, der Zugriff auf das betreffenden Smartphone erlangt, auch gleichzeitig Zugriff auf die App erlangt. An den Nutzercode werden abhängig von der Klasse der EMA unterschiedliche Anforderungen gestellt (siehe Tabelle 1).

Verbindungsaufbau

Der Verbindungsaufbau geht vom Client aus und durchläuft vier Stufen, wie in Abbildung 1 dargestellt:

1. Stufe: Nutzercode
Der Client darf die Verbindung zum Master nur aufbauen, wenn ein gültiger Nutzercode zum Start der App bzw. zur Initialisierung des Verbindungsaufbaus eingegeben wurde (s.o.).

2. Stufe: Schlüsselprüfung
Der Master kann das Datentelegramm nur verstehen, wenn es mit dem richtigen Schlüssel verschlüsselt wurde. Somit wird der Schlüssel inzident geprüft.

3. Stufe: Pairing-Prüfung
Kann der Master das Datentelegramm verstehen, prüft er, ob die enthaltene Identifikationsinformation des Clients in seiner Client-Liste bekannt ist und diese dem Client aktuell den Zugriff gestattet.

4. Stufe: Codeabfrage
Wurde der Zugriff aufgrund der vorangegangenen Prüfungen gestattet, sendet der Master eine Codeabfrage an den Client. Der Nutzer gibt im Client seinen Berechtigungscode ein. Der Client sendet diesen an den Master, wo er gegen die Berechtigungsdatenbank der EMZ geprüft wird. Das Ergebnis teilt der Master dem Client mit. In Abhängigkeit der mit dem Berechtigungscode gekoppelten Ansichts- und Bedienberechtigungen stellt die App nun die entsprechenden Funktionen zur Verfügung. Wird der Code dreimal hintereinander falsch eingegeben, wird der Client auf „Re-Pairing pending" zurückgestuft: Um wieder Zugriff zu erlangen, muss ein Re-Pairing durchgeführt werden.

Berechtigungen

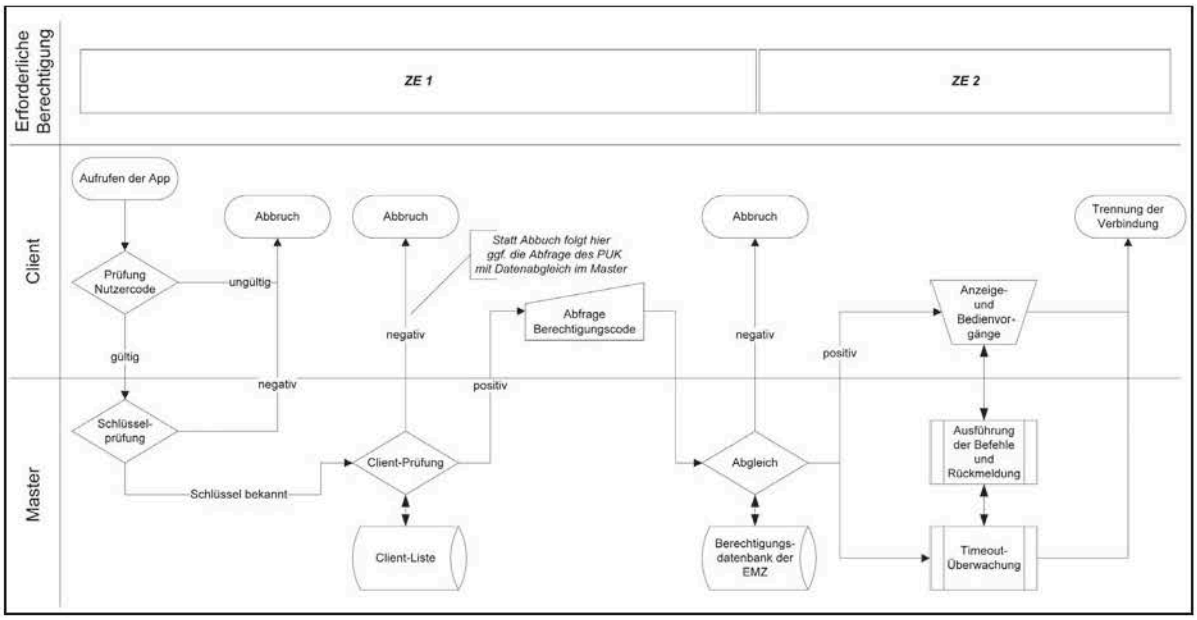
Für die App besteht grundsätzlich das gleiche Berechtigungskonzept wie für ein physisches Bedienteil im Sicherungsbereich. Die einzelnen Berechtigungen ergeben sich anhand des Codes, zu dem im Master die Berechtigungen und Beschränkungen hinterlegt sind.

Abweichend davon gilt in Einbruchmeldeanlagen der Klassen B und C, dass das Rücksetzen von Alarmen nur mit Vor-Ort-Bestätigung zulässig ist.

Tabelle 1

Klasse	Anforderung
Home	min. 4-stellig Klein- und Großbuchstaben, Ziffern
A	min. 6-stellig Klein- und Großbuchstaben, Ziffern
B	min. 8-stellig Klein- und Großbuchstaben, Ziffern Regelmäßige Aufforderung (Hinweis) zur Code-Änderung
C	min. 8-stellig Klein- und Großbuchstaben, Ziffern alle 30 Tage automatische Aufforderung (Pflicht) zum Codewechsel Alternativ kann alle 30 Tage der AES-Schlüssel automatisch gewechselt werden, entweder automatische Neuberechnung (synchron in Master + Slave) oder automatische Neu-Auswahl aus min. 255 Varianten.

Abb. 1: Der Verbindungsaufbau durchläuft vier Stufen



Ist die EMA extern scharf geschaltet, ist die Bedienung EMA-relevanter Funktionen nicht möglich. Andere Funktionen, wie etwa die Ansteuerung von Garagentoren über die EMA, sind jederzeit möglich, soweit sie rückwirkungsfrei ausgeführt sind.

Änderungen der VdS 2311

Die Richtlinien VdS 2311 enthalten in der Ergänzung VdS 2311-S1 den zusätzlichen Passus, dass Abweichungen von den Regelungen zur Fernabfrage zulässig sind, wenn eine Smart-Device-Applikation (z.B. Smartphone-App) gemäß VdS 3169 zum Einsatz kommt. Dadurch wird der richtlinienkonforme Einsatz von Apps ermöglicht und die Frage „App oder Attest?“ wird zukünftig beantwortet mit: „App und Attest!“