

DNSSEC für Zugangsprovider

Was passiert im Falle einer fehlerhaften DNSSEC-signierten Zone?

Ein validierender Resolver wird bei einer fehlerhaften Validierung SERVFAIL zurückliefern. Diese Antwort ist nicht DNSSEC spezifisch und kann in vielen anderen Fällen ebenfalls zurückgeliefert werden, allerdings gibt es aktuell für fehlgeschlagene DNSSEC Validierung keine sinnvollere Antwort. SERVFAIL bedeutet, dass die Anfrage aufgrund eines Serverproblems nicht beantwortet werden konnte. Jegliche Software, die diese DNS Antwort erhält, wird verstehen, dass die Namensauflösung aufgrund eines Fehlers gescheitert ist. Vor allem erhält sie keine Antwort derart: Die IP-Adresse lautet a.b.c.d, aber DNSSEC konnte nicht validiert werden. SERVFAIL stellt sicher, dass keinerlei Antwortdaten enthalten sind, wenn die Validierung fehlschlägt.

Für den Benutzer dürfte das Ergebnis in den meisten Fällen so aussehen, als ob die Domain nicht existiert, was aber im Hintergrund daran liegt, dass die Namensauflösung nicht durchgeführt werden kann. Diese strikte Art der Fehlerbehandlung ist Gegenstand von Diskussionen, allgemein wird aber SERVFAIL als sinnvolle Antwort gesehen, solange nicht im DNS Protokoll eine weitere spezifischere Fehlermeldung eingeführt wurde und flächendeckend unterstützt wird.

Einer Software, welche die Validierung selbst durchführt, ist es natürlich möglich und freigestellt, selbst darauf zu reagieren und dem Benutzer eine andersartige Fehlermeldung anzuzeigen.

Eindeutige ID: #1046

Verfasser: Thomas Klute

Letzte Änderung: 2010-04-29 13:26