

DNSSEC

Überblick, Problemfelder sowie Standpunkt der nic.at

Inhaltsverzeichnis

1	Einleitung.....	3
2	DNS.....	3
2.1	Überblick.....	3
2.1.1	Verwaltung des Namensraums und autoritative Nameserver.....	4
2.1.2	Resolving Nameserver.....	5
2.2	Probleme.....	6
3	DNSSEC.....	7
3.1	Überblick.....	7
3.1.1	DNSSEC Details.....	7
3.1.2	Chain-of-Trust.....	8
3.1.3	DNSSEC im Produktionsbetrieb.....	10
3.2	Probleme.....	10
3.2.1	Root-Zone nicht signiert.....	10
3.2.2	Status der DNSSEC-Software.....	11
3.2.3	DNSSEC erfordert laufende Administration.....	11
3.2.4	Fehlertoleranz von DNS nimmt ab.....	12
3.2.5	Support Probleme.....	12
3.2.6	Problem beim Nameserverwechsel.....	12
3.2.7	DNSSEC ist inkompatibel mit bestehenden Lösungen.....	13
3.2.8	DNSSEC ist noch nicht komplett standardisiert.....	13
4	DNSSEC für .at.....	14
5	Referenzen.....	14
6	Glossar.....	15

1 Einleitung

Das DNS (Domain Name System) ist eines der wichtigsten Protokolle des Internets. DNS ermöglicht das Mapping von einfach zu merkenden Namen wie z.B. *www.nic.at* auf die jeweiligen IP-Adressen. Dies ermöglicht das Auffinden des zu einer Domain gehörenden Web-Dienstes, aber auch das Zustellen von E-Mails und Voice-over-IP Telefonaten. Aus Sicht des Benutzers ist das Nichtfunktionieren von DNS gleichbedeutend mit dem Nichtfunktionieren des Internets: er kann keine Webseiten mehr abrufen, keine Emails verschicken und seine Instant-Messaging Applikation wird auch nicht mehr funktionieren. DNS ist die Basis für allgemein bekannte Funktionalität des Internet wie Surfen, Mailing, usw.

Gelingt es einem Angreifer, falsche Informationen in das DNS einzuschleusen, so kann er z.B. Internetbenutzer auf falsche Webseiten umleiten oder fremde E-Mails abfangen. Das DNS selbst bietet zwar Sicherheitsmaßnahmen, diese sind jedoch für die heutige Zeit zu schwach und können relativ leicht ausgehebelt werden. Das Grunddesign des DNS ist über 20 Jahre alt und in den letzten Jahren wurden Erweiterungen des DNS standardisiert, um die Sicherheit zu erhöhen.

Eine der am meisten diskutierten Techniken hierfür ist DNSSEC („DNS Security Extensions“). DNSSEC soll die Sicherheit im DNS-System signifikant erhöhen, gleichzeitig steigt allerdings auch die Komplexität und damit die Anzahl der möglichen Fehlerquellen massiv an. Vor allem aber erfordert es ein Umdenken in bzw. ein Redesign der bestehender Geschäftsprozesse im Registry/Registrar/Registrant-Betrieb.

Nic.at, Betreiber der Registry für .at und kompetenter Partner für alle Fragen rund um das Domain Name System, verfolgt die Weiterentwicklung von DNS aufmerksam und testet im Labor auch neue DNS-Technologien wie DNSSEC. Dieser Artikel beschreibt die Funktionsweise von DNS/DNSSEC und beleuchtet insbesondere die Vor- und Nachteile von DNSSEC. Im Weiteren wird der Standpunkt der nic.at bezüglich der Einführung von DNSSEC in der .at Zone dargelegt.

2 DNS

2.1 Überblick

Das Grundsystem des DNS wurde 1987 mit den RFCs 1034 und 1035 standardisiert. Die Idee war, ein einfaches, flexibles Protokoll zu schaffen, welches Informationen rasch und effizient zum Benutzer bringt. Eine dafür verwendete grundlegende Eigenschaft des DNS ist das Zwischenspeichern (caching) der Information nahe beim Benutzer, um bei weiteren Anfragen nach den gleichen Informationen diese bereits vorrätig zu haben und nicht nochmals nachfragen zu müssen. Der Namenraum des DNS ist hierarchisch organisiert und wird nicht zentral verwaltet. DNS wird mittels Delegationen als verteilte Datenbank aufgebaut, wo jeder Teilbereich für sich selbst verwaltet werden kann.

Die Funktionsweise von DNS kann in zwei Bereiche unterteilt werden:

- Verwaltung des Namensraums (autoritative Nameserver)
- Abfrage der eingetragenen Namen (Resolving Nameserver)

Im Weiteren werden diese Bereiche nun getrennt betrachtet, wobei die Beschreibung in vereinfachter Form erfolgt.¹

¹ Für die genaue Funktionsweise und Definitionen siehe RFC 1034 und 1035 (<http://tools.ietf.org/html/rfc1034> bzw. <http://tools.ietf.org/html/rfc1035>).

2.1.1 Verwaltung des Namensraums und autoritative Nameserver

Der DNS Namensraum ist baumförmig. Ein Domainname wird durch Punkte in Labels getrennt, die den Knotenpunkten des Baumes entsprechen. Mehrere Labels eines Unterbaums können zu einer Zone zusammengefasst werden. Jede Zone ist auf mindestens einem autoritativen Nameserver konfiguriert (aus Redundanz bzw. Lastverteilungsgründen werden jedoch mehrere autoritative Nameserver verwendet). Ausgehend von der Wurzel (Root) verweist jeder Knotenpunkt auf die autoritativen Nameserver der DNS-Zonen unterhalb.

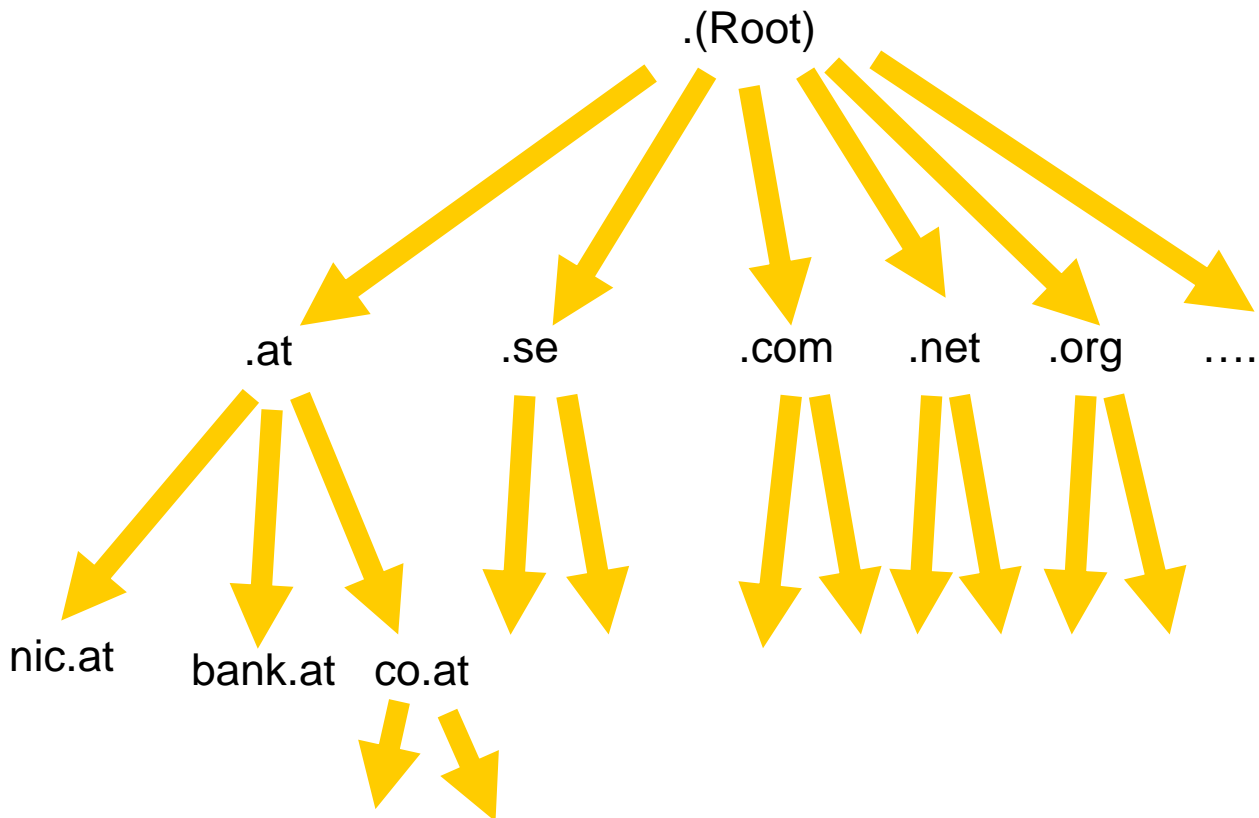


Abbildung 1: DNS-Baum

Die Auflösung bzw. Delegations von Domainnamen erfolgt von rechts nach links (das Trennzeichen für die einzelnen Ebenen ist der Punkt.).

Um z.B. den Domainnamen `www.nic.at` aufzulösen wird zuerst einer der sogenannten Root-Nameserver (diese müssen lokal konfiguriert sein) nach „`www.nic.at`“ gefragt, als Antwort erhält man die für `.at` autoritativen Nameserver. Diese werden wiederum nach „`www.nic.at`“ gefragt und als Antwort erhält man die für `nic.at` autoritativen Nameserver. Da www.nic.at in der Zone „`nic.at`“ liegt, antworten diese Nameserver auf die Frage nach „www.nic.at“ mit der IP-Adresse des zugehörigen Webservers.

2.1.2 Resolving Nameserver

Resolving Nameserver (kurz: Resolver) haben im Unterschied zu den autoritativen Nameservern keine Zonendaten konfiguriert und dienen rein zum Auflösen und meist auch dem Zwischenspeichern („cachen“) von DNS-Abfragen.

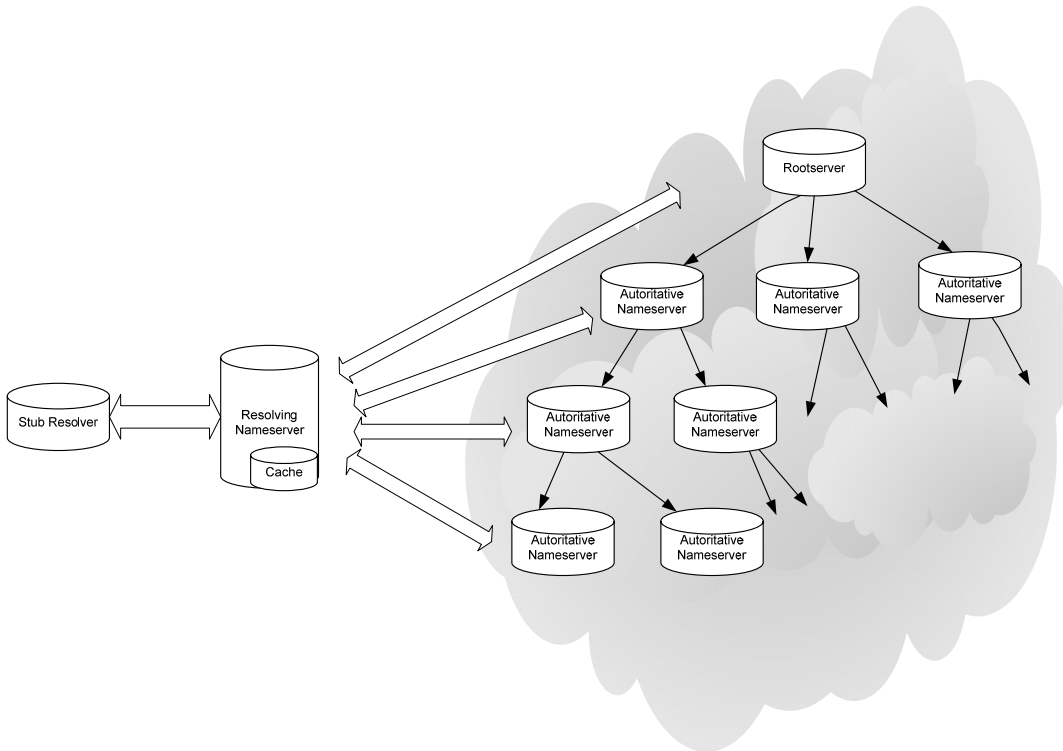


Abbildung 2: Resolving Nameserver

Jedes Betriebssystem hat üblicherweise einen sog. Stub-Resolver eingebaut, welcher die DNS-Anfragen von den lokal laufenden Programmen (z.B. Web-Browser, E-Mail Programm) annimmt und an einen (oder mehrere) konfigurierte Resolving Nameserver weiterleitet. Dieser fragt nun, an der Wurzel des DNS beginnend, iterativ die Nameserver der „Delegationskette“ ab und schickt die final erhaltene Antwort an den Stub-Resolver zurück. Mit jeder Antwort erhält der Resolving Nameserver zusätzlich eine Zeitspanne, für wie lange er die eben erhaltenen Informationen in seinen lokalen Cache aufnehmen darf. Innerhalb dieser Zeitspanne werden weitere Anfragen nach der gleichen Information sofort aus dem lokalen Cache des Resolving Nameserver beantwortet. Diese Zeitspanne nennt man Time-to-live (TTL) und kann bei der Konfiguration der autoritativen Nameserver gesetzt werden. Dieses Verhalten bietet zwei Vorteile:

1. schnellere Responsezeiten: Es muss nicht bei jeder Anfrage der gesamte DNS-Baum durchwandert werden, sondern wenn die Information bereits vorhanden ist kann die Anfrage lokal aus dem Cache beantwortet werden.
2. Minimierung der Last auf den autoritativen Nameservern: Kann die Anfrage bereits lokal beantwortet werden, müssen die autoritativen Nameserver nicht noch einmal befragt werden. Die DNS Informationen vielbesuchter Webseiten befinden sich üblicherweise in den Caches der Resolving Nameserver der Internet Zugangsprovider (ISP) und müssen z. B. bei einer TTL von einem Tag nur einmal täglich neu abgefragt werden. Auch wenn mehrere 10000 Kunden eines Providers so eine Webseite abrufen muss dafür nur ein DNS-Request zu den autoritativen Nameservern gesendet werden, alle weiteren Anfragen werden aus dem Cache beantwortet. Erst wenn die TTL abgelaufen ist und eine erneute Anfrage am Resolving Nameserver eintrifft müssen wieder die autoritativen Nameserver befragt werden.

2.2 Probleme

DNS verwendet als Transportprotokoll vorwiegend das User Datagram Protocol (UDP). UDP ist ein verbindungsloses Protokoll, d.h. es erfolgt im Gegensatz zu TCP kein dedizierter Verbindungsauf- bzw. Verbindungsabbau und es muss kein Status der Verbindungen (zu welchen Client besteht eine Verbindung, welcher Client baut gerade erst eine Verbindung auf, ...) gehalten werden, sondern die Datenübertragung beginnt sofort. Dies erhöht den Datendurchsatz, verringert die Serverlast und beschleunigt die Abfrage. Durch den fehlenden Handshake ist es allerdings leicht möglich, Datenpakete mit gefälschtem Absender zu versenden (Stichwort IP/UDP Spoofing). Weiß z. B. ein Angreifer, dass der Resolving Nameserver auf eine Antwort vom autoritativen Nameserver mit der IP-Adresse 1.2.3.4 wartet, ist es ein leichtes, ein gefälschtes UDP-Paket mit der Absender IP-Adresse 1.2.3.4 an den Resolving Nameserver zu schicken. Für den Nameserver ist nicht ersichtlich, dass die Absender IP-Adresse gefälscht ist, und nur die (nachstehend beschriebenen) Sicherheitsmassnahmen im DNS-Protokoll können nun noch verhindern, dass der Resolving Nameserver das gefälschte Paket als korrekte DNS-Antwort akzeptiert.

Die Sicherheitsmassnahmen im DNS bestehen aus einer eindeutigen, 16-bit langen Query-ID (65535 verschiedene Möglichkeiten), welche für jede Anfrage zufällig generiert wird und bei der Anfrage an den autoritativen Nameserver mitgeschickt wird. Antwortet nun der autoritative Nameserver, muss dieser in der Antwort die gleiche ID zurückschicken, anderenfalls verwirft der Resolving Nameserver die Antwort. Gelingt es nun einem Angreifer, die korrekte Query-ID zu erraten, kann er dem Resolving Nameserver falsche Daten unterschieben. Für den Resolving Nameserver ist nicht ersichtlich (wenn die Absender IP-Adresse und die Query-ID übereinstimmt), ob die Daten vom richtigen autoritativen Nameserver kommen und korrekt sind, oder ob es sich um eine gefälschte bzw. geänderte Antwort handelt. Damit wäre es für einen Angreifer z. B. möglich, einem Resolving Nameserver für www.bank.at die IP-Adresse 6.6.6.6 statt der korrekten IP-Adresse 1.2.3.4 unterzuschleusen. Dieser falsche Eintrag wird danach in den Cache des Nameservers aufgenommen (der Angreifer schickt eine möglichst lange TTL mit, damit der Eintrag auch möglichst lange im Cache bleibt) und jeder weitere Client, welcher diesen Resolving Nameserver verwendet erhält ebenfalls die falsche IP-Adresse. Dieses Verhalten nennt man Cache-Poisoning, es wird sozusagen der Cache des Resolving Nameservers mit falschen Daten vergiftet. Mittels Cache-Poisoning ist es also möglich Internetbenutzer auf falsche Webseiten umzuleiten (z.B. für Phishingattacken) oder E-Mails abzufangen.

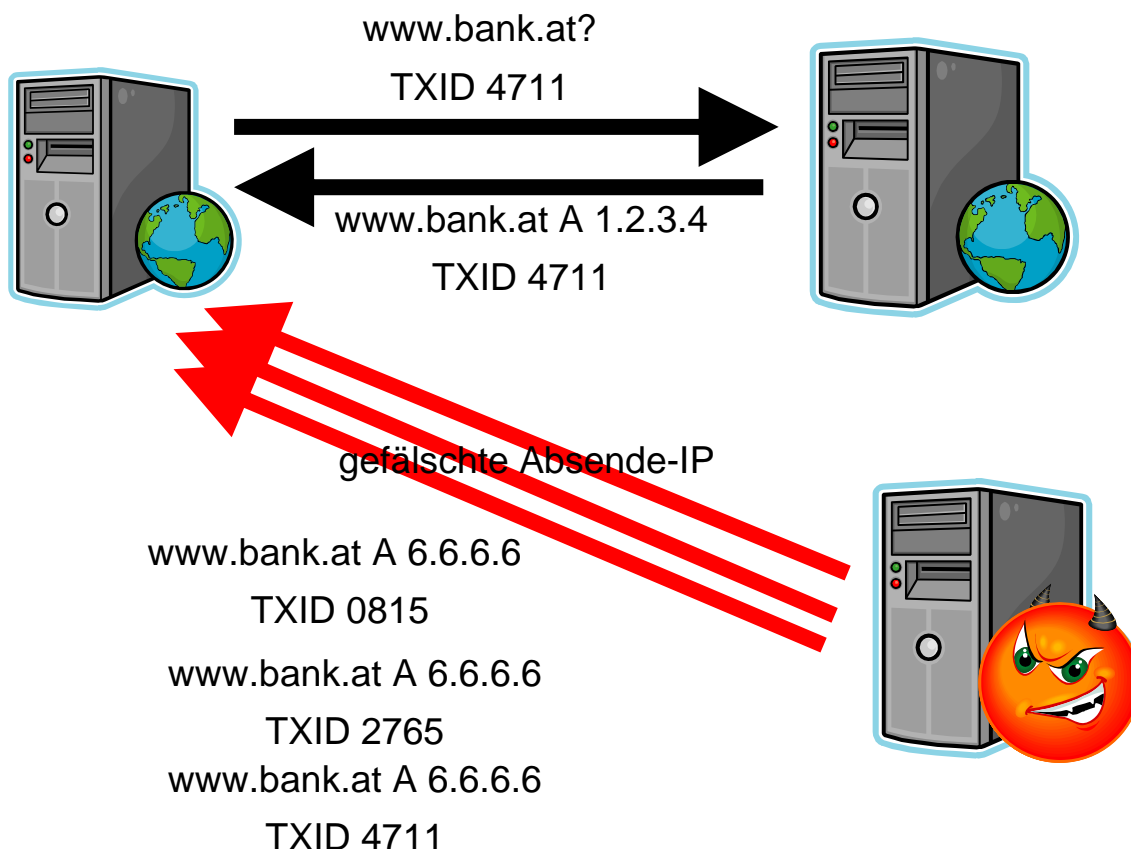


Abbildung 3: Wie funktioniert DNS-Cache-Poisoning

Als zusätzliche Sicherheitsmassnahme wird seit dem Bekanntwerden von neuen Angriffsszenarien im Sommer 2008 (sog. Kaminsky-Attacke, entdeckt von Dan Kaminsky) Port-Randomization von allen Nameserverimplementierungen verwendet (einige Nameserver wie Powerdns oder dnscache haben diese Technologie schon länger verwendet). Hier wird für jede Anfrage von einem Resolving Nameserver an einen autoritativen Nameserver ein zufällig ausgewählter UDP Source-Port gewählt. Ein Angreifer muss jetzt also zusätzlich zur IP-Adresse und der Query-ID auch noch den Port erraten, an den er die gefälschten Pakete schicken muss. Dadurch wird die Wahrscheinlichkeit, dass ein Angriff erfolgreich verläuft, deutlich minimiert.

3 DNSSEC

3.1 Überblick

Wie im vorigen Kapitel beschrieben, kann ein Resolving Nameserver die Antwort eines autoritativen Nameservers nicht überprüfen. Es kann nur die Absender IP-Adresse und die Query-ID, sowie ob die erhaltene Antwort überhaupt auf die Anfrage passt, überprüft werden – eine Validierung des Inhalts der Antwort ist nicht möglich. An diesem Punkt setzt DNSSEC an. DNSSEC fügt den DNS-Antworten eine digitale Signatur hinzu, welche mittels Public-Private-Key-Verfahren auf Empfängerseite überprüft werden kann. Damit soll sichergestellt werden, dass das DNS-Paket auch wirklich korrekte Daten enthält. Die Daten werden nur signiert, nicht verschlüsselt und werden also weiterhin im Klartext übertragen.

DNSSEC bietet nicht die „totale“ Sicherheit und löst auch nicht alle Sicherheitsprobleme des Internets. Es wird auch nach einer flächendeckenden Einführung von DNSSEC Probleme wie Spammails oder Phishingattacken geben. DNSSEC kann allerdings helfen, die Qualität anderer Techniken (welche das DNS als Weg zum Austausch von Informationen verwenden) zur Bekämpfung dieser Probleme zu heben. Z.B. verwendet DKIM (Domain Keys Identified Mail²) ein Public-Private-Key-Verfahren, um den Absender einer Email zu bestätigen. Dazu wird mit einem privaten Schlüssel eine Signatur über Bereiche der Email erstellt und der Email angefügt. Der Mailempfänger kann über den im DNS publizierten Public-Key die Signatur überprüfen und sicher sein, dass die Mail wirklich von diesem Absender kommt. Ohne DNSSEC besteht die theoretische Möglichkeit, dass ein Angreifer mittels Cache-Poisoning falsche Schlüssel in Umlauf bringt und so gefälschte, aber korrekt verifizierbare Phishingmails verschickt. DNSSEC verhindert dies und erhöht so das Vertrauen in die Technologie DKIM.

3.1.1 DNSSEC Details

Bei der Konfiguration der Zone auf den autoritativen Nameservern wird für jeden Eintrag (Record) eine digitale Signatur erstellt und der Zone als RRSIG Record hinzugefügt. Wenn nun der Resolving Nameserver einen Record abfragt, antwortet der autoritative Nameserver mit dem jeweiligen Record und zusätzlich wird der RRSIG Record mit der Signatur des angefragten Records mitgeschickt. Der Resolving Nameserver kann nun die Authentizität der Antwort durch Validierung der Signatur überprüfen.

Die Validierung der Signatur kann an mehreren Stellen passieren:

- In der Anwendung selbst
- Im Stub-Resolver der Betriebssysteme
- Im Resolving Nameserver

Erfolgt die Validierung im Resolving Nameserver hat dies den größten „Multiplier“ für die Verwendung von DNSSEC. Resolving Nameserver werden üblicherweise von einer Vielzahl an Kunden verwendet. Werden dort die Signaturen validiert, können alle Benutzer des Resolving Nameservers „sicheres“ DNS verwenden auch wenn das eigene Betriebssystem gar kein DNSSEC unterstützt.

Die oben beschriebene Validierungsmethode eignet sich zur Validierung von bestehenden Domains, jedoch nicht zur Validierung von nicht existierenden Domains bzw. DNS-Records. Da in diesem Fall kein Record zurückgeliefert wird, kann auch kein RRSIG geliefert werden. Um solche Antworten trotzdem validieren zu können wurde das NSEC Verfahren eingeführt: Dabei wird der Inhalt der Zone alphabetisch sortiert und über NSEC Records verkettet. Der letzte Name zeigt auf den ersten Namen, es entsteht eine ringförmige Kette. Die so generierten NSEC Records werden ebenfalls mit einer Signatur versehen (RRSIG Record) und dienen dem Beweis der Nicht-Existenz eines Records. Erhält ein autoritativer Nameserver eine Anfrage nach einem nicht existierenden Namen/Record liefert dieser eine negative Antwort (NXDOMAIN oder leere

² RFC 4871 - <http://tools.ietf.org/html/rfc4871>

„Answer Section“) zurück. Zusätzlich wird bei DNSSEC der Antwort noch der jeweilige NSEC Record aus der Verkettung mitgeliefert, wo der angefragte Record alphabetisch eingeordnet sein müsste. Anhand dieses Record und dessen Signatur kann der Resolving Nameserver überprüfen, ob die „leere“ Antwort des autoritativen Nameservers korrekt ist oder nicht.

Zum Beispiel eine Zone mit folgenden 3 Einträgen:

- aaaaaaa
- zzzz
- uuuuuu

Diese Einträge werden sortiert und verkettet:

aaaaaaa → uuuuuu → zzzz → aaaaaaa

Erhält der Nameserver jetzt eine Anfrage für die nicht vorhandene Domain eeeeeee wird der Record „aaaaaaa→uuuuuu“ zurückgeschickt. Somit ist es für den Client möglich zu überprüfen, dass eeeeeee (sofern vorhanden) zwischen aaaaaaa und uuuuuu eingeordnet sein müsste, dies aber nicht der Fall ist. Nachdem die Records zusätzlich mit einer Signatur versehen sind kann damit auch die Authentizität verifiziert werden.

Das oben beschriebene NSEC Verfahren (NSEC – Next Secure Record) hat den großen Nachteil, dass hier die Verknüpfung der Records im Klartext erfolgt, d. h. es ist für Externe möglich, über diese Verkettung eine Kopie der kompletten Zone rein mittels DNS-Abfrage zu generieren (sog. „Zonewalking“). Dies erzeugt nur unnötige Last auf den Nameservern und offenbart Angreifern möglicherweise sicherheitsrelevante Informationen bzw. ist es für einige Zonenbetreiber aus datenschutztechnischen Gründen nicht erwünscht, dass die Zone komplett offengelegt werden kann. Als Lösung wurde zusätzlich eine etwas geänderte Version dieser Technik standardisiert: NSEC3. Bei NSEC3 werden nicht die Klartextrecords miteinander verkettet, es wird vor der Verkettung aus jedem Record ein eindeutiger, nicht rückrechenbarer Hashwert gebildet, die Hashwerte anschließend sortiert und verknüpft.

Zum Beispiel eine Zone mit folgenden 3 Einträgen:

- aaaaaaa
- zzzz
- uuuuuu

Für die Einträge wird der Hashwert berechnet

- aaaaaaa → vfddf
- zzzz → tzjwf
- uuuuuu → aegdh

Diese Hashwerte werden jetzt sortiert und verknüpft

aegdh → tzjwf → vfddf → aegdh

Die Reihenfolge der Hashwert hat nichts mehr mit der ursprünglichen Reihenfolge zu tun.

Bei Anfragen nach einem nicht existenten Record, wird der Hashwert des angefragten Records gebildet und der jeweilig zugehörige NSEC3-Record zurückgeliefert (jene Stelle in der Kette, wo sich der Hashwert der Anfrage befinden müsste). Der Client kann nun ebenfalls den Hashwert aus seiner Anfrage bilden und prüfen, ob das Ergebnis zwischen den beiden erhaltenen Hashwerten liegt. Für einen Angreifer ist es nicht möglich von den erhaltenen Hashwerten auf den Klartext zurückzurechnen.

3.1.2 Chain-of-Trust

DNSSEC verwendet asymmetrische Kryptografie mittels öffentlichen und privaten Schlüsseln. Beim Generieren der Zone werden die Signaturen für die einzelnen RRSIG Records mit dem privaten Schlüssel der Zone erzeugt. Um auf Client-Seite die Signaturen überprüfen zu können, muss dort der zugehörigen öffentliche Schlüssel bekannt sein. Dazu werden die öffentlichen Schlüssel der Zone direkt in der Zone mittels spezieller Recordtypen (DNSKEY) publiziert. Dadurch ist es zwar technisch möglich die Signaturen zu überprüfen, allerdings stammen die Signaturen und die Schlüssel zur Überprüfung dieser aus derselben

Quelle, was den Schlüssel nicht sehr vertrauenswürdig macht. DNSSEC setzt hier auf eine Chain-of-Trust. Jede Ebene speichert und signiert (mit dem eigenen Key) die eindeutigen Fingerprints der Schlüssel der Ebene darunter. Zusätzlich zu dieser Vertrauenskette ist der Schlüssel der obersten Ebene (Root Zone) bekannt und diesem wird vertraut (der öffentliche Schlüssel der Root-Zone muss daher in den Nameservern manuell konfiguriert bzw. mitinstalliert werden).

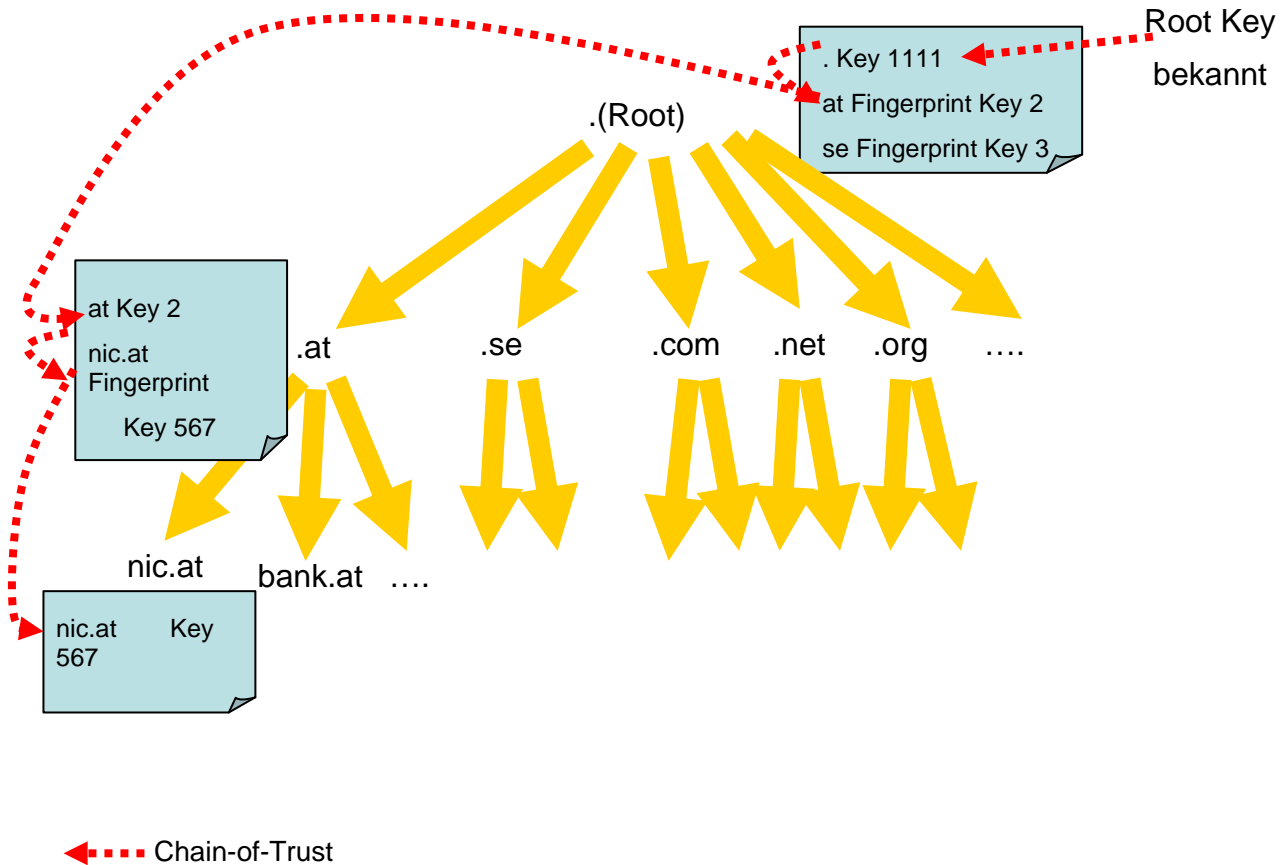


Abbildung 4: DNSSEC Chain-of-Trust

Das Konzept geht hier von einem komplett mit DNSSEC signierten DNS-Baum aus und der öffentliche Schlüssel der Root-Zone ist bekannt und diesem wird vertraut. In der signierten Root-Zone werden nun (zusätzlich zu den Delegationen) auch noch die eindeutigen Fingerprints der verwendeten Schlüssel der Zone darunter gespeichert und mit dem Root-Key signiert. Dieser Vorgang wiederholt sich nun zwischen jeder Ebene, z.B. werden in der .at Zone die Fingerprints der Schlüssel der unterhalb von .at liegenden Domains gespeichert und mit dem .at Schlüssel signiert. Ein Resolver, der z.B. eine Signatur für www.nic.at erhält, kann nun den Schlüssel der nic.at Zone abfragen und ausgehend von der Root-Zone über .at den Schlüssel der nic.at Zone verifizieren (der öffentliche Schlüssel für die Root-Zone ist im Resolver lokal konfiguriert, ähnlich wie die IP-Adressen der Root-Nameserver). Ist der Schlüssel verifiziert, so kann diesem vertraut werden und die Signatur für www.nic.at überprüft werden. Bei der Chain-of-Trust wird das Vertrauen in die Schlüssel von oben (ausgehend von Root) nach unten weitervererbt.

3.1.3 DNSSEC im Produktionsbetrieb

Obwohl sich wahrscheinlich der Großteil der weltweiten Registries mit DNSSEC beschäftigen, wird DNSSEC erst von einer Handvoll TLDs im Produktionsbetrieb verwendet. Folgende TLDs verwenden momentan (Stand 07/2009) DNSSEC:

- .bg – Bulgarien (NSEC)
- .br – Brasilien (NSEC)
- .cz – Tschechien (NSEC)
- .gov – US Government (NSEC3)
- .org – Organization gTLD (NSEC3)
- .pr – Puerto Rico (NSEC)
- .se – Schweden (NSEC)
- .th – Thailand (NSEC)

Folgende TLDs planen die Einführung von DNSSEC:

- Verisign: für alle Verisign-TLDs (.com, .net, ...) bis 2011³

3.2 Probleme

DNSSEC ist in der Theorie eine gute Lösung, um vorhandene Schwachstellen im DNS-Protokoll zu beheben und die Sicherheit bzw. Vertrauenswürdigkeit im DNS zu verbessern. Leider offenbaren sich in der Praxis (auch aufgrund der Tatsache, dass es bei laufendem Betrieb des DNS eingeführt werden muss) einige Schwächen bzw. Probleme was den Einsatz in einem so kritischen Bereich wie DNS problematisch macht. Wie bereits in der Einleitung erwähnt ist DNS ein sehr kritischer und wichtiger Dienst im Internet und selbst kurze Ausfälle sind nicht tolerierbar.

3.2.1 Root-Zone nicht signiert

Das DNSSEC-Konzept geht von einem komplett signierten DNS-Baum aus. Wichtigstes Element ist eine signierte Root-Zone, die der Ausgangspunkt für die Chain-of-Trust ist. Zurzeit ist die Root-Zone jedoch noch nicht signiert und eine (vorwiegend) politische Diskussion im Gange, wer die Root-Zone signieren soll bzw. wer den privaten Schlüssel für die Root-Zone halten soll. Derjenige hat de facto die „Macht“ über die Root-Zone. Ein Wechsel des Schlüssels zu einem anderen Betreiber ist nur schwer möglich, da die Schlüssel ja lokal in den weltweiten Resolvern konfiguriert sind und zuerst dort geändert werden müssen, da sonst die Chain-of-Trust zusammenbricht und alle DNSSEC-Anfragen als „insecure“ d. h. fehlerhaft behandelt werden und so nicht mehr auflösbar sind.

Mittlerweile gibt es (nach langen politischen Diskussionen) erste Bewegungen in dieser Sache, lt. Plan der US-Regierung soll die Root-Zone bis Ende 2009/Anfang 2010 signiert werden. Verisign soll die Schlüssel halten und die Root-Zone signieren.

Es gibt Zwischenlösungen für die nicht-signierte Root-Zone. IANA stellt ein „Interim Trust Anchor Repository“ (ITAR) bereit, welches die öffentlichen Schlüssel für die bereits signierten TLDs enthält. Die im ITAR gesammelten öffentlichen Schlüssel können auf den lokalen Resolvern konfiguriert werden. Man hat hier zwar keine globale Chain-of-Trust, erhält allerdings einzelne „Secure Islands“, welche ebenfalls die Validierung der Signaturen ermöglichen. Ein weiterer Workaround ist „DNSSEC Look-aside Validation“ (DLV). Hier werden die Schlüssel in einer extra DNS-Zone gespeichert und der Resolving Nameserver kann diese Zone nach dem benötigten Schlüssel fragen. Ist dieser dort gespeichert erhält man diesen DNSSEC-signiert zurück. Lokal muss nur noch der Schlüssel für die DLV-Zone gespeichert und gewartet werden.

³ <http://www.networkworld.com/news/2009/022409-verisign-dns-security.html>

3.2.2 Status der DNSSEC-Software

DNSSEC ist eine „relativ“ junge Technologie und die Unterstützung von DNSSEC in der verschiedenen Software ist recht unterschiedlich. Die beiden populären DNS-Server Bind und NSD unterstützen DNSSEC bereits seit längerem, nichts desto trotz gibt es bei jedem neuen Release eine Fülle von Bugfixes im DNSSEC Bereich. Jeder Protokoll-Standard (und vor allem für so komplexe Protokolle wie DNSSEC) bietet Interpretationsspielraum, welcher von unterschiedlichen Herstellern unterschiedlich ausgelegt werden kann und bis sich die verschiedenen Implementierungen auf ein stabiles Zusammenspiel „einspielen“, vergeht meist einige Zeit. Erschwerend bei DNSSEC kommt hinzu, dass einige Teile wie z.B. NSEC3 erst später standardisiert wurden und deshalb erst in den aktuellen Versionen implementiert werden konnten. NSEC3 wird z.B. erst ab Bind Version 9.6.0 unterstützt, welche Anfang 2009 veröffentlicht wurde. Bis diese Version in die verschiedenen Betriebssystem-Distributionen aufgenommen wird und dann auch auf den Nameserver installiert werden wird vergeht abermals viel Zeit. Mit einem nicht NSEC3-fähigen Resolver kann keine nach dem NSEC3-Standard signierte Zone (z.B. .gov) verifiziert werden. Im besten Fall wird die Zone wie eine nicht signierte Zone behandelt (ist so im Standard vorgesehen) im schlechtesten Fall wird die Zone (durch einen Implementierungsbug) als nicht korrekt signiert behandelt und kann nicht aufgelöst werden (bei .gov im Zusammenhang mit DLV mit Bind Version < 9.6 so aufgetreten).

Microsoft wird einen Teil von DNSSEC (NSEC, kein NSEC3) mit Windows 7 und Windows Server 2008-R2 unterstützen, für ältere Versionen ist nach jetzigem Wissensstand keine DNSSEC Unterstützung geplant. Windows 7 wird dabei die Validierung von DNSSEC als Stub-Resolver unterstützen, während Windows Server 2008-R2 als autoritativer Nameserver mit DNSSEC-Unterstützung dienen wird können.

Problematisch können auch noch Firewalls und SOHO-Router mit „Halbintelligenz“ sein, welche den DNS-Verkehr mithören und im Falle von Abnormalitäten blockieren. Haben diese Firewalls und Router keine DNSSEC Unterstützung blockieren diese möglicherweise die DNSSEC-Records, da die neuen Recordtypen nicht erkannt werden und als möglicher Angriff behandelt werden.

3.2.3 DNSSEC erfordert laufende Administration

Bisher war es möglich, die autoritativen DNS-Server zu konfigurieren, die Domain bei der Registry zu registrieren und dann das System auf „Autopilot“ ohne weiteren Eingriff laufen zu lassen. Gab es keine Änderung musste auch nichts an der Zone geändert werden. Dies ändert sich durch den Einsatz von DNSSEC:

- Die erzeugten Signaturen haben ein Ablaufdatum d.h. sind nicht „ewig“ gültig, auch wenn sich der zu Grunde liegende Record gar nicht geändert hat
- Die verwendeten Schlüssel sollen regelmäßig geändert werden, sogenannter „Key-Rollover“, um eine Kompromittierung mittels Brute-Force-Attacken auszuschließen

Der Nameserverbetreiber muss periodisch die Zonen neu signieren, da sonst die Signaturen auslaufen (und damit nicht mehr gültig sind) und die Domain nicht mehr aufgelöst werden kann. Der Key-Rollover bedeutet auch organisatorischen Ablauf: die Zone muss zusätzlich mit dem neuen Schlüssel signiert werden, der neue Schlüssel in der übergeordneten Zone als Fingerprint eingefügt werden und nach einer Übergangsphase die alten Signaturen, der alte Schlüssel und die Fingerprints in der höheren Zone entfernt werden. Eine sofortige Schlüsseländerung ist nicht möglich, da noch Signaturen mit dem alten Schlüssel in den Caches der Resolving Nameserver vorhanden sein können, welche ebenfalls noch validiert werden müssen.

Die Einführung bzw. der Einsatz von DNSSEC ist nicht nur ein reines Softwareupgrade. Es gehört auch eine Änderung bzw. die Neudefinierung von Geschäftsprozessen dazu.

Es gibt neue Anforderungen sowohl an die Nameserverbetreiber, die Registrare als auch an die Registries und die Resolving Nameserverbetreiber, beispielsweise:

- Schlüssel erstellen und Zonen signieren (Nameserverbetreiber)
- Regelmäßiges Neusignieren der Zone (Nameserverbetreiber)
- Regelmäßiger Schlüsselwechsel (Nameserverbetreiber)
- Melden der neuen Schlüssel an die Registry (Registrar)
- Löschen der alten Schlüssel aus der Registry (Registrar)
- Verifizieren der gemeldeten Schlüssel (Registry)
- Aktualisierung der Ausgangspunkte für die Chain-of-Trust (Registrar, Registry)

- Definition eines Prozesses für Emergency-Key-Rollovers im Falle von Problemen (Registry)
- Keyrollover und Aktualisierung der Trust-Anchors in der Root-Zone (Registry)

Beim Prozessdesign muss sowohl auf Sicherheit (damit keine falschen Schlüssel in die Chain-of-Trust eingeschleust werden können) als auch auf Geschwindigkeit (bei einem Emergency-Key-Rollover wegen eines kompromittierten Schlüssel muss rasch ein neuer Schlüssel in die Chain-of-Trust aufgenommen werden können) geachtet werden.

Weiters entsteht zusätzlicher Aufwand für die Sicherung/Geheimhaltung des privaten Keys (entsprechende Infrastruktur muss geschaffen werden und das administrative Vorgehen muss definiert werden).

3.2.4 Fehlertoleranz von DNS nimmt ab

DNS ist ein sehr fehlertolerantes Protokoll. Solange noch ein autoritativer Nameserver erreichbar ist funktioniert es meist noch „irgendwie“. Es gibt einen großen Graubereich wo trotz vieler Fehler das DNS für den Benutzer meist noch überraschend gut funktioniert. Mit dem Einsatz von DNSSEC ändert sich das nun. Stimmt etwas mit den Signaturen oder den Schlüsseln nicht, kann die Zone von den Resolvern nicht mehr validiert werden und ist nicht mehr auflösbar.

Wurde eine DNS-Zone durch fehlerhafte DNSSEC-Einträge „kaputt“ gemacht, zieht das große Probleme mit sich. Kunden können nicht mehr auf die Webseiten zugreifen (z.B. www.google.at ist nicht erreichbar), Emails können nicht zugestellt werden, selbst beim Versenden von Emails kann es zu Problemen kommen. Die Außendienstmitarbeiter können sich nicht mehr an das Firmennetzwerk anmelden und falls die Firma VoIP einsetzt kann es passieren, dass die Firma nicht einmal mehr per Telefon zu erreichen ist. Dieses Beispiel soll verdeutlichen wie viele Dienste direkt oder indirekt am DNS hängen und auf ein funktionierendes DNS angewiesen sind.

Vor allem beim Schlüsselwechsel (Key-Rollover) gibt es großes Potenzial für fatale Fehler. Ist einmal ein Fehler passiert und sind fehlerhafte Schlüssel im Umlauf, kann es durchaus einige Zeit dauern bis das Problem wieder behoben ist, da die fehlerhaften Records in den Caches der Resolver zwischengespeichert sind (und erst nach Ablauf der TTL entfernt werden). Solange die fehlerhaften, alten Records im Cache des Resolvers gespeichert sind wird versucht, die Signatur der Records (die mit einem neuen Schlüssel erzeugt wurden) mit dem alten Schlüssel zu überprüfen was natürlich fehlschlägt. Erst wenn die alten Schlüssel-Records aus dem Cache abgelaufen sind und der Resolver die neuen Schlüssel anfragt, klappt auch wieder die Validierung der Signaturen.

Ist eine Zone einmal DNSSEC signiert, kann dies nicht unmittelbar rückgängig gemacht werden. Es genügt nicht, einfach die Schlüssel und die Signaturen aus der Zone zu entfernen. Vorher müssen die Schlüssel aus der übergeordneten Zone entfernt werden und erst wenn diese in keinem Cache mehr vorhanden sind können die Signaturen entfernt werden. Ein „Entfernen wir halt schnell DNSSEC aus unserer Zone bis wir das Problem gelöst haben“ ist nicht möglich.

Hat ein wichtiger Zonenbetreiber sein DNSSEC-Setup zerstört, ist die Zone nicht mehr auflösbar, und die Clients erhalten Fehlermeldungen. Dies kann sich im schlimmsten Fall auch auf alle darunterliegenden Zonen auswirken.

3.2.5 Support Probleme

Hat eine Zone Probleme im DNSSEC-Setup (falsche Schlüssel im Umlauf, Signaturen sind abgelaufen, ...) ist diese für Kunden eines ISPs, welcher DNSSEC Validierung auf seinen Resolving-Nameservern aktiviert hat, nicht mehr auflösbar und die Kunden erhalten z.B. beim Zugriff auf die Webseite Fehlermeldungen. Die Kunden werden sich an ihren ISP wenden und dieser muss ihnen erklären, dass das Problem nicht in seinem Bereich liegt (Was allerdings für die Kunden u.U. nicht ersichtlich ist, da die Webseite bei anderen ISPs, die keine DNSSEC-Validierung aktiviert haben, sehr wohl funktioniert). Dadurch kann ein Druck auf den ISP entstehen, die Validierung abzudrehen. Für die meisten Kunden ist das Funktionieren der betroffenen Seite wahrscheinlich wichtiger als der Sicherheitsgewinn.

3.2.6 Problem beim Nameserverwechsel

Im bisherigen DNS-Setup konnte eine Domain im Falle von Problemen relativ einfach von einem Nameserverbetreiber zu einem anderen umgezogen werden. Bei DNSSEC ändert sich dieses Verhalten und die Rolle des Nameserverbetreibers nimmt an Bedeutung zu. Ist eine Domain DNSSEC signiert und der Nameserveroperator gibt den privaten Schlüssel der Domain nicht heraus, ist kein ausfallsfreier Umzug zu einem anderen Nameserveroperator möglich. Wie oben beschrieben, müssen bei einem Schlüsselwechsel kurzzeitig beide Schlüssel in der Zone aktiv sein. Kommt man allerdings an den aktuellen Schlüssel nicht

heran (Problem mit dem Nameserverbetreiber, Konkurs des Nameserverbetreibers, usw.) kann allerdings nur der neue Schlüssel verwendet werden und die alten Signaturen können nicht mehr validiert werden. Man muss also entweder den partiellen Ausfall in Kauf nehmen oder die Domain zuerst „DNSSEC-frei“ machen, danach transferieren und danach wieder neu signieren. Dafür wird allerdings Zeit benötigt.

3.2.7 DNSSEC ist inkompatibel mit bestehenden Lösungen

Der Einsatz von DNSSEC kann Probleme mit bestehenden technischen Lösungen verursachen:

DNSSEC und dynamische Updates

Einige Registrare verwenden zur Provisionierung der Nameserver dynamische Updates welche z.B. direkt von den internen Systemen generiert werden. Bind selbst unterstützt zwar dynamische Updates und DNSSEC, allerdings wird dafür der private Schlüssel der Zonen direkt auf den Nameservern benötigt, da die Zonen „on-the-fly“ neu signiert werden. Damit geraten bei einem eventuellen Zugriff auf den Nameserver auch die privaten Schlüssel in die Hand des Eindringlings.

DNS-manipulierende Anwendungen

Einige Anwendungen wie z.B. Captive-Portals und Filter-Proxies verwenden „falsche“ DNS-Pakete um Benutzer auf Webseiten mit Anmeldemasken oder Fehlermeldungen umzuleiten. Dieses Verhalten funktioniert mit DNSSEC nicht mehr, da die „falschen“ DNS-Pakete vom Client verworfen werden.

Davon betroffen sind auch die geplanten Netzzugangerschwernisse („Kinderpornosperr“) in Deutschland, welche die Internetbenutzer mittels „falschen“ DNS-Antworten auf eine sogenannte Stoppschildseite anstatt auf die Kinderpornoseite umleitet. Ist allerdings DNSSEC im Einsatz, wird die „falsche“ DNS-Antwort verworfen, der Benutzer erhält eine Fehlermeldung und landet nicht auf der Stoppschildseite (allerdings auch nicht auf der vermeidlichen Kinderpornoseite).

Nameserver mit Datenbankbackends

Einige Nameserver verwenden Datenbankbackends, wo die Zonendaten in einer Datenbank gespeichert werden und auch direkt dort provisioniert werden können. Für DNSSEC müssen diese Nameserver zumindest die Logik beherrschen, welche zusätzlichen Records sie wann mitschicken müssen (Signaturen, NSEC, NSEC3). Das Signieren der Zone kann unabhängig vom Nameserver erfolgen.

Split-DNS

Liefert ein Nameserver abhängig von anfragenden Client unterschiedliche DNS-Records aus, müssen auch die jeweiligen korrekten DNSSEC-Records mitgeschickt werden. Problematisch ist auch, wenn z.B. die eine Sicht einer Split-DNS-Installation DNSSEC-signiert werden soll, die andere jedoch nicht.

Router, Firewalls ohne DNSSEC-Unterstützung

Viele Router (vor allem im Heimbereich) bieten ihren Benutzern DNS-Funktionalität (Resolving Nameserver) an (und die Kunden verwenden diese Funktionalität oft automatisch), Diese Resolver bieten jedoch oft nur ein Minimum an DNS und haben mit hoher Wahrscheinlichkeit keine DNSSEC-Unterstützung eingebaut. Will jetzt ein Benutzer hinter einem solchen Router DNSSEC verwenden muss dieser einen anderen Resolving Nameserver verwenden. Problematisch wird es, wenn der Router dies nicht erlaubt und die DNS-Pakete verändert (DNSSEC-Signaturen sind nicht bekannt und werden entfernt o.ä.).

Ebenfalls problematisch sind Firewalls. Viele Firewalls analysieren auch den Inhalt der Pakete und prüfen ob das verwendete Protokoll auch korrekt ist. Prüft so eine Firewall jetzt DNS-Pakete mit DNSSEC-Inhalt, kann es sein, dass die Firewall DNSSEC nicht unterstützt und korrekte Pakete als möglicher Angriff bewertet und verworfen werden. Für die Benutzer dahinter ist dann keine DNS-Auflösung mehr möglich.

3.2.8 DNSSEC ist noch nicht komplett standardisiert

DNSSEC ist technisch weitgehend standardisiert, allerdings fehlt zum großen Teil noch die organisatorische bzw. administrative Standardisierung. Jede Registry, welche DNSSEC einführen will, muss selbst Wege und Prozesse für den Schlüsselwechsel, das Schlüsselmanagement, die Auswirkung von DNSSEC auf die bestehenden Registry-Transaktionen (Domaintransfer, ...) usw. überlegen und erarbeiten und diese Lösungen können sich von bereits bestehenden Lösungen anderer Registries unterscheiden. Große Registrare, welche mit mehreren Registries zusammenarbeiten, müssen unter Umständen für jede Registry eigene Prozesse implementieren was den Aufwand erhöht.

4 DNSSEC für .at

nic.at als Registry für .at beschäftigt sich bereits seit einiger Zeit mit DNSSEC. Es werden laufend Tests in einer Testumgebung durchgeführt und die aktuellen Entwicklungen im Auge behalten. Weiters erfolgt ein laufender Erfahrungsaustausch mit anderen Registries.

Aktuell sieht nic.at keinen Bedarf DNSSEC für .at einzuführen und hat auch keinen konkreten Zeitplan für die Einführung. Die Einführung von DNSSEC ist ein großer Aufwand sowohl für die Domainregistry, mehr jedoch noch für die Registrare bzw. die Vielzahl der Nameserverbetreiber. Erfahrung von Registries, welche bereits DNSSEC im Produktiveinsatz haben, zeigen, dass Kunden nur sehr geringes Interesse an „sichereren“ Domains haben und es auch kaum Nachfrage danach gibt, selbst wenn DNSSEC-signierte Domains zum gleichen Preis wie „normale“ Domains angeboten werden. Die zusätzliche Komplexität und möglichen neuen Fehlerquellen stehen zurzeit in keinem Nutzen zur zusätzlich gewonnenen Sicherheit. Weiters sind derzeit die Rahmenbedingungen (Signatur der Root-Zone, Verbreitung bzw. Stabilität der Software) noch nicht gegeben, um einen stabilen Einsatz von DNSSEC zu garantieren. Ein stabiles DNS-System ist zu wichtig um es durch einen zu raschen Einsatz von DNSSEC zu stören.

Um DNSSEC für .at einzuführen würde auf Seiten der nic.at ein Aufwand von mind. 300 Manntagen anfallen, welche durch Anpassungen bzw. Erweiterungen der bestehenden Systeme entstehen. Zusätzlich kommen noch Ausgaben für neue bzw. zusätzliche Hardware dazu. DNSSEC kann sehr ressourcenintensiv sein, die Größe der Zone kann sich im Extremfall bis zum Faktor 10 erhöhen, was entsprechende Anforderungen an die Hardware auslöst. Weiters bringt eine große Zone Probleme beim Laden bzw. Neuladen aufgrund von Änderungen mit sich. Je größer die Zone ist, desto länger dauert so ein Reload.

Weiters fallen noch Aufwendungen auf Seiten der Registrare und Nameserverbetreiber an. DNSSEC als Insellösung nur für die .at-Zone einzuführen (ohne Registrare und Nameserverbetreiber, die es ebenfalls unterstützen) bringt keinen Sicherheitsgewinn. In Gesprächen mit Registraren zeigt sich auch, dass von dieser Seite kein Interesse an DNSSEC besteht. Das Hauptproblem der Registrare ist, dass der Aufwand, der für die Einführung notwendig ist, nicht zurückverdient werden kann. Erfahrungen aus anderen Ländern, welche bereits DNSSEC eingeführt haben, zeigen, dass Kunden nicht bereit sind für DNSSEC-geschützte Domains extra zu bezahlen. Und selbst in Ländern wie Schweden, wo die .se-Registry DNSSEC-signierte Domains ohne Aufpreis anbietet, ist die Nachfrage danach sehr gering (Stand 07/2009: ~1900 signierte Domains von 886000 registrierten Domains, DNSSEC wird in Schweden seit 02/2007 angeboten).

Allerdings kann ein plötzlicher Notfall, z.B. eine neue, heute noch unbekannte Attacke auf das DNS, welche nur mit DNSSEC abgewehrt werden kann, dazu führen, dass rasch DNSSEC eingeführt werden muss. Für diesen Fall arbeitet nic.at an Plänen, um gerüstet zu sein. Weiters besteht die Möglichkeit - sollte der Wunsch bzw. Bedarf vorhanden sein - ein DNSSEC-Testfeld für .at zu entwickeln, um den Registraren die Möglichkeit zu geben selbst Erfahrungen mit DNSSEC zu sammeln.

5 Referenzen

DNS und alle dazugehörigen Erweiterungen werden von der IETF als RFCs veröffentlicht. Eine sehr gute Auflistung aller DNS relevanten RFCs findet sich unter <http://www.dns.net/dnsrd/rfc/>. Aktuelle Entwicklungen können den IETF Arbeitsgruppen „DNS Extensions“ (dnsext: <http://www.ietf.org/html.charters/dnsext-charter.html>) und „Domain Name System Operations“ (dnsop: <http://www.ietf.org/html.charters/dnsop-charter.html>) mitverfolgt werden.

Autor: Michael Braunöder
mib@nic.at

6 Glossar

Caching	Zwischenspeichern häufig benutzter Informationen
DNS	Domain Name System; einer der wichtigsten Dienste im Internet, dient zum Auflösen von Hostnamen auf IP-Adressen.
DNSSEC	DNS Security Extension; Erweiterung des DNS um Authentizität und Integrität von DNS-Abfragen zu gewährleisten.
IETF	Internet Engineering Taskforce; Standardisierungsgremium für das Internet
ISP	Internet Service Provider; Zugangsanbieter zum Internet
NSEC/NSEC3	Next Secure Record (3); Technologie in DNSSEC um die Nichtexistenz von DNS-Records zu beweisen.
Phishing	Versuch mit gefälschter Identität an sensible Daten wie z.B. Passwörter zu gelangen
Registrar	Domain Registrar; für die Domain Registrierung verantwortliche Organisation
Registrant	Domain Registrant; Inhaber einer Domain
Registry	Domain Name Registry; Organisation die Domains verwaltet
Root-Zone	Wurzel des hierarchisch organisierten DNS
RFC	Request for Comments; wichtigsten Standardisierungsdokumente des Internets
Spam	Unerwünschte und unverlangte Werbemails
Spoofing	Manipulation durch verwenden von falschen Daten
TCP	Transmission Control Protocol; zuverlässiges, verbindungsorientiertes Netzwerkprotokoll
TLD	Top Level Domain; Domain auf höchster Ebene der Namensauflösung (z.B.: .at, .com, .eu)
VoIP	Voice over IP; Telefonieren über das Internet
UDP	User Datagram Protocol; ein leichtes, verbindungsloses Netzwerkprotokoll
Zone	Bereich im DNS, der die Dateien einer Domain umfasst