Welche Schlüssellänge ist sinnvoll?

Über sinnvolle Schlüssellängen und deren entsprechende Gültigkeitsdauer gibt es unterschiedliche Meinungen. So wird z.B. von RFC4641 (DNSSEC Operational Practices) eine Schlüssellänge zwischen 1024 und 2048 für den KSK (Gültigkeit: 1 Jahr) vorgeschlagen und eine etwas geringere (nicht mehr als 100Bit weniger) für den ZSK (Gültigkeit: 1 Monat). Der "DNSSEC Good Practices Guide" gibt eine KSK-Schlüssellänge von 1280Bit mit einer Gültigkeit von maximal 4 Jahren und eine ZSK-Schlüssellänge von 1024Bit mit einer Gültigkeit von maximal einem Monat als empfehlenswert an.

Beim ZSK sollte bzgl. der Schlüssellänge auch in Betracht gezogen werden, dass die daraus resultierenden Länge der UDP-Pakete momentan eine Größe von 512 Byte nicht überschreiten sollten, da nicht jede aktuelle Hardware mit EDNS0 (RFC2671) umgehen kann.

Weitere Informationen:

- RFC4641
- ENISA "DNSSEC Good Practices Guide"

Eindeutige ID: #1016
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:58