Einheitliche Textverschlüsselung im BOS-Digitalalarm

Bei Anwendung der gesetzlichen Vorgaben – vorwiegend die Datenschutzgesetze der Länder – ist eine Sicherung personenbezogener Daten unvermeidlich. Unverschlüsselt betriebene Alarmierungsnetze sind nur über die Strafandrohung durch das Abhörverbot geschützt – eine Maßnahme ohne praktische Wirkung. Das Mitschreiben unverschlüsselter Alarmierungsnetze, oft mit Weiterverteilung per E-Mail oder Smartphone App, ist durch verfügbare und einfach anwendbare PC-Software weit verbreitet. Die gesetzlichen Vorgaben und die zugehörige Einschätzung der Landesdatenschutzbeauftragten sind aber seit vielen Jahren eindeutig, z.B. §9, Abs. 2, Satz 2, Landesdatenschutzgesetz Baden-Württemberg:
„(2) …. Erforderlich sind Maßnahmen, wenn ihr Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."
Der BOSKRYPT-Standard hat die Voraussetzung geschaffen, erforderliche Maßnahmen einfach und kostengünstig zu ergreifen. Ein im Jahr 2012 gegründeter Arbeitskreis der Hersteller digitaler BOS-Alarmgeber (BOS-DA) hat den BOSKRYPT-Standard im Januar 2016 verabschiedet. Es ist gelungen, ein offenes und kostenfreies Verfahren zur Anwendung bei der digitalen Alarmierung nach RPC1-Standard (Pocsag) zu definieren. Mit BOSKRYPT steht für die Anwender eine Alternative bereit, die den bisherigen Flickenteppich nicht kompatibler herstellereigener Verfahren ablösen kann.

Kryptofalle

Wenn die Anwender bereits zuvor gesetzeskonform auf die datenschutzrechtlichen Entwicklungen reagiert und wenigstens die Textverschlüsselung ihres Infrastrukturherstellers für den Rettungsdienst eingeführt haben, so sind sie in die „Kryptofalle" gegangen. Bei Nach- und Neubeschaffungen konnten sie kompatible Komponenten nur noch unter Ausschaltung des Wettbewerbs beziehen. Es ist aber gerade der Wettbewerb, der in der Regel zu Preissenkungen führt.

Dem Arbeitskreis, der BOSKRYPT entwickelt hat, gehören insgesamt 21 Unternehmen und Anwenderorganisationen an. Aufseiten der Unternehmen engagieren sich dort auch PMeV-Mitglieder (Foto: Istockphoto, Arisha Ray)

Leistungsmerkmale und Funktion der Technik

Unter www.boskrypt.de stehen alle relevanten Dokumente zur Verfügung: Neben der Spezifikation sind auch viele Hinweise zur praktischen Nutzung dort eingestellt. Bei der Verschlüsselung der Meldetexte kommen grundsätzlich zwei Stellen in Frage: Der digitale Alarmgeber nach Technischer Richtlinie (TR BOS DAG) oder das in den meisten Leitstellen eingesetzte Einsatzleitsystem (ELS). Die Nachrüstung dieser beiden Komponenten ist schnell und einfach möglich, da nur an einer Stelle eine erweiterte Software eingesetzt werden muss. Eine Nachrüstung im ELS ermöglicht auch dann die Einführung von BOSKRYPT, wenn der DA-Hersteller noch keine Aufrüstung anbietet. Beim Interoperabilitätsprozess (IOP) testen die Hersteller ihre Produkte nach den Vorgaben im Teil 3 der BOSKRYPT-Spezifikation gegenseitig auf Funktionalität. Die Idee dazu ist von der DMR-Arbeitsgruppe übernommen worden.

BOSKRYPT

Aktueller Sachstand

Die ersten Ausschreibungen, die BOSKRYPT verbindlich fordern, sind bereits erfolgt. Weitere sind in Planung. Es gibt auch Anwender, die bereits mehrere tausend digitale Meldeempfänger (DME) mit BOSKRYPT betreiben. Die meisten Hersteller des Arbeitskreises bieten bereits Komponenten an. Der Standard wird von Anwendern und Herstellern gut angenommen. Daher ist eine positive Marktentwicklung für BOSKRYPT in den nächsten Jahren zu erwarten.
Alle bisher realisierten Ausführungen basieren auf der Nachrüstung des DAG. Dies ist vermutlich den jahrelangen Betriebszeiträumen der DA-Technik geschuldet. Für die Ausführung durch das ELS bestand noch kein Bedarf, obwohl die ELS-Hersteller dazu bereit wären. Im Bereich der digitalen Sirenensteuerempfänger wird voraussichtlich noch 2017 das erste Produkt angeboten. Es erfüllt moderne Anforderungen wie Wiedereinspeise- und Passwortschutz.

Der Weg zu BOSKRYPT

Die Einführung von BOSKRYPT gestaltet sich am einfachsten bei erstmaliger Beschaffung der digitalen Alarmierung. Anwender, die kostengünstig zu BOSKRYPT migrieren wollen, können dies aber auch im Zuge von Ersatzbeschaffungen über Jahre hinweg durchführen. Dabei ist mit keinen oder sehr geringen zusätzlichen Kosten zu rechnen. Größerer Aufwand und damit die höchsten Kosten entstehen, wenn in kurzen Zeiträumen viele Endgeräte nachgerüstet werden sollen. Dies liegt hauptsächlich am Arbeitsaufwand. Deshalb sollten auf keinen Fall Endgeräte umgerüstet werden, die in kleinen Chargen für ein Hard- oder Softwareupdate zum Hersteller gesendet werden müssen.
Anwender, die für Beschaffungen Bedarf an Ausschreibungstexten haben, erhalten auf www.boskrypt.de weitere Informationen. Hier finden sich auch Musterdateien des offiziellen BOSKRYPT-Logos.

Dipl.-Ing. Dirk Barthelmes