DNSSEC für Registrare

Welche Debug-Möglichkeiten gibt es?

DNSSEC-Online Tests bieten eine erste Möglichkeit Fehlern auf die Spur zu kommen. So bietet http://dnscheck.iis.se/ eine detailierte Ausgabe von Testergebnisse. Allerdings werden dort die für das .de DNSSEC Testbed bereitgestellten DNSSEC .de Nameserver nicht einbezogen, so dass die Vertrauenskette nicht bis in die .de Zone fortgesetzt werden kann.

Für eine manuelle und detailierte Untersuchung bieten sich Command-Line Tools an. Dig und drill verfügen über Debug-Level-Einstellungen mit denen die DNSSEC-Auflösung und -Validierung schrittweise nachvollzogen werden kann:

- Dig:
  - http://www.isc.org
  - http://www.nlnetlabs.nl/publications/dnssec_howto/index.html#x1-560007

- Drill:
  - http://www.nlnetlabs.nl/ldns/
  - http://www.nlnetlabs.nl/publications/dnssec_howto/index.html#x1-550006

Beispiele (Dig):

Hinweis: Einige Beispiele verwenden die DNSSEC signierte Zone dnssec-faq.de unter der diese FAQ zu erreichen ist.

- Abfrage von Zoneneinträgen inkl. DNSSEC Signierung. Falls die Domain DNSSEC signiert ist, werden auch RRSIG, NSEC und DNSKEY Records ausgegeben: 'dig dnssec-faq.de. any'
- Abfrage von DS-Einträgen in der übergeordneten Zone: 'dig @a.nic.de -t DS dnssec-faq.de'
  Während des .de DNSSEC Testbeds muss an dieser Stelle ein .de Nameserver des Testbeds befragt werden:
  'dig @auth-fra.dnssec.denic.de -t DS dnssec-faq.de.'

Beispiele (Drill):

- Verfolgen der Signaturkette einer Domain bis zu einem ggf. vertrauenswürdigen Schlüssel: 'drill -DS dnssey-faq.de'
  Während des .de DNSSEC Testbeds enthalten die per DNS veröffentlichten .de Nameserver keine DS Records. Dementsprechend findet Drill bei Frage nach den DS Records für dnssec-faq.de keinen Einträge und bricht die Verfolgung ab. Drill verwendet zur Abfrage der Daten die für das Betriebssystem eingetragenen DNS Resolver. Falls diese Resolver zur Verwendung des .de DNSSEC Testbeds konfiguriert sind, ist eine Verfolgung der Signierung bis zu .de möglich.
- Verfolgen der Signaturkette in voll funktionalen DNSSEC Deployments: 'drill -DS dnssec.se'
  Drill kann in diesem Fall die Signaturen bis zu .se verfolgen. Die public keys

für .se müssten für eine vollständige Validierung explizit als vertraute Schlüssel hinterlegt werden.

- Erstellen eines trusted-Key files für drill:
  Achtung: Das format der Datei unterscheidet sich z.B. vom Format der für Bind verwendeten trusted keys. Auf exakte Einhaltung des Formats ist zu achten, da drill ansonsten angibt, keine trusted-keys in der Datei zu finden.
  Format: 'zone. IN DNSKEY 257 3 5 key', wobei keine Zeilenumbrüche erlaubt sind.
  Beispiel für .se:
  se. IN DNSKEY 257 3 5 AwEAAbaxTum9L7z1DmPiXPk0QZ2/qUM3to210Caey/ycZuvQ8Mh/dgGpwBmyZB9xZSkaCLa2Mw6pmDLrjK9hWOffq5PXRVm9RrcA/eIEBEvbQzkY5sFkWAczNAs58Oscxi+/Gd5KfuVi3lJpYgJwwa2JB4doZ00IXywcCn0VTz0Hsl/lqpA2Bqj+e+ATzA5hWyiNyHPjiYvyMCkSXTiGgFVVuG8H3N6Us8uSABuO2UoFQeQi6YikIiCbf1FfCzr4vBIRXW6MaDs8kqAAadKjLk3i39dviL/YeyGUvq9Dan9PsvkwQejKN/7J0yCr2nYXfwGGCHkcBKkagv79EaRlZigUCp8=

Eindeutige ID: #1040
Verfasser: Thomas Klute
Letzte Änderung: 2010-05-18 22:03