DNSSEC im Detail

Welche zusätzlichen DNS Einträge gibt es?

- DNSKEY (DNSSEC Key): Dient zur Veröffentlichung des öffentlichen Teils eines DNSSEC-Schlüssels. Dies kann sowohl der Zone-Signing-Key als auch der Key-Signing-Key sein.
- RRSIG (RRSET Signature): Enthält die Signatur eines DNS Resource-Record-Sets, also einer Menge von DNS-Einträgen gleichen Typs und Namens. Die Signatur kann anhand des entsprechenden DNSKEY-Eintrags überprüft werden.
- DS (Delegation Signer): Ein von der übergeordneten Zone unterschriebener Hashwert des DNSKEY-Eintrags des Key-Signing-Keys. Dient zur Bildung einer Vertrauenskette (Chain of Trust). Der Schüsselinhaber der übergeordneten Zone signiert den Schlüssel der untergeordneten Zone. Falls der übergeordneten Zone vertraut wird, kann auch dem Schlüssel der untergeordneten Zone vertraut werden.
- NSEC/NSEC3: Ein Eintrag mit dem die in der Zone vorhandenen Einträge verkettet werden, um auch eine signierte Antwort bei Nicht-Existenz eines Eintrags zu erhalten (was sonst nicht möglich wäre). Da die Namen bei NSEC im Klartext verkettet waren, war das Auflisten aller Einträge einer Zone möglich (Zone Walking), was durch die Einführung von Hash-Werten statt Klartext durch NSEC3 behoben wurde.

Weitere Informationen:

- DNSSEC http://de.wikipedia.org/wiki/DNSSEC
- DNSKEY-RR: http://de.wikipedia.org/wiki/DNSKEY_Resource_Record
- RRSIG-RR: http://de.wikipedia.org/wiki/RRSIG_Resource_Record
- DS-RR: http://de.wikipedia.org/wiki/DS_Resource_Record
- NSEC3-RR: http://de.wikipedia.org/wiki/NSEC3

Eindeutige ID: #1012
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:54