

DNSSEC im Detail

Was ist ein NSEC3-Record?

NSEC3 stellt eine Weiterentwicklung von NSEC dar, die das ungewünschte Auflisten kompletter Zonen (Zone Walking) umgeht, da die Einträge nicht mehr im Klartext sondern als Hash-Wert gelistet sind. Eine Anfrage nach einem nicht existenten Eintrag liefert den alphabetisch davorliegenden nächsten Eintrag der Zone zurück inklusive des Hashwertes des darauf folgenden Eintrags. Ist der Hashwert des angefragten Eintrags ungleich dem Hashwert im NSEC3 Record, so existiert der Eintrag nicht. Aus dem Hashwert kann aber nicht auf den alphabetisch folgenden Klartext-Eintrag geschlossen werden, was das Zone Walking verhindert.

Eindeutige ID: #1021

Verfasser: Thomas Klute

Letzte Änderung: 2010-04-29 12:44