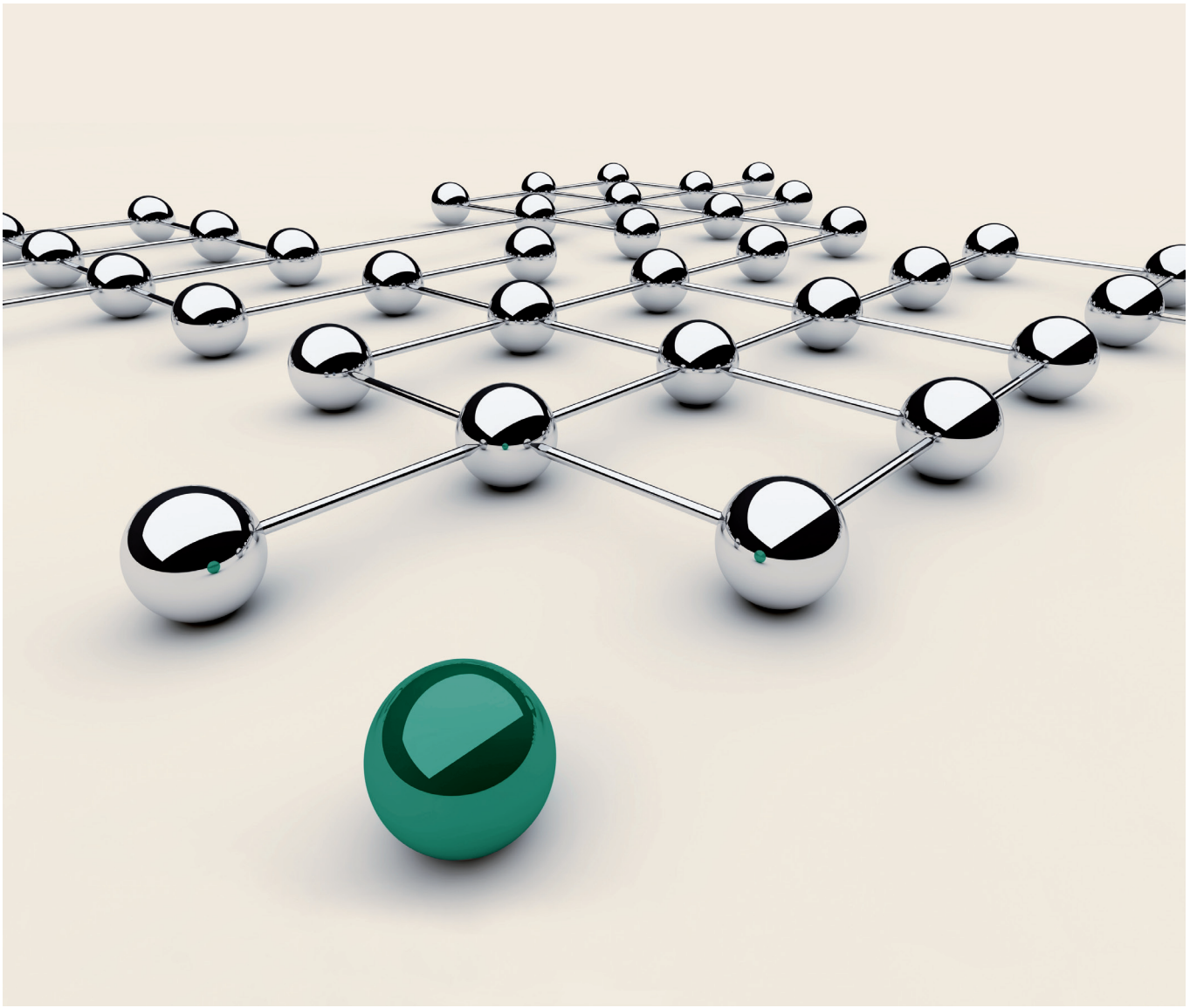
Das DNSSEC-Testbed

Abschlussbericht



Frankfurt am Main, 8. Februar 2011

Inhalt

Zusammenfassung

Domain Name Security Extensions (DNSSEC) sind ein Baustein zur Verbesserung der Sicherheit des Internets. DENIC hat am 13. Mai 2009 gemeinsam mit dem BSI und eco ein DNSSEC-Testbed ins Leben gerufen, um die Einführung von DNSSEC für .de-Domains zu evaluieren. Die DNS Protokollweiterentwicklung DNSSEC zielt darauf ab, Sicherheitslücken im Internet – wie Cache-Poisoning, DNS-Umleitungen und DNS-Spoofing - zu schließen. Innerhalb einer von DENIC bereitgestellten Testumgebung wurden operative und technische Erfahrungen gesammelt und geprüft, um zu beurteilen, welche Auswirkungen DNSSEC auf die Sicherheit und Zuverlässigkeit im deutschen Internet hat. Ziel war es, durch ausführliche Tests mögliche Risiken im Betrieb von DNSSEC frühzeitig auszuschließen und gleichzeitig dessen Akzeptanz zu prüfen. Neben einer Reihe von technischen Fragestellungen wurden zahlreiche organisatorische und wirtschaftliche Punkte detailliert untersucht. Die Beteiligung am Testbed, das vom 2. Juli 2009 bis 31. Dezember 2010 dauerte, stand Betreibern von DNS-nahen Anwendungen aber auch anderen Interessierten offen.

Maßnahmen des Testbeds waren:

- Einrichtung einer längerfristig angelegten Kooperation, damit alle an einem potentiell operativen DNSSEC Betrieb Beteiligten die Technik gemeinsam evaluieren können.
- Verabschiedung einer gemeinsamen Zielvereinbarung, in der sich alle Beteiligten zu einer aktiven Unterstützung eines DNSSEC-Testbeds bereit erklären,
- Aufbau eines Testbeds für DNSSEC für Anbieter und Nutzer des Internets in Deutschland sowie die
- Dokumentation und begleitende Beobachtung des 18-monatigen Testbeds.

Die Auswertung der erhobenen technischen und operativen Erfahrungen sowie die internationale Entwicklung haben zu der Entscheidung geführt, dass es sinnvoll ist DNSSEC auch in .de operativ einzuführen. Wichtige Meilensteine des Testbeds wie die Integration von DNSSEC in das Realtimeregistrierungssystem von DENIC sowie die Erfahrungen aus dem operativen DNS-Betriebs mit DNSSEC werden eine zügige Einführung unterstützen.

Zieltermin für die Einführung von DNSSEC in .de ist der 31. Mai 2011.

Hintergrund

Das Internet bildet heute eine zentrale Infrastruktur für das gesamte Wirtschaftsleben. Ohne die durch das Internet erbrachten Kommunikationsdienste sind viele tägliche Vorgänge sowohl im Geschäftsleben als auch im privaten Umfeld nicht mehr in der gewohnten Form möglich.

Dabei geht der Nutzer auch davon aus, dass Daten unverfälscht und unverändert im Internet übertragen werden. Es werden ständig neue Anwendungen und Verfahren im Internet eingeführt. Eine große Zahl dieser Anwendungen und Verfahren verlässt sich auf eine zuverlässig funktionierende und korrekte Auflösung von Namen auf Adressen durch das Domain Name System (DNS). Daneben gibt es eine ständig steigende Zahl von Anwendungen, die das DNS zusätzlich zum Ablegen und Abfragen weiterer Informationen nutzen. Dazu zählen unter anderem Verfahren zur SPAM-Bekämpfung und Sicherung des Mailverkehrs wie DKIM, die ihre Schlüssel im DNS ablegen, oder VoIP-Anwendungen wie Asterisk, die über ENUM aus dem DNS die Informationen zum Vermitteln von Telefongesprächen erhalten. Da bei vielen dieser Anwendungen kein Benutzer mehr an der Interaktion beteiligt ist, hat die Verlässlichkeit des DNS-Systems hierbei eine noch größere Bedeutung als beim Zugriff auf Webseiten, bei denen immer noch eine Prüfung des Inhalts durch den Anwender erfolgen kann.

Die breite Einführung von DNSSEC brächte durch die Sicherung der Datenintegrität eine Steigerung der Zuverlässigkeit im gesamten DNS. DNSSEC löst keinesfalls alle Probleme, aber schon allein die Sicherung der Übertragung zwischen DNS-Server und DNS-Resolver verringert mögliche Angriffspunkte und verbessert so die Gesamtsicherheit. DNSSEC ist aber nur eine Maßnahme zur Steigerung der Sicherheit im Internet. Deswegen sollten regelmäßig mit den betroffenen Industriekreisen etwaige alternative oder komplementäre Ansätze erörtert werden, um zu gewährleisten, dass DNSSEC tatsächlich über den Projektverlauf hinaus das Mittel der Wahl ist.

Das Domain Name System (DNS)

Das DNS ist ein verteiltes System zur Speicherung und Abfrage von Informationen im Internet. Die bekannteste Anwendung dient der Umwandlung von Namen in IP-Adressen. Neben dieser Grundfunktion wird das DNS noch zu einer Reihe anderer Abfragen genutzt, dazu zählen das Auffinden von Diensten wie Mailservern und Anmeldeservern, die flexible Abfrage von Rufnummern und den zugehörigen Servern und Diensten sowie anderes mehr. Die Verfügbarkeit und die Richtigkeit der Ergebnisse von DNS werden heute im Internet als gegeben betrachtet. Prinzipiell funktioniert das Internet auch ohne DNS, allerdings ist ein Verzicht auf Namen und Label und stattdessen die direkte Verwendung von numerischen IP-Adressen kaum vorstellbar. Ohne DNS müsste jeder Benutzer ständig IP-Adressen in seinem Browser oder in seiner Mail verwenden, was umständlich und fehleranfällig ist. IP-Adressen sind außerdem teilweise an den Provider gebunden und somit bei Serverwechsel/-umzug zwangsläufig Änderungen unterworfen. Das DNS basiert auf einer hierarchischen Serverstruktur, von der aus die Anfragen beantwortet werden. Diese Server stehen im Netz des Kunden oder beim Provider (für die lokale Zwischenspeicherung und die lokalen Netze), beim jeweiligen Anbieter von Diensten (für die Zielnetze), bei der jeweiligen Registry für Top Level Domains wie .de, .fr, .com, .net oder .org sowie auf oberster Ebene bei den Betreibern der Root-Zone.

DNSSEC

Das DNS-Protokoll selbst besitzt noch keine Maßnahmen zum Schutz seiner Inhaltsdaten, insbesondere gibt es keine Sicherung der Daten gegen Veränderungen auf dem Transportweg oder in den durchlaufenden Servern und Caches. Verfälschungen können daher weder erkannt noch verhindert werden. Unter dem Namen DNSSEC wurden aus diesem Grund von der IETF eine Reihe von Erweiterungen und Ergänzungen standardisiert. Nach anfänglicher Zurückhaltung kommt DNSSEC allmählich vermehrt, derzeit besonders durch TLD-Betreiber, zum Einsatz.

DNSSEC beschränkt sich ausschließlich auf die Quellenauthentisierung, das heißt, auf die Sicherung des Pfades zwischen DNS-Servern und validierenden DNS-Klienten, wobei auch dazwischen liegende Resolver mit ihren Caches mit in die Sicherheitskette eingeschlossen sind. Anhand der verwendeten Signatur lässt sich prüfen, ob die Daten von einer dazu berechtigten Stelle erzeugt wurden. Gleichzeitig bietet die Integritätssicherung Schutz vor Verfälschungen der Daten auf dem Transportweg. DNSSEC beinhaltet jedoch keine Aussagen bezüglich der Korrektheit der initial eingestellten Daten.

DNSSEC prüft Daten anhand von kryptografisch gesicherten Signaturen, die über die zu schützenden Daten errechnet werden und zusammen mit den Daten an den Client übertragen werden. Die Prüfung der Daten erfolgt im Client oder in dem davor liegenden Resolver gegenüber den zur jeweiligen Zone passenden öffentlichen Schlüsseln. Diese Schlüssel können ebenfalls am einfachsten wiederum im DNS hinterlegt und abgerufen werden.
Dies ist dann optimal und ohne Bruch des Sicherheitsmechanismus möglich, da auch dieser Transfer mit Hilfe von DNSSEC abgesichert erfolgt und lediglich der für den Beginn der Kette notwendige Schlüssel (der Key der Root) im Client fest hinterlegt oder per Konfiguration eingepflegt wird.

DNSSEC ist ein möglicher Baustein, um den Betrieb von DNS und damit einen Aspekt des Internets sicherer zu machen. DNSSEC schützt vor Fälschungen und dem Unterschieben falscher DNS-Daten, kann jedoch viele andere Probleme wie Domain-Hijacking, Phishing oder Manipulationen bei der Registrierung nicht verhindern. Die Vorteile von DNSSEC lassen sich auch erst dann komplett ausnutzen, wenn DNSSEC flächendeckend möglichst von jeder Hard- und Software sowie der überwiegenden Mehrheit der Resolver unterstützt wird. Bis dahin sind nur Teile nutzbar und Unsicherheiten, die durch den Bruch der Kette entstehen, zu überwinden.

Aufgabenstellung

Die Einführung eines erweiterten Authentifizierungsverfahrens berührt die Abläufe einer Vielzahl von Anspruchsgruppen:

- Betreiber von Root-Zonen
- Betreiber von Top Level Domains
- Nameserver-Betreiber
- Registrare
- Domaininhaber
- Internet Service Provider
- Software-Hersteller
- Hardware-Hersteller
- Endkunden

Ziele des DNSSEC-Testbeds waren deshalb, unter den Beteiligten ein gemeinsames Verständnis der Technologie zu fördern, Anwendungserfahrung zu sammeln und Lösungen zu erarbeiten. Themen im Einzelnen waren:

- Identifikation von Schwachstellen und Erarbeitung von Lösungen oder Lösungsansätzen,
- Identifikation technischer Probleme und deren Lösung,
- Identifikation wirtschaftlicher Probleme und Erarbeitung von Lösungsvorschlägen,
- Identifikation psychologischer und anderer Hindernisse sowie
- die Bereitstellung einer realen DNS-Umgebung, um allen Beteiligten und Interessierten Tests und Erfahrungen in einer produktionsnahen Umgebung zu ermöglichen.

Im Testbed sollte der gesamte Themenkomplex DNSSEC in Deutschland bearbeitet werden, wobei alle Dienste und Funktionen untersucht wurden, die notwendig sind, um das Internet in Deutschland zu betreiben. Insbesondere wurden dabei die Top-Level-Domain .de und der Namensbereich unterhalb der TLD betrachtet. Als zu untersuchende Bereiche wurden identifiziert:

- DNS-Root (IANA,ICANN, Root-Server-Operator, TAR-Betreiber)
- Registrierungssystem für die Top Level Domain .de (DENIC eG)
- Nameserverbetrieb für die Top Level Domain .de (DENIC eG)
- Kommunikation mit dem Registrierungssystem und den Endkunden (DENIC-Mitglieder, Registrare, Dienstleister bei Domainregistratur, DENIC),
- Betreiber von autoritativen Second Level Nameservern (DENIC-Mitglieder, Registrare, ISPs, größere Endanwender etc)
- Betreiber von Caching-Nameservern, Forwarding-Nameservern (Zugangsprovider, ISPs, größere Endanwender) und
- Betreiber von Resolvern, Zugangsroutern u.ä.. (Administratoren in Unternehmen und Endnutzer)

Neben den technischen und organisatorischen Fragestellungen sollten begleitend zum Testbed die Fragen nach den ökonomischen Auswirkungen und der Marktakzeptanz von DNSSEC beantwortet werden. Die Ergebnisse sollten – gegebenenfalls unter Einschluss von Erfahrungen im Ausland – in die weiteren Planungen eingestellt werden.

Projektablauf

Das DNSSEC-Testbed startete am 2. Juli 2009 mit einem initialen Meeting und endete offiziell am 31. Dezember 2010. In diesem Zeitraum führte DENIC insgesamt

- vier DNSSEC-Testbed-Meetings durch, die jeweils über den aktuellen Stand berichteten und die gesammelten Erfahrungen wiedergaben.
- 250 Teilnehmer besuchten diese Veranstaltungen, an denen
- 26 externe Referenten ein breites Spektrum an Vorträgen boten.

Begleitend zu den Meetings wurden DNSSEC-Hintergrundvorträge für Newcomer auf dem Gebiet angeboten. Dabei wurden immer wieder entscheidende Impulse für die Weiterentwicklung des Testbeds gegeben.

Flankierend wurden die Testbed-Konzepte und -Beobachtungen auf internationalen Branchentreffen mit einem kritischen Fachpublikum diskutiert. Diverse eingehende Medienanfragen wurden bearbeitet.

Chronologie

Im Zeitraum Juli bis Dezember 2009 wurde eine Übersicht über die in Deutschland verbreiteten Endgeräte, ADSL- und Kabelrouter und ihre DNSSEC-Eignung erstellt, die auf dem 2. DNSSEC-Testbed-Meeting am 26. Januar 2010 seitens des Testbedpartners BSI präsentiert wurde. Von den 38 getesteten Geräten waren bei Umgehung des eingebauten DNS-Proxies alle DNSSEC-kompatibel.

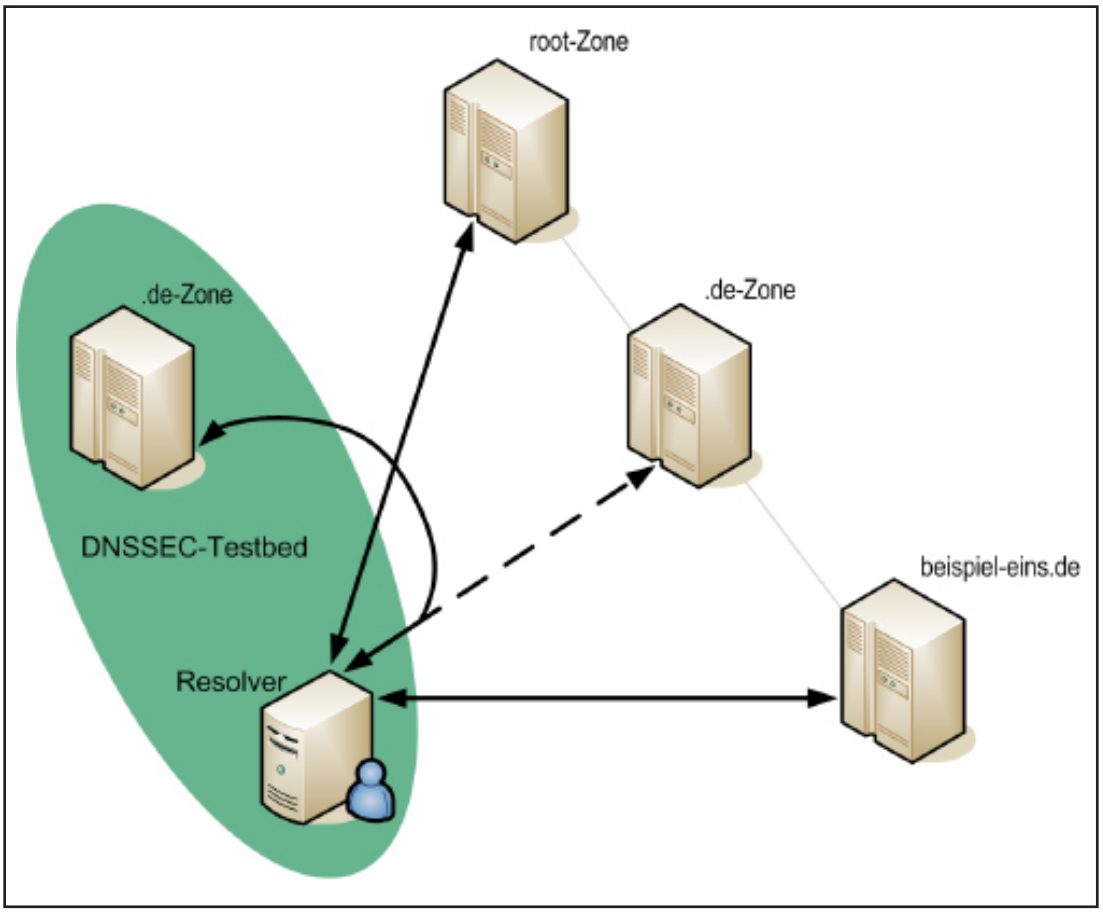
Schon vor Ende 2009 fand die Bereitstellung der parallelen Server-Struktur für .de, im ersten Schritt noch ohne DNSSEC, statt. Die beiden Nameserver-Cluster in Frankfurt auth-fra.dnssec.denic.de und Amsterdam auth-ams.dnssec.denic.de waren zunächst erst über IPv4 erreichbar. Sie beantworteten DNS-Anfragen mit DNSSEC-Daten autoritativ und nichtrekursiv.

Im Januar 2010 wurde die produktive DNSSEC-Testumgebung aufgebaut und die parallele Server-Struktur für .de mit DNSSEC zur Nutzung durch Internet Service Provider (ISPs) bereitgestellt. Die jeweils aktuelle .de-Zonenversion aus der Produktionsumgebung wurde einmal täglich signiert und in der DNSSEC-Testbedumgebung für DNS-Abfragen zur Verfügung gestellt. In einem validierenden Resolver gestattete das Set-Up, den „Trust Anchor“ für das .de-Testbed zu konfigurieren. Beim “Trust Anchor“ handelt es sich um eine Kopie des öffentlichen Teils des Key Signing Keys, der dem Resolver als „Trusted Key“ angegeben wird. Dieser „Trust Anchor“ oder „Secure Entry Point“ wurde auf einer https-gesicherten DENIC-Webseite publiziert. Neben dem 2048bit „Key Signing Key“ kam ein 1024bit „Zone Signing Key“ zum Einsatz, der fortan regelmäßig alle fünf Wochen gewechselt wurde. Beide Schlüssel erzeugten Signaturen nach dem standardisierten RSA/SHA256-Verfahren. Die Signierung der .de-Zone erfolgte mit Opt-Out unter Verwendung von NSEC3-Records.

Auf Grund der großen Menge an autoritativen Daten, die die DE- Zone enthält, war die DE-Zone im Testbed zu diesem Zeitpunkt (Januar 2010) die größte DNSSEC-TLD im Internet bezogen auf die Anzahl von signierten Domains.

Inzwischen wurde die IPv6-Erreichbarkeit des Testbeds gewährleistet und zudem ein dritter DNSSEC-Nameserver-Cluster an einem netztopologisch weit entfernten Standort (Hong Kong) in Betrieb genommen, aber nicht öffentlich gemacht, um interne Zonentransfertests durchzuführen.

Im März 2010 wurde die Testumgebung ausgebaut und die Registry/Registrar-Schnittstelle für DNS-Schlüsselmaterial erweitert. Die DENIC-Auskunftsdienste wie Domainabfrage wurden um die DNSSEC-Daten ergänzt. Ab diesem Zeitpunkt war auch für Second Level Domains unter .de die Möglichkeit gegeben, am DNSSEC-Testbed teilzunehmen und das zugehörige Schlüsselmaterial zu hinterlegen. Dabei wurden die als Trust Anchor fungierenden Key Signing Keys registriert und daraus die entsprechenden DS-Records in der im Testbed zugänglichen .de-Zone veröffentlicht. Für die betreffenden Second Level Domains erhielten die Teilnehmer am Testbed somit erstmals auch DNSSEC-gesicherte Antworten.



Seit Ende August 2010 lassen sich über das öffentliche Web-Interface für Nameserver-Checks auch die seit März 2010 für die Registrierung eingesetzten DNSSEC-spezifischen Prüfungen durchführen. Nutzer können diese gezielt zuschalten, um die technischen Parameter von DNS-KEY-Records und die Validierbarkeit der entsprechenden Signaturen zu testen. Die Aktualisierung der signierten Zone erfolgte inzwischen zwei bis drei Mal pro Tag.

Das Monitoring für den Traffic auf den DNSSEC-Name Server Locations (NSLs) wurde eingeführt. Ergänzend erfolgte die quantitative und qualitative Analyse von Faktoren wie Paketgrößen und Queryraten, die gemeinsame Bandbreiteanforderungen an NSL definieren. Der Zu- und Abgang von Domains in und aus dem Testbed wurde beobachtet, die Verwaltung der DNSKEYs analysiert und deren Eigenschaften geprüft. DNSSEC-spezifische Predelegationchecks haben die Qualität der gesicherten Delegationen verfolgt und unerwartete Phänomene wurde seitens DENIC nachgegangen. Die Ergebnisse dieser Analysen flossen kontinuierlich in die Testbed-Meetings und wurden auf der eigens eingerichteten DENIC-Projektwebseite veröffentlicht.

Aktueller Status

Das Testbed wurde offiziell zum 31. Dezember 2010 beendet. Jedoch wird die Testinfrastruktur weiter betrieben und umfasst derzeit noch 110 Domains, die von 13 Registrierungs-Accounts verwaltet werden. Darüber hinaus sind weiterhin 230 Abonnenten für die Testbed-Mailingliste registriert. Die durchschnittliche Anzahl Queries pro Sekunde beläuft sich täglich auf rund 120 Anfragen, von denen 20 bis 30 Prozent über IPv6 erfolgen. Die Zone wird derzeit zwölf Mal täglich aktualisiert, was bereits der Rate des Produktivbetriebes entspricht.

Ergebnisse

Die 12 Monate umfassende Testphase zu DNSSEC erbrachte im Einzelnen folgende Ergebnisse:

- Die Auswahl der Parameter für Schlüssel, Signaturen und NSEC3-Records erwiesen sich als produktivtauglich.
- Der durch NSEC3 angestrebte Schutz vor Zone-Walking wurde auf die Probe gestellt und im Wesentlichen bestätigt. Vgl. „Teilnahme am Testbed und Messungen zu NSEC3: Ein Erfahrungsbericht“, F. Obser (Hostserver GmbH) unter http://www.denic.de/fileadmin/public/events/DNSSEC_testbed/20100616/DNSSEC_20100616_Obser.pdf
- Die DNSSEC-spezifischen Erweiterungen des Registrierungssystems sowie der Auskunftsdienste wurden konzipiert, angepasst und dokumentiert. Der DNSKEY wurde dabei als Registrierungsobjekt gewählt. Es wurden entsprechende Mitgliederdokumentationen sowie die öffentlichen Dokumente DENIC-23p und DENIC-12p (http://www.denic.de/fileadmin/public/documentation/DENIC-12p_DE.pdf und http://www.denic.de/fileadmin/public/documentation/DENIC-23p_DE.pdf) erstellt.
- Konzeption und Implementierung eines HSM-basierten Signierungssystems mit rollenbasiertem Zugriff wurden durchgeführt.
- Ein DNSSEC Practice Statement wurde erarbeitet.
- Ein Verfahren zum Operatorwechsel unter DNSSEC wurde ausgearbeitet.
- DNSSEC-Erweiterungen an Open Source-Software wurden gesponsert.
- Ein Konzept für DNSSEC-spezifische Predelegationchecks wurde erstellt, im Testbed angewandt und als Webanwendung öffentlich zugänglich gemacht. Dabei wurde zusätzlich eine Referenzimplementierung als Open Source zur Verfügung gestellt.
- Speziell zu Schulungszwecken wurde ein Werkzeug zur Visualisierung der DNSSEC-Validierung als Webanwendung entwickelt.
- Eine eigene Projektwebseite wurde unter DENIC.de bereitgestellt.
- Neue, DNSSEC-relevante Abläufe wurden eingeführt und geübt.
- Alle DENIC-Systemkomponenten wurden auf Stabilität und Massenbetrieb getestet.
- Im Rahmen einer umfangreichen Studie wurden Zugangsrouter auf ihre DNSSEC-Tauglichkeit und -Funktionalität geprüft.. Vgl. BSI-Studie zur DNSSEC-Unterstützung durch Heimrouter unter https://www.bsi.bund.de/cae/servlet/contentblob/995592/publicationFile/63661/DNSSEC_pdf.pdf

Weitere Beobachtungen

Zudem wurde beobachtet, dass der Umfang der Zone, bedingt durch die Signaturen über autoritative Daten und NSEC3-Records um 30 Prozent wuchs. Erwartungsgemäß stieg der Bandbreitenbedarf für die DNS-Antworten im Schnitt um den Faktor 3. Der Anteil des über IPv6 eingehenden Verkehrs ist deutlich höher als in der Produktion.

Alle Ergebnisse des DNSSEC Testbeds wurden laufend in den begleitenden Meetings und auf den Testbed-Webseiten präsentiert. Dort stehen die Details auch zum Download bereit.

Fazit und weitere Schritte

Die Auswertung der erhobenen technischen und operativen Erfahrungen sowie die internationale Entwicklung haben ergeben, DNSSEC auch in .de operativ einzuführen. Wichtige Meilensteine des Testbeds wie die Integration von DNSSEC in das Realtimeregistrierungssystem von DENIC sowie die Erfahrungen aus dem operativen DNS-Betriebs mit DNSSEC werden eine zügige Einführung unterstützen. Zieltermin für die Einführung von DNSSEC in .de ist der 31. Mai 2011.

Mit dieser Einführung von DNSSEC in den Regelbetrieb bietet DENIC den Internetnutzern zusätzliche Quellenauthentisierung und es werden Sicherheitslücken wie Cache-Poisoning, DNS-Umleitungen und DNS-Spoofing geschlossen, zudem wird sichergestellt, dass eine Antwort des DNS exakt den Informationen entspricht, die der verantwortliche Zonenverwalter in das System eingepflegt hat.

Linkübersicht

Links	URL
DNSSEC-Projekt	http://www.denic.de/dnssec
Initiales Strategiepapier zum Start des DNSSEC Testbeds von BSI, DENIC und eco	http://www.denic.de/fileadmin/public/events/DNSSEC_testbed/DNSSEC_Testbed_fuer_Deutschland.pdf
1. DNSSEC-Testbed-Meeting	http://www.denic.de/domains/dnssec/veranstaltungen/meeting-2-juli-2009.html
2. DNSSEC-Testbed-Meeting	http://www.denic.de/de/domains/dnssec/veranstaltungen/meeting-26-januar-2010.html
3. DNSSEC-Testbed-Meeting	http://www.denic.de/de/domains/dnssec/veranstaltungen/meeting-16-juni-2010.html
4. DNSSEC-Testbed-Meeting	http://www.denic.de/domains/dnssec/veranstaltungen/meeting-24-november-2010.html
5. DNSSEC-Testbed-Meeting	http://www.denic.de/de/domains/dnssec/veranstaltungen/meeting-8-februar-2011.html
Name Server Tester NAST	http://nast.denic.de
DNSSEC – Interaktiver Resolver	http://www.denic.de/domains/dnssec/dnssec-vv.html
DENIC-12p Dokumentation: whois	http://www.denic.de/fileadmin/public/documentation/DENIC-12p_DE.pdf
DENIC-23p Dokumentation: Nameserver Predelation Check	http://www.denic.de/fileadmin/public/documentation/DENIC-23p_DE.pdf
Erfahrungsbericht zu NSEC3	http://www.denic.de/fileadmin/public/events/DNSSEC_testbed/20100616/DNSSEC_20100616_Obser.pdf
BSI-Studie zur DNSSEC-Unterstützung durch Heimrouter	https://www.bsi.bund.de/cae/servlet/contentblob/995592/publicationFile/63661/DNSSEC_pdf.pdf

Impressum

Herausgeber:
DENIC eG

Kaiserstraße 75-77
60329 Frankfurt am Main

ViSdP:

Sabine Dolderer
Dr. Jörg Schweiger