DNSSEC für Domaininhaber

Welche Abläufe sind zu beachten, wenn Domainverwaltung und DNS-Service von unterschiedlichen Dienstleistern betrieben werden?

Falls die Schlüssel vom Kunden selbst erzeugt werden, so muss jeder erzeugte Schlüssel zuerst dem DNS-Provider mitgeteilt werden, damit er diesen sowohl als DNSKEY-Record als auch für die Signierung der Zone verwendet. Sobald dies geschehen ist, kann der öffentliche Teil des Schlüssels bei der Registry für die entsprechende Zone veröffentlicht werden. Der alte Schlüssel und dessen Signaturen können nach Ablauf der Caching-Zeit (TTL) zuerst bei der Registry entfernt werden und anschließend aus der Zone selbst. Dieser Prozess wird für Key-Signing-Keys wahrscheinlich 1-2 mal pro Jahr anfallen - je nachdem wie lange ein KSK gültig sein soll.

Falls der DNS-Provider die Schlüssel erzeugt und verwaltet, muss der Kunde den öffentlichen Teil des KSKs über den Domainprovider bei der Registry veröffentlichen lassen bzw. alte Schlüssel dort entfernen. In diesem Fall ist sicherzustellen, dass der Prozess beim DNS-Provider in jedem Fall auf die Eintragungen wartet (entweder manuell oder per automatischem Test), bevor alte Schlüssel entfernt werden.

Eindeutige ID: #1034
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 13:13