DNSSEC im Detail

Ist die Unterteilung in ZSK und KSK notwendig?

Nein, grundsätzlich nicht. Eine Zonensignierung funktioniert auch nur mit einem Schlüssel ohne weitere Unterteilung in KSK und ZSK. Allerdings entspräche das Vorgehen nicht den Empfehlungen (RFC4641 DNSSEC Operational Practices) und auch nicht dem üblichen Vorgehen. Grund für die Unterteilung ist der Wunsch nach einer längeren Gültigkeit des KSK, was eine größere Schlüssellänge notwendig macht. Eine größere Schlüssellänge erhöht allerdings die Rechenzeit bei Signierung und Validierung und vergrößert die Signaturen, die mittels des DNS Protokolls ausgetauscht werden müssen. Für UDP Pakete besteht aber ab einer gewissen Größe die Gefahr, dass sie nicht von allen momentan eingesetzten Hardwarekomponenten fehlerfrei behandelt werden.

Aus diesen Gründen ist es sinnvoll, die einzelnen DNS-Einträge der Zone mit einem kürzeren Schlüssel, dem ZSK, zu signieren und nur den ZSK selbst mit dem KSK zu unterschreiben. Eine kürzere Schlüssellänge erfordert dementsprechend einen häufigeren Schlüsselwechsel. Dies ist beim ZSK weniger problematisch als beim KSK, da bei einem ZSK-Schlüsselwechsel keine neuen Informationen in der übergeordneten Zone veröffentlicht werden müssen.

Eindeutige ID: #1014
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:57