DNSSEC im Detail

Was ist ein NSEC-Record?

Mithilfe von NSEC sind auch Negativ-Antworten (Eintrag x gibt es nicht) validierbar. Ohne NSEC könnten böswillig Teile eines DNS-Antwortpaketes gelöscht werden, so dass es für den Empfänger aussähe, als gäbe es den angefragten Eintrag nicht. NSEC verkettet die Einträge einer Zone in alphabetischer Reihenfolge. Beispiel: Sind Eintrag a und c in einem NSEC-Record verknüpft, kann es keinen Eintrag b geben.

Da die NSEC-Records ebenfalls durch RRSIG-Records signiert werden, ist eine DNSSEC-Validierung dieser Einträge und somit eine kryptografisch gesicherte Aussage über die Nichtexistenz eines Eintrags möglich.

Nachteil der NSEC-Verkettung ist die Möglichkeit, die Zoneneinträge aufzulisten (Zone Walking), da die Zoneneinträge im Klartext in den NSEC Records gelistet sind. Da dies üblicherweise nicht gewünscht ist, wurde mit NSEC3 eine Variante geschaffen, die dieses Problem umgeht.

Weitere Informationen:

- http://de.wikipedia.org/wiki/NSEC_Resource_Record

Eindeutige ID: #1020
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 12:44