08 Kryptographie (Verschlüsselung)

Mit Hilfe kryptographischer Verfahren, wie die Verschlüsselung, sollen Daten vor unbefugtem Zugriff geschützt und sicher ausgetauscht werden. Diese Möglichkeit bietet jeder Hersteller von DMR-Geräten in seiner Gerätekonfiguration.

Uns ist in der DLRG die Kommunikation aller DLRG-Einheiten untereinander, und damit die Einhaltung der Grundsätze des digitalen DLRG-Betriebsfunks (siehe auch **Ach, Umstellung?! Warum überhaupt?**) gesamtverbandlich gesehen, sehr wichtig. Ein besonderes Merkmal, das keine andere Hilfsorganisation aufweisen kann.

Für die Verschlüsselungsoption "Advanced" nutzen DMR-Funkgeräte entweder eine 128-Bit-Verschlüsselung oder den Standard AES (Advanced Encryption Standard) mit 256-Bit. AES 256 zählt allgemein zu den sicheren Verschlüsselungsoptionen - leider ist aber eine herstellerübergreifende Kompatibilität im DMR nicht gegeben.

Würden wir also unseren Funkverkehr mittels eines AES-Schlüssels verschlüsseln, so müssten wir zur Sicherstellung, dass niemand Kenntnis über diesen Schlüssel erhält - und nur dann ist eine Verschlüsselung dauerhaft wirksam - eine zentrale Programmierung sicherstellen und den Zugriff auf die Gerätekonfiguration für wirklich alle Anderen geeignet unterbinden. Auf jedem DLRG-Betriebsfunkgerät müsste der identische Schlüssel programmiert werden, damit wir alle miteinander kommunizieren können. Dies würde uns in der DLRG massiv einschränken und einen erheblichen zeitlichen und finanziellen extra-Aufwand bedeuten, da jede Anpassung an der Programmierung nur durch die zentrale Programmierstelle erfolgen könnte.

Würden wir dagegen den Schlüssel an alle Gliederungen herausgeben, damit diese ihn selbst programmieren oder auch ihrem lokalen Funkhändler zur Programmierung übergeben könnten, wäre es leider nur eine Frage der Zeit - und das ist nicht böse gemeint - bis der Schlüssel auch außerhalb der DLRG bekannt werden würde - was nützt also ein Schlüssel, wenn er eh relativ schnell öffentlich bekannt werden würde? Genau - gar nichts!

Daher wird es im gesamten DLRG-Betriebsfunk keine Verschlüsselung des Funkverkehrs geben!

Einzige Ausnahme stellt der OTAP-Schlüssel (Over The Air Programming) dar. Dieser sollte lokal gesetzt werden, damit eine (unberechtigte) Programmierung bzw. Parameteränderung über die Luftschnittstelle nicht erfolgen kann. Wird dieses Feature nicht genutzt, sollte es grundsätzlich im Gerät deaktiviert werden, wenn das Gerät OTAP grundsätzlich unterstützt.