

Synopsis: DNSSEC-Testbed-Meeting 16. Juni 2010

Bei der dritten Veranstaltung zum DNSSEC-Testbed für Deutschland konnten mit knapp 60 Teilnehmern wieder viele Interessenten in Frankfurt begrüßt werden.

Interessenten, die nicht teilnehmen konnten, hatten die Möglichkeit, diese über einen Live-Stream zu verfolgen. Alle Informationen zum Meeting einschließlich der Live-Mitschnitte zu den Präsentationen und Diskussionen stehen unter <http://www.denic.de/domains/dnssec/projektueberblick/meeting-16-juni-2010.html> zur Verfügung.

Der Fokus der Veranstaltung lag dieses Mal stärker auf der Praxis. Neben Informationen zum aktuellen Stand des Testbeds durch die Projektleiter berichteten die Referenten über ihre Erfahrungen im Testbed und die Fortschritte. Zusätzlich präsentierten auch einige Anbieter Lösungen, die DNSSEC bereits unterstützen.

Diskussionsstoff boten unter anderem die Themen:

- Wieviel Rechenaufwand ist notwendig, um wenigstens einen Teil der Zonendaten einer NSEC3-Kette zu ermitteln?
- Wie können Validatoren gegen Validierungsfehler gehärtet werden, die auf Konfigurationsprobleme bzw. abgelaufene Signaturen zurückzuführen sind, und welche Möglichkeiten gibt es für bestimmte Domains, die Validierung manuell und zeitlich begrenzt abzuschalten?
- Welche Möglichkeiten gibt es, die Validierung einzelner Domains abzuschalten - Bind versus Unbound?
- Für welche Gerätegenerationen stellt der Fritzbox-Hersteller AVM noch eine DNSSEC-kompatible Firmware zur Verfügung?
- Wie skalieren Prozesse und Tools, wenn statt einer großen Zone sehr viele kleine Zonen zu administrieren sind – Beispiel InterNetX GmbH: Wie skaliert Online-Signierung oder Key-Rollover bei 1,5 Millionen Zonen?
- Kann es eine für alle TLDs gleiche Policy für Provider- und DNS-Operator-Wechsel geben?
- Welche Möglichkeiten gibt es für den Provider- und DNS-Operator-Wechsel – genannt wurde auch ein Verfahren, das bei der Hinterlegung einer AuthInfo für einen Transfer registryseitig ein Transferschlüsselpaar generiert und den beiden beteiligten Registraren zur Verfügung gestellt wird.?

Die Diskussion zum Thema Registrartransfer (Provider- und DNS-Operator-Wechsel) unter DNSSEC zum Ende der Veranstaltung verdeutlichte, dass es zur Einführung von DNSSEC noch der Klärung operativer und administrativer Fragen bedarf. Speziell bei Teilnehmern, die Support für Endkunden bieten, wurden potenzielle Probleme umrissen, die kritisch für eine erfolgreiche Einführung gesehen werden. In diesem Umfeld kommt der Komplexität der Prozesse und den damit verbundenen Kosten eine hohe Bedeutung zu. Angemessene Lösungen für unterschiedliche Szenarien, etwa mit und ohne Beteiligung des abgebenden Registrars zu entwickeln, nahmen die Diskutanten als Aufgabe für die zweite Hälfte des Testbeds mit. Dabei wird Kooperation unter den Registrierungsstellen groß geschrieben, sowohl um Registraren möglichst ähnliche Bedingungen zu bieten, als auch um einen möglichst breiten Erfahrungsschatz für die Lösungsansätze zur Verfügung zu haben.

Die Diskussionen können bei den Live-Mitschnitten im Detail nachverfolgt werden.

Die Präsentationen im Einzelnen:

Testbed: DNSSEC für DE - Kurz vor dem Halbzeitpiff

Marcos Sanz Grossón / Peter Koch (DENIC eG)

Das DNSSEC-Testbed für Deutschland hat inzwischen Fahrt aufgenommen und seine wichtigsten Milestones erreicht: Für produktiven DNSSEC-Traffic seit Jahresbeginn 2010 nutzbar, ist seit März auch die Provisionierung von Schlüsselmaterial möglich. In ihrem Vortrag bilanzieren die Referenten den aktuellen Stand des Testbeds und geben einen Ausblick auf die nächsten Projektetappen und -ziele.

DNSSEC - Ein Erfahrungsbericht

Florian Obser (Hostserver GmbH)

Der Internetdienstleister Hostserver GmbH, Anbieter von Hostinglösungen und Domaindelegationen für gewerbliche Anwender, ist Testbed-Teilnehmer der ersten Stunde. Nach dem Erfahrungsbericht wie DNSSEC für die am Test beteiligten Kunden aufgesetzt wurde, fühlt der Referent der Wirksamkeit von NSEC3 Resource Records auf den Zahn: Wie steht es um Zeitaufwand und Nutzen einer gezielten Unterwanderung?

DNSSEC am Leibniz-Rechenzentrum

Bernhard Schmidt (LRZ)

Seit Anfang Mai nimmt das Leibniz-Rechenzentrum München, das neben den Hochschulen der bayerischen Landeshauptstadt auch verschiedene Forschungseinrichtungen des Freistaats betreut, mit einem Haupt- und einem Backup-Resolver am DNSSEC-Testbed teil. Auch der Kunde IABG Teleport ist im Testbed. Der Vortrag vermittelt einen Querschnitt der im bisherigen Testverlauf gewonnenen Erkenntnisse und gibt einen Status zur Webschnittstelle Nixu.

DNSSEC-Einführung in „bund.de“

Thorsten Dietrich (BSI)

Als Pilot der Bundesverwaltung ist auch die Second-Level-Domain .bund.de aktiv im Testbed vertreten. Seit dem 7. April stehen deren Einträge kryptographisch signiert zur Verfügung. Die zugrunde liegenden Betriebsparameter und bisher gesammelten Erfahrungswerte wie CPU-Last und Transfervolumina werden im Vortrag ebenso beleuchtet wie die DNSSEC-Validierung im Informationsverbund Berlin-Bonn und weitere geplante Teilprojekte.

DNSSEC als Sicherheitskomponente im Heimnetzwerk der FRITZ!Box

Martin Duzy / Jan Schöllhammer (AVM GmbH)

Die Referenten, Mitarbeiter im Entwicklungsteam und technischer Produktmanager bei AVM, spannen den Bogen von den individuellen Services und Sicherheitsfeatures bis hin zur DNSSEC-Unterstützung durch die FRITZ!Box. Neben Ablauf und Umsetzung von DNSSEC in Heimnetzwerken stehen aktuelle Grenzen und ungelöste Fragestellungen im Hinblick auf Schnittstellen, Validierungsprozesse und künftige Erfordernisse an Betriebssysteme im Mittelpunkt des Vortrags.

Nachrichtlich:

DNSSEC-kompatible Firmware für den DNS Proxy wird im Sommer 2010 als Standard-Release verfügbar sein.

Ein Firmware-Upgrade für DNSSEC wird ab AVM FRITZ!Box 7170 möglich sein.

Die Unterstützung von TCP ist derzeit nicht geplant.

Es gibt derzeit keine Planung auch einen validierenden Resolver aufzusetzen – ist jedoch nicht ganz vom Tisch.

Die Signierung der Rootzone: „Anpiff“ zum Finale

Peter Koch (DENIC eG)

Beinahe zeitgleich mit dem heutigen Testbed-Meeting bei DENIC findet in den USA die erste offizielle Key Ceremony von ICANN zum erfolgreichen Abschluß der Rootzonensignierung statt, welche das Fundament für die globale Nutzung von DNSSEC bildet. Chronologie und Ablauf der einzelnen Signierungsphasen werden in einem kurzen Überblick dargestellt sowie das grundlegende Prozedere des Key-Signing-Prozesses.

Links zur KSK-Zeremonie:

<http://dns.icann.org/ksk/facilities/east-coast/>

<http://www.root-dnssec.org>

DNSSEC@Earth: Blick über den Tellerrand

Carsten Strotmann (Men & Mice)

Ein internationaler Vergleich offenbart deutliche Unterschiede in den Projektfortschritten bei der Einführung von DNSSEC sowohl bei generischen (gTLDs) als auch bei länderbezogenen (ccTLDs) Domains. Der Vortrag beleuchtet schlaglichtartig die verschiedenen Stadien der Implementierung im zeitlichen und regionalen Marktkontext und wirft auch einen Blick auf den Status von OpenDNSSEC.

Software-Unterstützung für DNSSEC

Ralf Weber (Nominum Inc.)

Ein effizientes DNSSEC-Management wird durch Tools zur Automatisierung der Zonenverwaltung wesentlich erleichtert. Der Vortrag geht auf Konfiguration und zentrale Features von Werkzeugen, die durch den Referenten mitentwickelt wurden, sowie deren Zusammenspiel mit den wesentlichen DNSSEC-Funktionalitäten ein.

DNSSEC-Erweiterungen aus Registrarsicht

Volker Janzen (InterNetX GmbH)

Welche Besonderheiten ergeben sich bei der Handhabung von DNSKEYs und EPP (Extensible Provisioning Protocol)-Autorisierungs-codes nach RFC 4310 und 5910 in verschiedenen Registries? Aus Sicht des größten DENIC-Mitgliedsunternehmens mit 2,9 Mio. verwalteten Domains und 1,5 Mio. verwalteten Zonen wird ein Anforderungskatalog an effiziente Nameserver-Software definiert und auf aktuell bestehende Probleme bei Schnittstellen sowie noch unzureichende Notstrategien hingewiesen.

Domain-Transfer unter DNSSEC

Samuel Benz (SWITCH)

Die DNSSEC-Fähigkeit von Registraren ist entscheidend für die sichere Migration signierter Domains. Der Referent beleuchtet mögliche, an den Providerwechsel unter DNSSEC geknüpfte Probleme und Lösungsansätze, bevor er auf die Methodik des von der Schweizer Registry SWITCH angewandten Modells eingeht. Die anschließende Diskussion soll die Thematik um potenzielle Szenarien für den DNS-Operator-Wechsel erweitern.