DNSSEC allgemein

Wie funktioniert DNSSEC?

DNSSEC fügt dem DNS weitere Arten von Einträgen (Resource-Records) hinzu, mit denen Signaturen, Schlüssel und Schlüsselverweise im DNS veröffentlicht werden können. Die Absicherung einer Zone geschieht dann durch das "Signieren" der ursprünglichen Zonendaten sowie dem Publizieren des öffentlichen Schlüssels entweder zur übergeordneten Zone oder als Eintrag in einem separaten Repository, das bei validierenden Resolvern als Vertrauensbasis hinterlegt ist. Grundsätzlich wird jeder Eintrag einer DNS-Zone mit einer entsprechenden Signatur versehen.

Stellt ein DNS-Client, der DNSSEC-Signaturen verifizieren kann (ein sogenannter "validierender Resolver") eine Anfrage an einen DNS-Server einer DNSSEC-gesicherten Zone, liefert der DNS-Server nicht nur die angefragten Informationen sondern auch deren Signatur zurück. Der validierende Resolver kann dann mit Hilfe des öffentlichen Schlüssels die Integrität der Daten und die Authentizität des DNS-Servers überprüfen.

Die verwendeten Schlüssel für die Signierung sollten regelmäßig getauscht werden, um die Sicherheit der Zone zu gewährleisten. Die Notwendigkeit eines solchen sog. Key-Rollovers ist vor allem bei kürzeren Schlüssellängen gegeben, längere Schlüssellängen sind möglich, verursachen aber größeren Rechenaufwand auf Seite der validierenden Resolver. Somit existiert ein Trade-Off zwischen Sicherheit und Rechenzeit, der durch die Unterteilung in zwei Schlüsselarten unterschiedlicher Länge entschärft wird.

Der ZSK (Zone Signing Key) hat eine kürzere Schlüssellänge und dient zum Signieren der einzelnen Zoneneinträge. Der öffentliche Teil des ZSK wird innerhalb der Zone als DNSKEY-Entry publiziert und mit dem KSK (Key Signing Key) signiert, der im Gegensatz zum ZSK eine größere Schlüssellänge besitzt. Der öffentliche Teil des KSK wird ebenfalls in der Zone als DNSKEY-Entry publiziert. Des weiteren wird für den KSK ein Hash-Wert ermittelt, der in einem DS-Record der übergeordneten Zone oder einem DLV-Repository (siehe "Was ist ein DLV?") zur Verfügung gestellt werden kann und durch den dortigen ZSK signiert wird. Auf diese Weise bildet sich eine Vertrauenskette, die im Idealfall bis zur Root-Zone reicht.

Eindeutige ID: #1007
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:47