DNSSEC im Detail

Warum ist ein regelmäßiger Wechsel der Schlüssel notwendig?

Wie bei allen Verschlüsselungsverfahren gibt es auch bei der im DNSSEC verwendeten Public-Key-Kryptografie Angriffsszenarien. Diese Angriffe benötigen abhängig von der Schlüssellänge eine meist immense Rechenleistung und dementsprechend viel Zeit und Geld um einen solchen Angriff durchzuführen. Daher stellt sich bei jeder Schlüssellänge nicht die Frage, ob ein Angriff Erfolg haben wird sondern lediglich wie lange es dauert und wieviele Ressourcen dafür aufgewendet werden müssen.

Aus diesen Gründen ist ein regelmäßiger Schlüsselwechsel sinnvoll obwohl nicht zwingend erforderlich.

Eindeutige ID: #1015
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:57