DNSSEC im Detail

Welche Key-Rollover-Strategien gibt es bei DNSSEC?

RFC4641 ("DNSSEC Operational Practices") beschreibt zwei verschiedene Strategien:

Pre-Publish

In der Zone wird ein neuer DNSKEY bereits einige Zeit vor Benutzung veröffentlicht. Zu einem Umschaltzeitpunkt können dann die Signaturen des alten Keys durch jene des neuen Keys ersetzt werden. Anschließend kann der alten DNSKEY nach Ablauf der Caching-Wartezeit aus der Zone gelöscht werden. Dieses Verfahren bietet den Vorteil, dass nicht gleichzeitig mit mehreren Schlüsseln signiert werden muss, wodurch die Größe der Zonendaten deutlich erhöhen würde. Zudem ist dieses Verfahren besser für Notfall-Schlüsselwechsel geeignet, da ggf. bereits ein neuer Key veröffentlicht ist, mit dem sofort signiert werden kann.

Double-Signature

In der Zone wird ein neuer DNSKEY zugleich mit der Signierung der Zone durch diesen Schlüssel veröffentlicht. Für eine gewisse Zeit muss die Zone mit beiden Schlüsseln signiert bleiben, bevor der alte Schlüssel entfernt werden kann. Diese Verfahren erhöht die Zonengröße, da gleichzeitig mit zwei Schlüsseln signiert werden muss. Allerdings ist der Ablauf des Verfahrens weniger komplex als das Pre-Publish-Verfahren.

Eindeutige ID: #1018
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 12:06