DNSSEC für Registrare

Wann ist ein Notfall-Rollover notwendig?

Sollte sich herausstellen, dass ein Angriff auf eine Zone stattfindet, bei der offenbar korrekt signierte aber gefälschte Daten in Umlauf gebracht werden, ist von einer öffentlichen Kenntnis der verwendeten Schlüssel auszugehen. Auch wenn ein Schlüssel verwendet wurde, dessen privater Teil aus anderen Gründen öffentlich bekannt ist, muss ein sofortiger Schlüsselwechsel erfolgen. Hierbei sind allerdings - wie bei allen Rollover-Prozeduren - sowohl die zeitliche Abfolge als auch Wartezeiten für Veröffentlichung und Cache-Timeouts zu beachten. Eine vorschnelle Löschung alter Signaturen kann zu einer Nichterreichbarkeit der Zone für neue Besucher führen. Für Besucher denen bereits gefälschte DNS-Daten ausgeliefert wurden, ist die gefälschte Zone solange gültig, bis die Einträge im Cache des validierenden Resolvers ungültig geworden sind.

Ein Notfall-Keyrollover kann durch Verwendung eines "pre-publish rollover"-Verfahrens beschleunigt werden, wenn bereits ein neuer Schlüssel veröffentlicht ist aber noch nicht für die Signierung verwendet wird. Allerdings ist es denkbar, dass - je nachdem durch welche Sicherheitslücke die privaten Schlüssel bekannt geworden sind - auch der private Teil des neuen Schlüssels bereits bekannt ist.

Der sicherste Weg besteht in der Erzeugung von neuen Schlüsseln auf einem unabhängigen neuen System und der anschließenden Verwendung dieser neuen Schlüssel im Rahmen eines koordinierten Key-Rollovers.

Eindeutige ID: #1041
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 13:21