Was ist DNSSEC?

DNSSEC (Domain Name System Security Extensions) umfasst sicherheitsbezogene Erweiterungen des DNS-Standards. Spezifiziert wird DNSSEC u.a. in folgenden RFCs:

- RFC4033
- RFC4034
- RFC4035

DNSSEC ermöglicht es, DNS-Daten (ganze Zonen und Antworten auf einzelne Anfragen) digital zu signieren. Die Signatur beruht auf Public-Key-Kryptographie, welche auf öffentlichen Schlüsseln (public key) und geheimen Schlüsseln (private key) basiert. Anhand des öffentlichen Schlüssels können solche Signaturen beim Empfänger der Daten verifiziert werden. Die jeweils übergeordneten Zonen (z.B. die zugehörige TLD-Zone oder die Root-Zone für die TLDs) können den verwendeten Schlüssel mit ihrem Schlüssel unterschreiben und auf diese Weise eine Vertrauenskette erstellen, die im Idealfall mit der Signatur der Root-Zone beginnt. Der public-Key ist öffentlich zugänglich und kann zur Verifizierung der Signatur verwendet werden. Die Signatur selbst kann nur mit Kenntnis des private-Keys erstellt werden.

DNSSEC bewirkt zwei Verbesserungen in Bezug auf die Sicherheit des DNS:

- Quellenauthentifizierung: Bei korrekter Signierung und vorhandener Vertrauenskette ist sichergestellt, dass die Quelle der DNS-Daten den geheimen Schlüssel kennt und die Daten mit diesem Schlüssel signiert wurden. Der Empfänger weiß somit, dass der Domaininhaber oder der zuständige Provider die Daten signiert haben und die Quelle vertrauenswürdig ist.
- Datenintegrität: Aufgrund der Signatur ist sichergestellt, dass die Daten auf dem Weg zwischen Quelle und Ziel nicht von Dritten manipuliert werden können.

Lediglich nach Kompromittierung des Schlüssels (Zugänglichkeit des privaten Schlüssels durch Dritte oder die mathematisch komplexe Kryptoanalyse der Daten bei der der private Schlüssel ermittelt wird) sind beide Vorteile nicht mehr gegeben. Aus diesem Grunde werden in regelmäßigen Abständen Schlüsselwechsel vollzogen.

Eindeutige ID: #1000
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:38