Am besten zentral „Ende zu Ende"

Textverschlüsselung von Alarmmeldungen

Robert Bolecek

Bei der Alarmierung von Einsatzkräften über Funknetze oder andere behördliche Kommunikationsnetze werden häufig personenbezogene Daten übermittelt. Eine Textverschlüsselung ist somit Pflicht. Worauf sollte der Anwender im Hinblick auf die Verschlüsselung achten?

Bild 1: Bei verschlüsselten Alarmierungen entschlüsselt das Endgerät die Meldungen an das Rettungspersonal vor Ort

Die seit dem 25. Mai EU-weit geltende Datenschutzgrundverordnung (EU-DGSVO) hat dem Thema „Textverschlüsselung von Alarmmeldungen" zusätzliche Dynamik verliehen.

Abhören ist eine durchaus reale Bedrohung

Unter den Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in Deutschland bestand aber auch schon vor der Diskussion um die Folgen der DGSVO Einigkeit darüber, dass eine solche Verschlüsselung sinnvoll und notwendig ist. Schließlich gehört es zu den Aufgaben der BOS, das Abhören bzw. Weiterverbreiten von Alarmmeldungen durch Unbefugte zu verhindern. Zum Beispiel sollen Einsatzort und Einsatzstichwort nur den beteiligten Einsatzkräften bekannt werden (*Bild 1*).

Besonders notwendig wird die Verschlüsselung bei Kommunikationsnetzen, in die Rettungsdienste eingebunden sind. Hier enthalten die Meldungen an die Einsatzkräfte besonders häufig personenbezogene Daten.

Ein reines Abhörverbot reicht in diesem Fall nicht aus. Das zeigt schon die Tatsache, dass solche Verbote bewusst unterlaufen werden können. In den vergangenen Jahren gab es mehrere Gerichtsverfahren wegen des unbefugten Abhörens des BOS-Funks, die allesamt mit der Verurteilung des Beschuldigten endeten.

Ende-zu-Ende-Verschlüsselung

Unabhängig von der Art des Protokolls ist die Grundstruktur der Verschlüsselung von Alarmmeldungen bei der digitalen Funkalarmierung stets identisch. Die Verschlüsselung findet in der alarmauslösenden Stelle (Leitstelle bzw. FEZ) im sogenannten digitalen Alarmgeber (DAG-Rechner), in Einzelfällen auch im Einsatzleitsystem (ELS) statt. Das Pocsag-Funknetz überträgt die Meldung verschlüsselt, und im Endgerät (Melder) wird sie wieder entschlüsselt. Diese Ende-zu-Ende-Verschlüsselung ist eine Voraussetzung für größtmögliche Sicherheit.

Für die Verschlüsselung stehen drei verschiedene Verfahren zur Verfügung: AES-128 (Advanced Encryption Standard), DiCal-IDEA (International Data Encryption Algorithm) und BOS-Krypt. Alle drei Verfahren sind lizenzfrei nutzbar und gewährleisten als Ende-zu-Ende-Verschlüsselung einen hohen Sicherheitsstandard. Jedoch wurde AES-128 nicht dezidiert für die Funkrufübertragung entwickelt, sondern als allgemeiner Standard für Internet und Kommunikation.

Robert Bolecek ist Head of Corporate Communication bei der Swissphone Wireless AG in Samstagern, Schweiz

Weitere Unterschiede gibt es unter anderem bei der maximalen Klartextlänge. Sie ist bei BOSKrypt auf 180 Zeichen beschränkt, bei DiCal-IDEA hingegen wurde auf eine Begrenzung der Klartextlänge verzichtet. Außerdem zeichnet sich DiCal-IDEA durch den mit Abstand geringsten „Overhead“ aus, so dass nur wenig Ressourcen des Alarmierungsnetzes benötigt werden und das Netz schnell wieder für den nächsten Alarm bereit ist. Zudem unterscheiden sich die Verfahren in der Empfangswahrscheinlichkeit der Nachrichten. Im Falle von BOSKrypt müssen deutlich mehr Daten fehlerfrei empfangen werden, damit die Meldung angezeigt wird. Dies wirkt sich speziell bei Funkübertragungen sehr negativ aus.
Die Marktanteile der drei Verfahren sind mehr als deutlich verteilt. Allein in Deutschland nutzen mehr als hundert Alarmierungsfunknetze mit mehreren hunderttausend Endgeräten die DiCal-IDEA-Verschlüsselung mit 128 bit (*Bild 2*). Damit ist dieses Verfahren das bei weitem gebräuchlichste. Bei AES-128 liegt der Marktanteil im einstelligen Prozentbereich, und bei BOSKrypt gibt es nach Schätzungen von Swissphone bislang wenige tausend Endgeräte, die mit dieser Verschlüsselung arbeiten. Somit kann DiCal-IDEA als De-facto-Standard bei den deutschen BOS gelten.

Interoperabilität?

BOSKrypt verspricht, Melder mehrerer Hersteller mit einem Verschlüsselungs-verfahren betreiben zu können. Auf der Ebene der reinen Verschlüsselung trifft dies zu. Aufgrund herstellerabhängiger Zusatzfunktionen gibt es aber Einschränkungen in Bezug auf das Sperren von Meldern, auf die Zeichenlänge, auf das Setzen der Zeit sowie den Einsatz des von Swissphone patentierten Verfahrens ExpressAlarm. Das bedeutet, dass Betreiber eines Netzes mit dem BOSKrypt-Verschlüsselungsverfahren diese Funktionen nur eingeschränkt nutzen können. Handelt es sich um ein herstellerproprietäres Verfahren, sind sie gewährleistet.

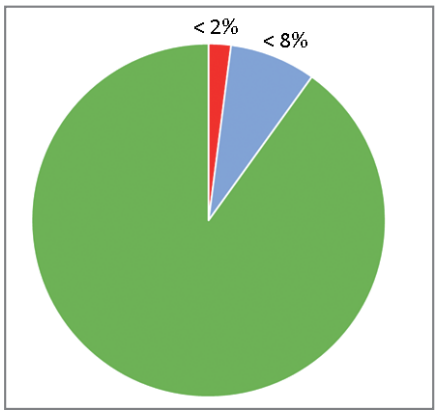

Bild 2: Marktanteile (Schätzung) der drei Verschlüsselungsverfahren für digitale Alarmierungsnetze in Deutschland
rot – BOSKrypt, blau – AES-128, grün – IDEA

Zentrale Steuerung der Endgeräte

Zum hohen Sicherheitsniveau des von Swissphone entwickelten Alarmierungssystems gehört außerdem, dass sich über eine zentrale Software alle Melder uneingeschränkt steuern lassen. Damit hat der Administrator in der jeweiligen Leitstelle die Möglichkeit, Endgeräte zu sperren, deren Zeit zu stellen oder den Schlüssel zu wechseln. Dies erfolgt jeweils über die Luftschnittstelle des Netzes.

Ein Ansprechpartner bei Unklarheiten?

Institutionen, die die Einführung einer Verschlüsselung planen, sollten aus Sicht von Swissphone ihre Alarmierungslösung ganzheitlich betrachten, da nicht die Wahl eines bestimmten Verfahrens die Ende-zu-Ende-Verschlüsselung ausmacht, sondern der sinnvolle Einbezug aller Komponenten der Alarmierungskette. Aus Sicht von Swissphone empfiehlt sich deshalb die Wahl eines Generalunternehmers, der das gesamte System, das heißt DAG-Rechner, Endgeräte sowie Verwaltungssoftware, aus einer Hand liefert. Damit kann einerseits die Kompatibilität aller Netzkomponenten im Hinblick auf eine reibungslose Umsetzung vorausgesetzt und sichergestellt werden. Andererseits steht dem Betreiber ein alleiniger Ansprechpartner zur Verfügung, sollte es tatsächlich einmal zu Fehlern oder Nichtalarmierungen kommen.

Sicherheit im Gesamtsystem

Ein weiteres Sicherheitsmerkmal, auf das der Anwender bei der Gesamtkonzeption achten sollte, ist die Sicherheit der Schlüssel-Files, die die Grundlage für die Entschlüsselung der personendatenbezogenen Nachrichten auf dem Endgerät sind. Die Alarmsysteme von Swissphone organisieren das Schlüssel-Handling so, dass die entsprechenden Files selbst auch verschlüsselt sind. Nur die Systemkomponenten DAG-Rechner, Programmiersoftware und – neu – die Fernprogrammierung können diese Files einlesen und entschlüsseln. Dabei werden die Schlüssel nie im Klartext dargestellt, um sicherzustellen, dass die Schlüssel nicht lesbar werden, wenn sie in falsche Hände kommen.
Dies funktioniert unabhängig davon, ob ein Schlüssel pro Organisation oder einer pro Rufnummer vergeben wird, mit entsprechenden Konsequenzen für die Verschlüsselungskonzepte. Entweder werden in allen Meldern dieselben Schlüssel-Files programmiert. Swissphone-Melder z.B. können bis zu 32 Schlüssel speichern. Diese vordefinierten Schlüssel können dynamisch über die Luftschnittstelle gewechselt werden – pro Einzel- oder pro Gruppenruf. Dieser Ansatz verlangt minimalen Verwaltungs- und Programmieraufwand und wird deshalb von den meisten Betreibern bevorzugt.
Der zweite Ansatz beinhaltet individuelle Schlüssel pro Rufnummer, wobei bei Verlust der Integrität eines Schlüssels nur dieser neu vergeben werden muss. Dieses Konzept hat dann Vorteile, wenn man häufig mit Einzelrufen arbeitet. Jedoch bedarf dieser Ansatz eines ständigen Abgleichs zwischen Programmierzustand der Melder und der digitalen Alarmgeber. Bei gemeinsam genutzten Adressen wie Gruppenrufen müssen alle Melder mit diesem Gruppenruf umprogrammiert werden. Zur dezentralen Verwaltung und zentralen Ablage von Einzel- und Gruppenrufen stellt Swissphone deshalb neuerdings eine Fernprogrammierungslösung zur Verfügung.

Alarmierungssystem im Saarland aus einer Hand

Das Saarland setzt Swissphone Melder mit Rückkanal und DiCal-IDEA-Verschlüsselung ein. Rainer Buchmann, Leiter der integrierten Leitstelle des Saarlandes: „Seit wir den Schlüssel eingeführt haben, läuft er tadellos. Und falls Probleme auftreten sollten, haben wir einen konkreten Ansprechpartner.“ Als Vorteil wird auch die Packungsdichte der Meldungen angesehen: „Unser Netz ist recht belegt. Da ist es wichtig, dass wir ein System mit geringem Overhead einsetzen. Damit halten wir die Übertragungszeit kurz und, als Konsequenz, die Netz-Performance hoch.“

Rainer Buchmann macht noch einen anderen Aspekt auf, der mit einer Lösung aus einer Hand einherkommt: „Die Markenbindung bezieht sich nicht nur auf die Verschlüsselung. Spätestens wenn man weitere Funktionen wie Rückmeldung oder zusätzliche Erreichbarkeit außerhalb des GSM-Versorgungsbereichs einführen möchte, muss der Betreiber sich ohnehin wieder auf einen Hersteller festlegen. Oder die zentralen Komponenten mehrfach vorhalten, was sehr teuer werden dürfte. So sind wir im Saarland zum Beispiel gerade dabei, ein System zur Eingabe der Programmierdaten für die DME auf einem zentralen Server mit dezentralen Programmstationen in den Kommunen zu entwickeln und einzuführen. Müssten wir das für mehrere Hersteller realisieren, würden sich die Kosten vervielfältigen und wären nicht mehr finanzierbar. Auch eine Vielzahl von Herstellern kann zur Kostenfalle werden.“

Kann man vorhandene Netze verschlüsseln?

BOS mit bislang noch unverschlüsselten Alarmmeldungen werden sich fragen, wie hoch der Investitionsaufwand für die Verschlüsselung ist. Aus Sicht von Swissphone ist der Aufwand überschaubar, weil sich vorhandene Endgeräte über verschiedene Modellgenerationen hinweg (ab Modellreihe BOSS 920) in verschlüsselte Netze einbinden lassen, unabhängig davon, ob ein Betreiber DiCal-IDEA oder ein anderes Verschlüsselungsverfahren wählt. Dabei lassen sich auch mehrere Verschlüsselungsverfahren in einem Netz gleichzeitig betreiben, z.B. wenn ein Betreiber einen gemischten Melderbestand führt.

Ein Wort zu den Kosten

Eine Verschlüsselung gibt es von keinem Hersteller umsonst, auch nicht mit „herstellerunabhängigen“ Verfahren. Die Entwicklung der Software, ihre Pflege und Weiterentwicklung verursachen Kosten, die je nach Hersteller entweder separat berechnet oder in den Endgerätepreis eingerechnet werden. Diese überschaubaren Kosten sind aus Sicht der Anwender nicht nur vertretbar, sondern gut investiert, weil sie die Verfügbarkeit und Sicherheit der gewählten Lösung gewährleistet.

So sieht es auch Rainer Buchmann, Leiter der integrierten Leitstelle des Saarlandes: „Im Vergleich zu einem möglichen Imageschaden, der in der Öffentlichkeit entsteht, wenn das Netz abgehört wird, sind die Kosten sehr moderat.“ *(bk)*