DNSSEC für Registrare

Wie wird eine Zone signiert?

Es gibt verschiedene Möglichkeiten eine Zone zu signieren. Grundsätzlich sollte unterschieden werden, ob die Zone auf dem Nameserver signiert wird oder im Vorhinein erzeugt, signiert und erst anschließend auf den Nameserver übertragen wird. Eine Signierung auf dem Nameserver setzt das Vorhandensein des privaten Schlüsses auf dem Nameserver voraus, was aus Sicherheitsgründen ggf. nicht erwünscht ist.

Die einfachste Lösung besteht in der Nutzung existierender Commandline-Tools, die sowohl zur Schlüsselerzeugung als auch zur Signierung eines bestehenden Zonenfiles eingesetzt werden können. Bind bringt die entsprechenden Tools (dnssec-keygen und dnssec-signzone) mit.

Eine weitere Lösung bieten DNSSEC-Libraries, die Schlüsselerzeugung und Signierung als API für bestimmte Programmiersprachen anbieten. Es existieren Libraries u.a. für Phyton, Java, Perl, C. Eine Auflistung entsprechender Tools findet sich unter http://www.dnssec.net/software . Abschließend ist es natürlich immer möglich, die Schlüsselerzeugung und/oder Zonensignierung anhand der entsprechenden RFCs in der Programmierumgebung seiner Wahl zu entwickeln. Bestimmte Anforderungen oder Gegebenheiten können eine solche Eigenentwicklung notwendig machen. In diesem Fall kommt dem Test der erzeugten Zonensignaturen auf Korrektheit und Kompatiblität eine große Bedeutung zu.

Es wird empfohlen ("Good Practices Guide for Deploying DNSSEC"), das signierende System sowie das System zur Aufbewahrung der Schlüssel vom Netz zu trennen oder zumindest durch eine Security-Lösung abzusichern. Eine Zonensignierung direkt auf den Nameservern hat zwar durchaus Vorteile, allerdings müssen dann die privaten Schlüssel auf den jeweiligen Nameservern verfügbar sein, was aus Sicherheitsgründen vermieden werden sollte.

Alle angeführten Lösungen müssen auch eine (teil-)automatisierte Lösung für den Schlüsselwechsel realisieren, dies kann in der einfachsten Form durch entsprechende Skripte erreicht werden oder indem ein dafür vorgesehenes Tool eingesetzt wird. Eine Liste der existierenden Tools findet sich unter http://www.dnssec.net/software .

Zu beachten ist des weiteren, dass bei der KSK-Rollover-Prozedur unter Einhaltung der wichtigen zeitlichen Abstände die Publizierung der DS-Records an die übergeordnete Zone oder in ein DLV-Repository erfolgen muss. Die Entfernung des bisherigen KSKs aus der Zone darf erst dann erfolgen, wenn sichergestellt ist, dass der DS-Record des neuen Schlüssels bereits publiziert ist und er sich auch bereits unter allen noch validen gecachten DS-Einträgen auf den Resolvern befindet.

Eindeutige ID: #1035
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 13:15