DNSSEC bij Byte

Imre Jonk

2018-11-06

Samenvatting

Webhostingbedrijf Byte wil domeinnamen van klanten gaan beveiligen met DNSSEC. Dat is een oplossing voor de structurele beveiligingsproblemen in het Domain Name System. Byte heeft DNSSEC nodig om te kunnen voldoen aan de nieuwe eisen van Thuiswinkel.org, een organisatie waar veel klanten van Byte aan verbonden zijn. In dit onderzoek worden daarom de mogelijkheden tot implementatie en de geïdentificeerde risico's behandeld. Er wordt een implementatieplan geschreven waarin de wijzigingen aan de DNS-infrastructuur van Byte worden omschreven en er wordt software ontwikkeld voor het geautomatiseerd kunnen uitrollen van DNSSEC. Daarnaast worden de keuzes met betrekking tot cryptografie en sleutelbeheer behandeld.

Onderwijsinstelling:	Hogeschool van Amsterdam
Opleiding:	HBO-ICT
Richting:	System and Network Engineering
Jaar:	4
Afstudeerbegeleider:	David Zeegers
Stagebedrijf:	Byte B.V., Amsterdam
Bedrijfsbegeleiders:	Jeroen van Heugten, Saskia van Leeuwen

Inhoudsopgave

1 Introductie

Byte biedt e-commerce hosting aan op een zelfontwikkeld platform. De klant kan naast een hostingpakket ook een domeinnaam afnemen dat daar met het Domain Name System (DNS) aan kan worden gekoppeld. Om de beveiliging van deze koppeling te kunnen garanderen wil Byte Domain Name System Security Extensions (DNSSEC) implementeren. De klanten van Byte, voornamelijk webshops, hebben veel baat bij deze maatregel omdat zij vanaf volgend jaar voor het keurmerk Thuiswinkel Waarborg moeten voldoen aan een aantal technische beveiligingsmaatregelen, waarvan DNSSEC een basismaatregel is. Daarnaast krijgt Byte een vergoeding van het .nl-register wanneer de geregistreerde .nl-domeinnamen met DNSSEC worden beveiligd. De implementatie vereist aanpassingen aan het DNS-platform die in deze scriptie worden beschreven.

1.1 Onderzoeksvraag

De onderzoeksvraag luidt: "Hoe kan DNSSEC worden geïmplementeerd op de authoritative nameservers van Byte?"

Deelvragen:

1. Wat is het DNS?
2. Wat is DNSSEC?
3. Hoe werken de authoritative nameservers van Byte?
4. Welke aanpassingen zijn nodig om de zones met DNSSEC te ondertekenen?
5. Welke risico's introduceert DNSSEC?

1.2 Scope

Deze scriptie behandelt de werking en beveiliging van het Domain Name System en systemen die afhankelijk zijn van het DNS. Hierbij zijn de systemen, diensten en processen van Byte het uitgangspunt. De stageopdracht omvat drie onderdelen: een overzicht van de risico's van het invoeren van DNSSEC bij Byte, een implementatieplan waarin tegenmaatregelen zijn verwerkt en een werkende implementatie op een testomgeving.

De werking en beveiliging van het DNS zal worden omschreven met als doel inzicht te krijgen in de structurele beveiligingsproblemen van het Domain Name System, zodat de noodzaak van het invoeren van DNSSEC bij Byte kan worden aangetoond. Tevens zal het onderzoek hiernaar leiden tot het vinden van risico's voor de dienstverlening van Byte wanneer DNSSEC wordt geïmplementeerd.

De risico's en tegenmaatregelen moeten relevant zijn voor de systemen, diensten en processen van Byte. Ook het implementatieplan moet hierop afgestemd zijn.

Omdat de implementatie van DNSSEC naast een veiligere DNS-infrastructuur kan bijdragen aan de veiligheid van andere systemen van Byte en haar klanten, zal deze scriptie daar ook op ingaan.

1.3 Methode

Eerst zal literatuuronderzoek plaatsvinden naar de werking van het DNS, welke kwetsbaarheden er bekend zijn en hoe DNSSEC zorgt voor een betere beveiliging. Vervolgens wordt de situatie bij Byte onderzocht en de gewenste situatie geschetst. Dan zullen de risico's van een DNSSEC-implementatie bij Byte onderzocht worden en wordt er een implementatieplan geschreven. Tot slot wordt er een werkende testimplementatie ontwikkeld.

2 Werking van het Domain Name System

Het Domain Name System wordt gebruikt op het internet voor het opvragen van informatie op een hiërarchische manier. Hierbij gaat het voornamelijk om het opvragen van IP-adressen (bijvoorbeeld 2001:db8:fe7:3::1) aan de hand van makkelijk te onthouden hostnames (bijvoorbeeld www.example.com). Een client die het IP-adres van www.example.com nodig heeft zal de geconfigureerde *resolver* bevragen [44]. Een resolver geeft in principe antwoord op alle queries van clients. Een resolver kan statisch worden geconfigureerd, maar ook met een DHCP-server, DHCPv6-server of IPv6 router advertisement [29, 28, 5].

Naast resolvers kent het DNS ook authoritative nameservers. Dat zijn servers die alleen antwoord geven op queries voor geconfigureerde zones. Een zone omvat in principe alle DNS-data van een domeinnaam waar de authoritative nameserver over beschikt.

De resolver zal eerst kijken of het IP-adres van www.example.com is opgeslagen in de cache. Als dit het geval is wordt de query direct beantwoord. Zo niet, dan zal de resolver het Domain Name System gebruiken om het IP-adres op hiërarchische wijze op te vragen [44]. In dat geval zal de resolver eerst één van de dertien *root servers* proberen, die statisch zijn geconfigureerd in de software van DNS resolvers [20]. Omdat de root server niet authoritative is voor www.example.com, maar wel weet welke nameservers authoritative zijn voor de .com-zone, geeft de root server de resolver een lijst met authoritative nameservers van de .com-zone. De resolver zal het vervolgens aan een nameserver van de .com-zone vragen, die ook niet authoritative is voor www.example.com, maar wel weet welke nameservers authoritative zijn voor example.com. De resolver herhaalt de query bij een authoritative nameserver van example.com. Deze server beschikt, indien er geen verdere delegatie van toepassing is, over het IP-adres van www.example.com, samen met een time to live waarde. Deze TTL-waarde wordt door de resolver gebruikt om het antwoord voor de opgegeven tijd op te slaan in de cache. Tot slot stuurt de resolver het antwoord door naar de client [44].

Het Domain Name System wordt niet alleen gebruikt voor het opvragen van IP-adressen bij hostnames (A of AAAA resource records), maar ook voor het opvragen van hostnames aan de hand van IP-adressen (PTR resource records), om aan te geven welke nameservers authoritative zijn voor een zone (NS resource records), welke servers e-mail moeten ontvangen (MX resource records) en nog veel meer [45, 11]. Een goede werking van het Domain Name System is daarom van groot belang voor het internet.

3 Kwetsbaarheden in het DNS

De ontwerpers van het Domain Name System hebben geen rekening gehouden met de beveiliging. Dat was niet nodig voor de oorspronkelijke opzet van het ARPANET (de voorloper van het internet), maar nu het is uitgegroeid tot een wereldwijd netwerk zijn de beveiligingseisen toegenomen. Eén van de problemen is dat het DNS geen mogelijkheid biedt voor het controleren van de antwoorden. Dit staat een aanval toe die DNS cache poisoning heet [55].

3.1 DNS cache poisoning

Bij DNS cache poisoning zorgt de aanvaller ervoor dat verkeerde informatie in de cache van een resolver terechtkomt. Hierdoor kunnen alle clients van deze

resolver omgeleid worden naar een (phishing)site van de aanvaller [55]. In de extremere gevallen kan de aanvaller ervoor zorgen dat e-mail wordt omgeleid, zodat hij onder andere wachtwoorden kan resetten en ongeautoriseerd TLS-certificaten kan aanvragen [27]. De aanvaller kan een kwetsbaarheid in de resolver misbruiken, maar kan ook gebruikmaken van een race attack. Hierbij probeert de aanvaller het antwoord van de authoritative nameserver voor te zijn met een vervalst antwoord. Het vervalste antwoord kan dan vaak tot een week of zelfs langer door de resolver gecachet worden. Deze aanval kan deels worden voorkomen door het gebruik van technieken als source port randomization [27] en willekeurige nonces. Om te bepalen hoeveel pogingen er gemiddeld nodig zijn om de combinatie nonce en source port te raden kan deze formule gebruikt worden:

$$\chi = \frac{2^{16}(\delta + 1)}{2}$$

Waarbij χ gelijk is aan het gemiddeld aantal pogingen en δ gelijk is aan het verschil tussen de hoogst mogelijke source port en de laagst mogelijke source port. Linux kernel versie 4.9 gebruikt standaard als laagste source port 32768 en als hoogste source port 60999. Dit is op te vragen met het commando "cat /proc/sys/net/ipv4/ip_local_port_range"[32]. Het invullen van deze waarden in de formule resulteert in gemiddeld 925.106.176 pogingen (1.850.212.352 mogelijkheden). Deze berekening gaat ervan uit dat de selectie van de nonce en de source port perfect willekeurig is. De Linuxkernel heeft sinds versie 2.6.24 ondersteuning voor UDP source port randomization [36]. Zogenaamde middleboxes die netwerkverkeer inspecteren, blokkeren en modificeren met firewalls en technieken als network address translation (NAT) kunnen de source port echter voorspelbaar maken [43, 64, 27], waardoor enkel de juiste 16-bit nonce geraden hoeft te worden, zodat de aanval significant sneller kan worden uitgevoerd. Een 16-bit nonce is namelijk in gemiddeld 32.768 pogingen geraden.

4 DNSSEC

Domain Name System Security Extensions (DNSSEC) voegt cryptografische ondertekeningen toe aan DNS-antwoorden waardoor de antwoorden op authenticiteit kunnen worden gecontroleerd. Dit voorkomt succesvolle DNS cache poisoning attacks, omdat een validerende resolver niet meer blind op het antwoord van een authoritative nameserver vertrouwt. Voor de crypto-

grafische ondertekeningen wordt public key cryptography gebruikt. Hierbij wordt een private key gebruikt voor het ondertekenen van DNS resource records, terwijl een public key gebruikt wordt voor het controleren van de ondertekeningen. De ondertekeningen worden toegevoegd met RRSIG resource records [9]. Een antwoord dat ondertekend is met DNSSEC ziet er zo uit:

```
example.com.      86400  IN  A      93.184.216.34
example.com.      86400  IN  RRSIG  A 8 2 86400 20180307063923
   20180213201202 54756 example.com. pGaAd+J/eG10GaOIvzNUeGD3bYee/
   ExMj1o5E5yLFAkVjfLaBG3u53Fu 1
   ABZ3ufMOAX8UYJsoIfUtL5MEu8ILaf0i3i1ejbsvZ2nGxoWVn/56l7N
   QLl6S3wJDZ1McFylTdo/qBETOnrgMSQ6goUnb+5t7k2JQBrpanxNXIsm hEU=
```

De public key die gebruikt kan worden om de ondertekeningen te controleren heet de Zone Signing Key (ZSK) en wordt ook opgenomen in de zone met het DNSKEY resource record [8]:

```
example.com.      3600   IN  DNSKEY 256 3 8
   AwEAAblDjCPejMhknWXZqbwBEUPI6LkwjvpOXlUNTBqW2glZrgf3MXjJ
   ZBXl8rhYoTkrov7jmbBaBOPTkqlQAbfOKFNoG+U+boGG6Zmy00l2XRP1
   nckVMpJ2TxiDVcXJqs78MetC1Ztu4p6bj4VrJCYTmv3ZULSrWleMSWtv
   YXqY0S23
```

In dit geval worden de resource records ondertekend met een 1024-bit RSA key. De Internet Assigned Numbers Authority (IANA) houdt bij welke algoritmes gebruikt kunnen worden voor DNSSEC [38]. De ZSK wordt ondertekend met een langetermijn Key Signing Key (KSK). De KSK kan zo veilig offline worden bewaard. Deze constructie is overigens niet verplicht, er kan ook een Combined Signing Key (CSK) gebruikt worden die de functies van de ZSK en KSK combineert [35].

Om er zeker van te zijn dat de resolver de juiste public key gebruikt voor het controleren van de ondertekeningen, is de uitkomst van een cryptografische hashfunctie (de hash) van de KSK opgenomen in de parent zone. Bij example.com is de hash van de public key dus opgenomen in de .com-zone. Dit wordt gedaan met een Delegation Signer (DS) resource record [9]:

```
example.com.      86400  IN  DS  31406 8 2
   F78CF3344F72137235098ECBBD08947C2C9001C7F6A085A17F518B5D 8
   F6B916D
```

Op dezelfde manier is de hash van de KSK van de .com-zone opgenomen in de root zone. De KSK van de root zone wordt beheerd door IANA [17] en is

aanwezig in resolvers die DNSSEC ondersteunen [21]. Het technisch beheer van de root ZSK is, net als de root zone zelf, uitbesteed aan het Amerikaanse bedrijf Verisign [16]. IANA voert vier keer per jaar een Root KSK Ceremony uit om de ZSKs van het komende kwartaal te ondertekenen [19].

4.1 Authenticated denial of existence

Als een domeinnaam niet bestaat, dan laat een traditionele authoritative nameserver dat weten met een NXDOMAIN-antwoord. Als een domeinnaam wel bestaat maar het opgevraagde resource record niet, dan wordt er een NODATA-antwoord teruggestuurd [12]. Het is belangrijk dat DNSSEC man-in-the-middle-attacks voorkomt waarbij de aanvaller bijvoorbeeld doet alsof een DS resource record niet bestaat, waardoor de resolver de child zone niet zal valideren. De oplossing voor dit probleem is het verplicht cryptografisch bewijzen dat een resource record niet bestaat. Deze techniek heet authenticated denial of existence. Omdat er oneindig veel domeinnamen niet bestaan is het niet mogelijk om vooraf NXDOMAIN-antwoorden te ondertekenen. Hierdoor zullen alle authoritative nameservers dus over de private keys van hun zones moeten beschikken om het NXDOMAIN-antwoord *live* te ondertekenen. Omdat dit niet de opzet was van DNSSEC is deze methode in eerste instantie niet gestandaardiseerd [8]. In plaats daarvan werd gekozen voor het Next Secure resource record, dat aangeeft welk resource record alfabetisch gezien de volgende is [9]. Wanneer een resolver aan een authoritative nameserver vraagt wat het IP-adres is van een hostname die niet bestaat (in dit voorbeeld abc.example.com), zal de nameserver een ondertekend NSEC resource record teruggeven:

```
example.com.      3600   IN  NSEC   www.example.com. A NS SOA TXT
   AAAA RRSIG NSEC DNSKEY
example.com.      3600   IN  RRSIG  NSEC 8 2 3600 20180220002754
   20180130042118 61743 example.com. DWp3phV+0
   FIkm50pysp3LYfpwmqCjJg42ISCHQt7QBov4qqAVJCf2jpp /HiovN+
   Vu9N3kQuDiooxAGXAQr7cIUh9K+ivXTqA8ArBJxC7oW2v0p+D nGuD583i+
   EZlvHwleuZvaXhedPJ031kUdWMbMDXt/SFJ3r8Bm/gNga6x Wlw=
```

In dit geval geeft de nameserver met het NSEC resource record aan dat er tussen example.com en www.example.com geen domeinnamen bestaan, en dat alleen de resource record types A, NS, SOA, TXT, AAAA, RRSIG, NSEC en DNSKEY bestaan voor de domeinnaam example.com.

4.2 Uitrol van DNSSEC in Nederland

De Stichting Internet Domeinregistratie Nederland (SIDN) beheert de .nl-zone [48]. SIDN heeft op 23 augustus 2010 de .nl-zone ondertekend [49] en houdt de uitrol van DNSSEC bij .nl-domeinnamen scherp in de gaten. De voortgang van de uitrol is te volgen op `https://stats.sidnlabs.nl/nl/dnssec.html`. Op 6 augustus 2018 was 52.64 % van de .nl-domeinnamen met DNSSEC beveiligd.

Een registrant (de houder van een domeinnaam) heeft zijn domeinnaam doorgaans niet direct bij het register (bijvoorbeeld SIDN) geregistreerd, maar bij een tussenpartij, de zogenaamde registrar. Byte is ook een registrar. Registrars die DNSSEC ondersteunen wisselen naast whois-gegevens en nameservers ook DNSSEC public keys uit met het register. Op die manier kan het register de hash van de public key opnemen als DS resource record in de parent zone, en is de koppeling tussen parent en child zone beveiligd. Registrars implementeren hier uiteenlopende oplossingen voor. Sommige registrars houden DNSSEC keys volledig in eigen beheer, terwijl andere registrars hun klanten de optie geven zelf hun domeinnamen te ondertekenen en de public key via het service panel te uploaden. Dit kan nuttig zijn wanneer de klant zelf of bij een andere partij het DNS-beheer regelt.

De Nederlandse overheid heeft DNSSEC verplicht gesteld voor “alle overheidsdomeinnamen én op DNS-resolvers die clients van overheidsorganisaties direct of indirect van DNS-antwoorden voorzien” [57]. Deze omschrijving omvat dus ook authoritative nameservers en resolvers van derde partijen waar de overheid gebruik van maakt. DNSSEC staat op de lijst ‘Verplicht (pas toe of leg uit)’ van het Forum Standaardisatie [58]. Dit houdt in dat overheidsorganisaties DNSSEC als open standaard hanteren. Afwijken van de verplichting mag alleen bij zwaarwegende redenen, waarvoor verantwoording in het jaarverslag moet worden afgelegd [23]. Bovendien staat het gebruik van de technieken STARTTLS en DNS-based Authentication of Named Entities (DANE) voor mailservers op dezelfde lijst [58]. STARTTLS wordt gebruikt om een onveilige verbinding te upgraden naar een beveiligde verbinding [39]. DANE wordt in deze context gebruikt om de public key van de ontvangende mailserver met DNSSEC te authenticeren, waardoor een succesvolle man-in-the-middle-attack wordt voorkomen [62].

4.3 Andere DNS security-uitbreidingen

Naast de DNSSEC resource records zijn er nog andere securitygerelateerde resource records:

Type	**RFC**	**Functie**
IPSECKEY	RFC 4025	Publiceren van IPsec public keys
SSHFP	RFC 4255	Publiceren van SSH key fingerprints
TLSA	RFC 6698	Publiceren van TLS public keys
CAA	RFC 6844	Aangeven welke CA's certificaten voor een domeinnaam mogen tekenen
OPENPGPKEY	RFC 7929	Publiceren van OpenPGP public keys

5 DNS bij Byte

Byte heeft drie authoritative nameservers beschikbaar voor zones van klanten en Byte zelf: nsa.byte.nl, nsb.byte.nl en nsc.byte.nl. NSA en NSB zijn in een datacenter van telecomprovider KPN ondergebracht terwijl NSC in een datacenter van netwerkleverancier euNetworks draait. Klanten kunnen ook gebruikmaken van $\{nsa|nsb|nsc\}$.byteinternet.com. Dit is handig als er problemen zijn met de .nl-zone waardoor de byte.nl-nameservers onbereikbaar kunnen worden, zoals op 29 mei 2008 gebeurde [63].

De nameservers maken gebruik van de software PowerDNS en wisselen zonedata uit via MySQL replication. PowerDNS ondersteunt DNSSEC [25] maar dat is op de nameservers van Byte niet ingeschakeld. De nameservers bij KPN worden met de automatiseringssoftware Puppet van configuratie voorzien, de nameservers bij euNetworks met Ansible.

Het service panel biedt de klant de mogelijkheid om zelf DNS resource records aan te maken, te wijzigen en te verwijderen. De ondersteunde resource record types zijn A, AAAA, CNAME, MX, TXT en SRV. Het service panel is geschreven in de programmeertalen Perl en Python en maakt gebruik van het Django web framework. De achterliggende application programming interface (API) is geschreven in Perl en kan tabellen in de PowerDNS-database lezen en bewerken. Deze database wordt gesynchroniseerd met de nameservers zodat zij altijd over de meest recente zonedata beschikken.

Byte registreert .nl-domeinnamen rechtstreeks bij SIDN, overige extensies worden via RRPproxy (onderdeel van het Duitse bedrijf Key-Systems GmbH) geregistreerd. Zowel SIDN als RRPproxy ondersteunen het Extensible Pro-

visioning Protocol (EPP), wat onder andere gebruikt wordt voor het uitwisselen van houdergegevens, nameservers en DNSSEC keys tussen registers en registrars [37, 33, 40].

Wanneer een klant in het service panel een domeinnaam registreert, roept het service panel de API van SIDN of RRPproxy aan om de domeinnaam te registreren, de whois-gegevens in te stellen en de nameservers te configureren. Dit gebeurt met de Perl libraries Byte::DRS en Net::DRI. Net::DRI ondersteunt DNSSEC, Byte::DRS niet. De nameservers zijn in principe altijd nsa.byte.nl, nsb.byte.nl en nsc.byte.nl. In het service panel kunnen de nameservers van een domeinnaam niet gewijzigd worden, dit moet via de supportkanalen.

Er valt nog een opmerking te maken over het beheer van de PowerDNS database. Sommige subdomeinen zijn namelijk opgegeven als aparte zones, terwijl de domeinnaam zelf ook als zone in de database staat. Er is hiervoor gekozen om het beheer van pakketten te vergemakkelijken. Deze constructie heeft als nadeel dat de DNSSEC-keten moet worden verlengd omdat de subzones als aparte schakel moeten worden toegevoegd. Dit houdt concreet in dat de subzone een aparte DNSSEC-sleutel moet krijgen en dat er via de PowerDNS-database een DS-record moet worden aangemaakt in de parent zone.

6 Overwegingen

Het doorvoeren van een verandering binnen een organisatie gaat altijd gepaard met risico's. Bij een onderdeel zo cruciaal als DNS is de impact vanzelfsprekend hoog. Het is dus van groot belang dat de kans op problemen met DNSSEC zo klein mogelijk wordt gehouden. In dit onderdeel worden daarom de geïdentificeerde risico's en tegenmaatregelen besproken.

6.1 Amplification attacks

Risico: een antwoord dat met DNSSEC is ondertekend is significant groter dan een antwoord dat niet is ondertekend. Dit is aantrekkelijk voor cybercriminelen die een DDoS-aanval willen uitvoeren door nameservers te misbruiken in een *amplification attack*. Daarbij stuurt de aanvaller veel kleine DNS queries met een vervalst source IP-adres naar een aantal nameservers.

Deze nameservers sturen daardoor veel grote antwoorden naar het slachtoffer. De verbinding of de server van het slachtoffer kan al dit verkeer niet aan en wordt onbereikbaar [1].

Tegenmaatregel: er zijn een aantal maatregelen die internetproviders en beheerders van authoritative nameservers en resolvers kunnen nemen om de impact van een amplification attack zo klein mogelijk te houden:

1. Implementeer ingress filtering (BCP 38, BCP 84) [51, 30]. Hiermee filteren internetproviders het uitgaande verkeer van hun klanten, zodat alleen pakketten met toegestane source IP-adressen doorgelaten worden.
2. Biedt geen open resolver aan zonder adequate beveiliging. Open resolvers staan iedereen toe om queries te doen, en kunnen door aanvallers gebruikt worden om extreem grote antwoorden in de cache van de resolver te plaatsen en vervolgens met een amplification attack naar een slachtoffer te sturen [1].
3. Hou antwoorden van nameservers zo klein mogelijk. Des te kleiner het antwoord, des te kleiner de amplification factor.
4. Implementeer response rate limiting (RRL). RRL limiteert het aantal antwoorden dat per seconde naar een netwerk kan worden verstuurd [26].

6.2 Zelf-veroorzaakte denial-of-service

Risico: DNSSEC voegt complexiteit toe aan het beheren van DNS-zones. Het is belangrijk dat het ondertekenen van de zones goed gebeurd, omdat de resource records anders niet opgevraagd kunnen worden door clients die een DNSSEC-validerende resolver gebruiken. Dit is tevens de belangrijkste reden waarom nog niet alle internetproviders DNSSEC op hun resolvers ondersteunen: als een populaire website haar DNS-zone niet goed ondertekent zal de website niet bereikbaar zijn voor klanten van een internetprovider die DNSSEC ondersteunt op haar resolvers, terwijl de website wel gewoon bereikbaar is voor internetproviders die DNSSEC niet ondersteunen. Hierdoor ontstaat een soort kip-en-ei probleem [52].

Problemen met DNSSEC komen regelmatig voor. De meest noemenswaardige voorvallen worden bijgehouden op de website IANIX.com [41].

Het is dus belangrijk dat ondertekeningen ten alle tijden kloppen. Dit betekent dat alle resource records altijd ondertekend moeten zijn met een private key waarvan de corresponderende public key in een DNSKEY resource record is opgenomen en dat de hash van de public key als DS resource record is opgenomen in de parent zone. Daarnaast hebben ondertekeningen een bepaalde geldigheidsperiode, dus het is tevens van belang dat de zones op tijd opnieuw ondertekend worden [8]. Bovendien zullen de private keys soms (al dan niet preventief) vervangen moeten worden [60].

Tegenmaatregel: Byte standaardiseert en automatiseert zoveel mogelijk processen om menselijke fouten te voorkomen. Dit moet dus ook gedaan worden bij de implementatie van DNSSEC. De implementatie moet uitvoerig getest worden voordat deze in gebruik wordt genomen. Daarnaast moet het bestaande monitoringsysteem worden geconfigureerd voor DNSSEC-validatie, zodat problemen met DNSSEC niet onopgemerkt blijven.

6.3 Denial-of-service veroorzaakt door parent zone

Risico: een DNSSEC-validerende resolver moet de complete keten tot aan de *root trust anchor* kunnen controleren. Dit houdt in dat, naast de zone van een klant van Byte, ook de zone van het register (bijvoorbeeld .nl) en de root zone (beheerd door IANA) ten alle tijden correct ondertekend moet zijn. Websites van klanten zullen voor een deel van de bezoekers onbereikbaar zijn als ergens in deze keten een fout wordt gemaakt. Zoals IANIX.com aangeeft komen problemen bij parent zones zoals .nl wel degelijk voor, en zelfs de root servers hebben in het verleden problemen gehad [41].

Tegenmaatregel: Byte heeft geen controle over het DNSSEC-proces van parent zones. Het lijkt daarom niet mogelijk om een audit te doen van elke mogelijke keten. Sommige parent zones erkennen dit probleem en proberen daarom zo transparant mogelijk te zijn over hun DNSSEC-beleid. Onder andere IANA en SIDN publiceren DNSSEC Practice Statements [22] [2] [46] waarin het beleid wordt omschreven. Omdat deze processen voor Byte van groot belang zullen zijn zodra zones van klanten met DNSSEC zijn beveiligd, zou Byte er goed aan doen om te bepalen of de statements van IANA en de relevante registers afdoende zijn.

6.4 MTU-problemen

Risico: ondertekende antwoorden die door authoritative nameservers en resolvers worden verstuurd zullen vaker dan traditionele antwoorden groter zijn dan de maximum transmission unit (MTU) [34]. Dit houdt in dat een router tussen de authoritative nameserver en de resolver of de resolver en de client het antwoord moet fragmenteren of weigeren omdat het te groot is voor de uitgaande verbinding [61]. Dit levert problemen op als een (al dan niet verkeerd geconfigureerde) middlebox gefragmenteerde pakketten en Path MTU Discovery (PMTUD) blokkeert, omdat het antwoord dan helemaal niet aankomt. Path MTU Discovery is een techniek waarmee de MTU tussen twee systemen op een netwerk bepaald kan worden [42]. Bij Internet Protocol version 4 (IPv4) kan de router fragmentatie toepassen [61], maar dat is niet mogelijk met Internet Protocol version 6 (IPv6) [54] waardoor PMTUD de enige optie wordt om pakketten zowel betrouwbaar als efficiënt te kunnen versturen.

Systemen die gebruikmaken van load balancing om de capaciteit van nameservers beter te benutten kunnen PMTUD ook breken. NSA en NSB maken gebruik van load balancing. Een situatie waarbij het mis kan gaan is als volgt:

1. Een resolver stuurt een query via een PPPoE-verbinding over IPv6 naar NSA.
2. Eén van de nameservers in het NSA-cluster stuurt het antwoord terug in twee fragmenten van 1500 en 122 bytes.
3. De PPPoE access router aan de kant van de internetprovider gooit het fragment van 1500 bytes weg en stuurt een antwoord in de vorm van een ICMPv6 Packet Too Big bericht. Het fragment was namelijk te groot voor de MTU van de PPPoE-verbinding (standaard 1492 bytes).
4. Het ICMPv6 Packet Too Big bericht komt door load balancing bij de verkeerde nameserver terecht, die het voor hem onbekende bericht weggooit.
5. De resolver ontvangt alleen het fragment van 122 bytes, maar moet het na enige tijd weggooien omdat de rest van het antwoord uitblijft.

Tegenmaatregel: probeer antwoorden zo klein mogelijk te houden en zorg ervoor dat PMTUD en fragmentatie in ieder geval binnen het netwerk van Byte betrouwbaar werkt. De nameservers van Byte hebben momenteel geen ondersteuning voor IPv6, maar wanneer dat wordt ingevoerd moeten deze

path MTU black holes voorkomen worden.

6.5 Zone enumeration

Risico: het gebruik van Next Secure resource records voor authenticated denial of existence staat zone enumeration (ook wel zone walking genoemd) toe. Zone enumeration is het ontdekken van alle resource records in een zone door alle aan elkaar gelinkte NSEC resource records af te gaan [3]. Deze mogelijkheid kan tegenstrijdig zijn met een beveiligingsbeleid dat het inzien van alle resource records door onbevoegden juist verbiedt.

Tegenmaatregel: gebruik hashed authenticated denial of existence. Deze techniek maakt gebruik van NSEC3 resource records. NSEC3 werkt vrijwel hetzelfde als NSEC, met een belangrijk verschil: de 'vorige' en 'volgende' domeinnamen zijn beveiligd met een cryptografische hashfunctie en een willekeurige salt [3]. Hierdoor wordt het voor een aanvaller significant moeilijker om alle resource records één voor één af te gaan, maar kan een DNSSEC-validerende resolver wel controleren of een domeinnaam niet bestaat. Neem bijvoorbeeld de domeinnaam internet.nl:

```
qficn779on7a7huiu5h895lompgcp00o.internet.nl. 3600 IN NSEC3 1 0 5
   4560C528EBC549B6 QFJLVD0DD3C7A765ST8SOM2TNQTPOTS8 A NS SOA MX
   TXT AAAA SSHFP RRSIG DNSKEY NSEC3PARAM CAA
```

Het is aan de hashes niet eenvoudig af te lezen welke domeinnaam de vorige en volgende zijn, maar een validerende resolver kan wel bepalen of een domeinnaam wel of niet bestaat. Het nadeel van deze aanpak is dat de hashes gebruikt kunnen worden voor een offline woordenboekaanval waarmee vaak alsnog veel bestaande domeinnamen geraden kunnen worden. Om hier tegen te beschermen kan PowerDNS geconfigureerd worden voor NSEC3 in *narrow* mode. Hierbij omvat een NSEC3 resource record niet precies de vorige en volgende domeinnaam, maar niet-bestaande domeinnamen alfabetisch net voor en achter de opgevraagde domeinnaam. Deze techniek heet 'minimally covering NSEC records' en wordt ook wel 'DNSSEC white lies' genoemd. Deze methode vereist echter dat de authoritative nameserver elk NSEC3-antwoord voor iedere unieke query *live* ondertekent, en dat kan de prestaties nadelig beïnvloeden waardoor een DDoS-aanval tegen de servers eenvoudiger wordt. Een alternatief is de verbeterde versie NSEC5, maar het specificatiedocument is nog in de conceptfase [10, 6].

6.6 Domeinnaamverhuizingen

Risico: wanneer een registrant zijn domeinnaam wil verhuizen naar een andere DNS-hoster moeten de DNSSEC keys uit veiligheidsoverwegingen vervangen worden. Hierbij kunnen problemen ontstaan waardoor de domeinnaam korte tijd onbeveiligd is of de DNSSEC keten niet meer gevalideerd kan worden, met alle gevolgen van dien.

Tegenmaatregel: maak bij verhuizingen tussen registrars gebruik van EPP key relay. EPP key relay zorgt voor een veilige verhuizing [4]:

1. De nieuwe registrar maakt een zone aan voor de domeinnaam en ondertekent deze met nieuwe DNSSEC keys. De public keys stuurt zij vervolgens met het "keyrelay"EPP-commando en de benodigde verhuiscode naar het register.
2. Het register neemt de hash van de KSK (of CSK) op in de parent zone als DS resource record en stuurt de public keys en de verhuiscode door naar de oude registrar.
3. De oude registrar controleert of de verhuiscode geldig is en plaatst dan de nieuwe public keys als ondertekende DNSKEY resource records in de zone. Hierdoor worden de nieuwe keys opgenomen in de keten.
4. De nieuwe registrar start de verhuizing en wijzigt de nameservers en whois-informatie bij het register.
5. Nadat alle TTLs verlopen zijn verwijdert de nieuwe registrar het oude DS resource record uit de parent zone.

Deze aanpak dekt niet de verhuizingen van domeinnamen waarbij de klant zelf of bij een andere partij de DNS-hosting regelt. In die gevallen zal een veilige verhuizing handmatig moeten plaatsvinden.

6.7 Root KSK rollover

Risico: De KSK van de root zone moet iedere vijf jaar vervangen worden [22]. De eerste root KSK werd op 16 juni 2010 tijdens de eerste Root KSK Ceremony gegenereerd, de tweede op 27 oktober 2016 [19]. Volgens de oorspronkelijke planning zou de root zone voor het eerst ondertekend worden met de nieuwe KSK op 11 oktober 2017, maar omdat ontdekt werd dat veel validating resolvers de nieuwe root KSK nog niet in hun trust store hadden werd de rollover uitgesteld. Als de rollover volgens planning was voortgezet

zouden de clients van deze resolvers ondertekende domeinnamen niet meer kunnen opvragen [14].

De Internet Corporation for Assigned Names and Numbers (ICANN), de nonprofit die IANA beheert, heeft op 1 februari 2018 een conceptplan aangekondigd voor het voortzetten van de rollover, waarin 11 oktober 2018 wordt voorgesteld als nieuwe datum voor de rollover. ICANN verwacht dat zij voor die tijd voldoende beheerders van validating resolvers heeft bereikt [15].

Tegenmaatregel: zorg ervoor dat alle gebruikte resolvers de nieuwe root KSK in de trust store hebben. Dit kan op drie manieren:

1. Via een software-update van de resolver [47]. De nieuwe root KSK is standaard aanwezig in PowerDNS versie 4.0.5 en nieuwer [24].
2. Met een automatische update via RFC 5011 [59].
3. Door handmatige configuratie [47].

7 Implementatieplan

7.1 Keys en hashes

Voordat een zone ondertekend kan worden moet er een private key worden gegenereerd. De grootte van de keys en het gebruikte algoritme is belangrijk om de antwoorden zo klein mogelijk te houden en de overhead van de authoritative nameservers en resolvers tot een minimum te beperken. Daarnaast is het niet geheel onbelangrijk om een algoritme te kiezen dat breed ondersteund wordt, zodat zoveel mogelijk gebruikers kunnen profiteren van de beveiliging die DNSSEC biedt. Voor het gebruikte algoritme zijn er twee soorten beschikbaar: RSA en elliptic curve cryptography (ECC). RSA maakt gebruik van grote priemgetallen en heeft daardoor relatief grote keys nodig. Daarnaast zijn de ondertekeningen relatief groot en vereist het genereren van een ondertekening veel processorkracht. ECC werkt met elliptische krommen in plaats van priemgetallen waardoor ondertekeningen sneller gegenereerd kunnen worden, maar het controleren van die ondertekeningen duurt juist langer [35].

Naast een algoritme voor public key cryptography is er ook een algoritme nodig voor het berekenen van hashes. In plaats van een ondertekening te maken van een compleet resource record wordt namelijk alleen de hash van het resource record ondertekend [31]. De hash moet zo klein mogelijk zijn om

de ondertekening klein te houden, maar toch veilig genoeg om te voorkomen dat iemand een andere public key of resource record kan produceren dat dezelfde hash heeft.

Voor DNSSEC-ondertekeningen kunnen de algoritmes DSA/SHA-1, RSA/SHA-1, RSA/SHA-256, RSA/SHA-512, GOST R 34.10-2001, ECDSA Curve P-256 met SHA-256, ECDSA Curve P-384 met SHA-384, Ed25519 en Ed445 worden gebruikt [18]. Van deze algoritmes is alleen RSA/SHA-1 door de Internet Engineering Task Force (IETF) verplicht gesteld. RSA/SHA-256, RSA/SHA-512, ECDSA Curve P-256 met SHA-256 en ECDSA Curve P-384 met SHA-384 worden aangeraden voor DNSSEC-implementaties, en alle overige algoritmes zijn optioneel [53]. Omdat er een aanval bestaat tegen SHA-1 hashes wordt RSA/SHA-1 nu afgeraden [7]. Op dit moment is de root zone ondertekend met RSA/SHA-256, wat het implementeren van RSA/SHA-256 op alle resolvers dus ook verplicht stelt, omdat zij anders geen enkele zone kunnen valideren.

Uit een onderzoek uit februari 2016 bleek dat DNS-clients bij 39,5 % van de queries gevalideerde antwoorden kregen wanneer de opgevraagde zones ondertekend waren met RSA/SHA-256. Deze antwoorden waren in 98,36 % van de gevallen correct. Dat was respectievelijk 34,7 % en 97,99 % wanneer de zone was ondertekend met ECDSA Curve P-256 met SHA-256. RSA/SHA-256 wordt dus breder ondersteund en kan dus, wanneer geïmplementeerd bij Byte, op dit moment meer clients van ondertekende antwoorden voorzien. Hetzelfde onderzoek stelt echter dat het gebruik van RSA keys de uitrol van DNSSEC op de lange termijn juist in de weg zit vanwege de eerde genoemde nadelen van RSA. Het algoritme GOST R 34.10-2001 is ook geen goede keuze, omdat slechts 9,8 % van alle clients gevalideerde antwoorden krijgen van zones die met dit algoritme zijn ondertekend [13]. De algoritmes Ed25519 en Ed445 worden tevens slecht ondersteund omdat deze pas in februari 2017 zijn gestandaardiseerd voor gebruik met DNSSEC [50].

De beste kandidaat is op dit moment dus ECDSA Curve P-256 met SHA-256. Dit algoritme heeft de kleinste key, maakt zeer snelle ondertekeningen mogelijk, wordt door relatief veel resolvers ondersteund en wordt door de Duitse federale dienst voor informatiebeveiliging (BSI) tot na 2022 veilig geacht, in tegenstelling tot RSA met de huidige standaard 2048-bit keys [56]. Mocht een transitie naar een ander algoritme of grotere keys in de toekomst nodig zijn, dan is dat met een key rollover mogelijk.

7.2 PowerDNS

De authoritative PowerDNS servers van Byte hebben ingebouwde ondersteuning voor DNSSEC. Om PowerDNS antwoorden te laten ondertekenen hoeft de te ondertekenen zone enkel een corresponderende private key in de database te hebben. Omdat de database onversleuteld wordt gerepliceerd naar NSC (in een extern datacenter) kunnen de private keys door derden worden onderschept. Om dit te voorkomen moet de replicatie met Transport Layer Security (TLS) beveiligd worden. TLS voorkomt met cryptografie dat de private keys door onbevoegden ingezien of gemanipuleerd kunnen worden.

Voor authenticated denial of existence kan in PowerDNS het beste gekozen worden voor NSEC3 in *narrow* mode. Hierdoor wordt zone enumeration effectief tegengegaan. Het gebruik van *narrow* mode heeft wel een negatieve invloed op de prestaties van de authoritative nameservers omdat er niet efficiënt gecachet kan worden, maar omdat de nameserver minder vaak de database hoeft aan te spreken, er minder vaak hashberekeningen gedaan hoeven te worden en woordenboekaanvallen niet mogelijk zijn wegen de voordelen op tegen de nadelen.

7.3 Office servers

Byte heeft een paar servers in het datacenter van KPN draaien die gebruikt worden door medewerkers voor het beheer van het platform. Hier draaien ook cronjobs op. Dat zijn taken die automatisch op vooraf geconfigureerde tijden worden uitgevoerd. Deze office servers worden wederom met Puppet automatisch van configuratie voorzien. Op een van deze servers moet een cronjob worden geconfigureerd die periodiek, bijvoorbeeld elk uur, DNSSEC keys voor nieuwe zones aanmaakt en deze in de gerepliceerde PowerDNS database opslaat. Vervolgens moet dezelfde cronjob de public keys versturen naar de parent zones. Daar is nu nog geen ondersteuning voor in de Perl library Byte::DRS, hier moet de library dus op aangepast worden. Met deze aanpassing moeten DS resource records in parent zones kunnen worden toegevoegd en verwijderd via zowel SIDN als RRPproxy.

Een tweede cronjob die moet worden aangemaakt moet de databasetabel bijwerken die bijhoudt welke Top Level Domains (TLDs, zoals .nl) DNSSEC ondersteunen. Dit is belangrijk omdat een domeinnaam alleen beveiligd kan worden als de parent zone het DS record kan opnemen en ondertekenen. Deze cronjob hoeft niet vaak uitgevoerd te worden omdat de DNSSEC-ondersteuning onder TLDs niet zo snel meer toeneemt. Een keer per maand

zou gepast zijn.

Een derde cronjob moet ervoor zorgen dat oude DNSSEC-sleutels en NSEC3 parameters uit de PowerDNS database worden verwijderd, nadat DNSSEC voor een domein is uitgeschakeld. In dat geval is de procedure als volgt:

1. In de domeintabel van de Byte database wordt de dnssec_enabled flag uitgeschakeld. Dit voorkomt dat de domeinnaam opnieuw ondertekend wordt.
2. In dezelfde tabel wordt de waarde last_modified geüpdatet met het huidige tijdstip.
3. Via Byte::DRS wordt de API van de registry aangeroepen zodat het DS-record uit de parent zone verwijderd wordt.
4. De cronjob controleert of het tijdstip in last_modified ten minste twee dagen geleden was en verwijdert dan de oude DNSSEC-sleutel en NSEC3 parameters uit de PowerDNS database.

Stap 1, 2 en 3 kunnen in één keer worden uitgevoerd. Het is belangrijk dat het daadwerkelijk verwijderen van de sleutel en NSEC3 parameters pas na twee dagen gebeurt, omdat PowerDNS dan onmiddelijk stopt met het serveren van de publieke sleutels, ondertekeningen en NSEC3 parameters. Dit kan de validatieketen breken als het DS-record nog in de parent zone of in de cache van een resolver aanwezig is.

7.4 Monitoring

De monitoringsystemen van Byte gebruiken resolvers die niet op DNSSEC valideren. Als er problemen ontstaan met de DNSSEC-ketens van klanten of infrastructuur van Byte zal er dus geen alarm afgaan. Twee mogelijke opties om dit te voorkomen zijn DNSSEC-validatie inschakelen op de resolvers en aparte checks inbouwen in het monitoringsysteem die zelfstandig DNSSEC valideren. Het is vanzelfsprekend duurzamer om DNSSEC ook op de resolvers in te schakelen. Dit kan met een update van de PowerDNS resolvers en een kleine configuratiewijziging. Bij Byte is het belangrijk dat de interne zone ‘internal.’ wordt uitgezonderd van validatie. Deze zone bestaat namelijk niet in het Domain Name System, waardoor de root servers een ondertekend NSEC-antwoord teruggeven, en de resolvers de query niet kunnen beantwoorden. Bij de twee andere interne zones ‘10.in-addr.arpa.’ en ‘168.192.in-addr.arpa.’ is dit niet van toepassing. De zones bestaan namelijk wel in het DNS, maar omdat er geen DNSSEC-keten is vanaf de root zone

tot deze zones is het voor de prestaties van de resolvers en overhead op de root servers verstandig om deze zones ook uit te zonderen van validatie.

7.5 Key rollovers

Het is belangrijk om keys regelmatig te vervangen:

1. Het wordt beschouwd als een goede beveiligingsmaatregel, net zoals het regelmatig veranderen van wachtwoorden.
2. Het voorkomt dat anderen de public keys als onveranderlijk gaan zien en het daardoor statisch gaan configureren.
3. Het oefenen van rollovers zorgt voor een snelle rollover in een noodgeval.

Om key rollovers zo eenvoudig mogelijk te maken moet er een script worden geschreven dat zoveel mogelijk automatiseert. Dit script moet rekening houden met het API limiet van RRPproxy. Die is op dit moment 2,5 commando's per seconde. Tijdens een key rollover moet er één commando per domeinnaam worden uitgevoerd om de DNSSEC data in de parent zone te updaten. De gebruikte methode heet 'Straightforward Rollover in a Single-Type Signing Scheme' en is beschreven in sectie 4.1.3 van RFC 6781. Bij deze methode zijn er vier fasen:

initial: Het DS record van de parent zone verwijst naar de oude DNSKEY. Alle resource records in de zone zijn ondertekend met de oude DNSKEY.

new DNSKEY: Een nieuwe DNSKEY wordt aangemaakt en alle resource records worden met zowel de oude als de nieuwe DNSKEY ondertekend.

DS change: Nadat de TTL van het DNSKEY resource record is verlopen, wordt het DS record in de parent zone gewijzigd.

DNSKEY removal: Nadat het oude DS resource record niet meer door resolvers wordt gecachet kan het oude DNSKEY resource record uit de zone worden verwijderd.

Het nadeel van deze methode is dat elk resource record tijdelijk twee ondertekeningen heeft, waardoor antwoorden van nameservers een stuk groter zijn. Een alternatief is de methode genaamd 'Double-DS Rollover in a Single-Type Signing Scheme'. Hierbij publiceert de parent zone tijdelijk twee DS records en hoeven de nameservers van Byte niet twee DNSKEYS en twee ondertekeningen per resource record te publiceren. De nadelen van deze methode zijn dat de parent het nieuwe DS record niet kan controleren omdat de nieuwe,

ondertekende DNSKEY nog niet gepubliceerd is, en de API van de registry tweemaal per domeinnaam moet worden aangeroepen waardoor een rollover in de praktijk langer duurt. Omdat het belangrijk is dat key rollovers snel gebeuren in het geval de private keys ontoegankelijk of uitgelekt zijn, is gekozen voor de 'Straightforward Rollover in a Single-Type Signing Scheme'.

7.6 Service panel

Om gebruik te kunnen maken van de resource records IPSECKEY, SSHFP, TLSA, CAA en OPENPGPKEY moet het service panel worden aangepast. Hiervoor moeten extra keuzes worden toegevoegd in het "record type"dropdownmenu en moet de Perl-code die deze invoer controleert worden gewijzigd.

8 Conclusie

Het doel van dit onderzoek was een werkende testimplementatie ontwikkelen voor de uitrol van DNSSEC bij Byte. Hiervoor is een kwalitatief onderzoek uitgevoerd naar een mogelijke implementatie.

Uit de resultaten van het onderzoek is gebleken dat een implementatie kan bestaan uit een aantal wijzigingen aan de DNS-infrastructuur en een script dat periodiek uitgevoerd kan worden om nieuwe domeinnamen te ondertekenen. De wijzigingen aan de DNS-infrastructuur waren een upgrade en configuratiewijziging van de authoritative nameservers en de recursive resolvers. Daarnaast moest de databasereplicatie naar het externe datacenter versleuteld worden om te voorkomen dat de DNSSEC private keys in handen van derden zouden vallen.

Het script dat is geschreven om de uitrol van DNSSEC mogelijk te maken heeft uiteindelijk de volgende functies gekregen:

1. Het ondertekenen van zones met het algoritme ECDSA Curve P-256.
2. Het inschakelen van narrow mode NSEC3 processing.
3. Het berekenen van SHA-256 hashes voor DS-records.
4. Het uploaden van public keys en hashes naar de registries.
5. Het verzorgen van een secure delegation indien de nameservers van Byte ook verantwoordelijk zijn voor de parent zone.

6. Het eenvoudig maken van rollovers.

7. Het gecontroleerd verwijderen van DNSSEC-sleutelmateriaal.

Met deze implementatie heeft Byte de mogelijkheid om alle domeinnamen die zij voor klanten en zichzelf in beheer heeft te ondertekenen. Dankzij de incentiveregeling van SIDN kan Byte de implementatie direct gebruiken voor financieel gewin. Tevens hoeven de klanten niet bang te zijn dat zij hun Thuiswinkel Waarborg keurmerk verliezen omdat de domeinnamen van hun webshops niet zijn beveiligd met DNSSEC.

Woordenlijst

application programming interface Een technische koppeling tussen applicatiecomponenten. 9

cache Tijdelijke opslag van data waardoor toekomstige verzoeken sneller kunnen worden verwerkt. 4

child zone Zone die lager staat in de hiërarchie van het Domain Name System (bijvoorbeeld example.com in de parent zone "com". 7

client Computer die gebruik maakt van een dienst die een server aanbiedt. 3

datacenter Gebouw of ruimte dat is ingericht voor het onderbrengen van computersystemen. 9

DHCP-server Server die gebruikmaakt van het Dynamic Host Configuration Protocol om clients automatisch van netwerkconfiguratie te voorzien. 3

DHCPv6-server Server die gebruikmaakt van het Dynamic Host Configuration Protocol for IPv6 om clients automatisch van netwerkconfiguratie te voorzien. 3

domeinnaam Naam dat de administratieve grens van een deel van het Domain Name System aangeeft. 2

hash Uitkomst van een cryptografische functie die de invoer dusdanig bewerkt dat de uitkomst uniek, onomkeerbaar en relatief klein is. 6

hosting Dienst die zorg draagt voor de bereikbaarheid van een online dienst (zoals een website of e-mailaccount). 2

hostname Naam in het Domain Name System van een apparaat op een netwerk. 3

Internet Protocol version 4 Protocol dat gebruikt wordt voor communicatie tussen op het internet aangesloten systemen, maar dat niet meer voldoet door het beperkte aantal IP-adressen. 13

Internet Protocol version 6 Nieuwe versie van het Internet Protocol dat onder andere meer adresruimte biedt dan versie 4. 13

IP-adres Adres dat een computer volgens het Internet Protocol identificeert op een netwerk. 3

IPv6 router advertisement IPv6-bericht dat door een router wordt verstuurd naar alle apparaten op een lokaal netwerk waarmee netwerkconfiguratie wordt ingesteld. 3

man-in-the-middle-attack Aanval waarbij de aanvaller communicatie tussen twee partijen actief manipuleert, meestal om het gebruik van sterke versleuteling te voorkomen zodat meegeluisterd kan worden. 7

maximum transmission unit Grootte van het grootste netwerkpakket dat over een verbinding kan worden getransporteerd. 13

network address translation Techniek waarmee IP-adressen (en vaak ook poortnummers) worden vertaald om twee incompatibele netwerken met elkaar te kunnen verbinden. 5

nonce Een willekeurig getal dat gebruikt wordt voor beveiligingstoepassingen. 5

parent zone Zone die hoger staat in de hiërarchie van het Domain Name System (bijvoorbeeld "com" bij de child zone example.com). 6

query Een verzoek aan een authoritative nameserver of resolver. 3

resource record Een informatie-element in het Domain Name System. 4

root server Nameserver die authoritative is voor de rootzone van het Domain Name System. 4

root zone DNS-zone die bovenaan staat in de hiërarchie. 6

router Apparaat dat verkeer tussen computernetwerken uitwisselt volgens het Internet Protocol. 13

RSA Public key versleutelingsmethode dat afhankelijk is van grote priemgetallen, waardoor meer processorkracht en grotere sleutels en ondertekeningen nodig zijn dan bij elliptic curve cryptography. 6

salt Willekeurige waarde die gebruikt wordt om hashes te beschermen tegen zogenaamde rainbow table attacks. 14

source port randomization Techniek die ervoor zorgt dat de gebruikte TCP- en UDP-poorten van een client willekeurig zijn waardoor DNS cache poisoning deels wordt voorkomen. 5

time to live Tijdslimiet voor het opslaan van data in een cache. 4

TLS-certificaat Digitaal certificaat dat gebruikt wordt om de verbinding tussen een client en een server te beveiligen. 5

whois Protocol waarmee informatie over een domeinnaam of IP-adres opgevraagd kan worden bij het register. 8

Referenties

[1] Inc. Akamai Technologies. *Security Bulletin: DNSSEC Amplification DDoS*. 16 feb 2016. URL: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/dnssec-amplification-ddos-security-bulletin.pdf. (opgehaald op: 19-02-2018).

[2] A. Bolivar et al. *DNSSEC Practice Statement for the Root Zone ZSK operator*. 27 apr 2016. URL: https://www.iana.org/dnssec/dps/zsk-operator/dps-zsk-operator-1532.pdf. (opgehaald op: 13-02-2018).

[3] B. Laurie et al. *DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*. Mrt 2008. URL: https://tools.ietf.org/html/rfc5155. (opgehaald op: 12-02-2018).

[4] H.W. Ribbers et al. *Key Relay Mapping for the Extensible Provisioning Protocol*. Feb 2017. URL: https://tools.ietf.org/html/rfc8063. (opgehaald op: 15-02-2018).

[5] J. Jeong et al. *IPv6 Router Advertisement Options for DNS Configuration*. Nov 2010. URL: https://tools.ietf.org/html/rfc6106. (opgehaald op: 13-02-2018).

[6] J. Vecelak et al. *NSEC5, DNSSEC Authenticated Denial of Existence*. 3 jan 2018. URL: https://datatracker.ietf.org/doc/draft-vcelak-nsec5/. (opgehaald op: 14-02-2018).

[7] M. Stevens et al. *The first collision for full SHA-1*. 23 feb 2017. URL: https://shattered.io/static/shattered.pdf. (opgehaald op: 26-02-2018).

[8] R. Arends et al. *DNS Security Introduction and Requirements*. Mrt 2005. URL: https://tools.ietf.org/html/rfc4033. (opgehaald op: 19-02-2018).

[9] R. Arends et al. *Resource Records for the DNS Security Extensions*. Mrt 2005. URL: https://tools.ietf.org/html/rfc4034. (opgehaald op: 08-02-2018).

[10] S. Goldberg et al. *NSEC5: Provably Preventing DNSSEC Zone Enumeration*. 17 okt 2014. URL: https://www.cs.bu.edu/~goldbe/papers/nsec5.pdf. (opgehaald op: 14-02-2018).

[11] S. Thomson et al. *DNS Extensions to Support IP Version 6*. Okt 2003. URL: https://tools.ietf.org/html/rfc3596. (opgehaald op: 19-02-2018).

[12] M. Andrews. *Negative Caching of DNS Queries (DNS NCACHE)*. Mrt 1998. URL: https://tools.ietf.org/html/rfc2308. (opgehaald op: 19-02-2018).

[13] M. Andzinski. *ECC support in DNS resolvers as seen by RIPE Atlas*. Feb 2016. URL: https://www.dns.pl/dnssec/ecc_support_in_dns_resolvers.pdf. (opgehaald op: 26-02-2018).

[14] Internet Corporation for Assigned Names en Numbers. *KSK Rollover Postponed*. 27 sep 2017. URL: https://www.icann.org/news/announcement-2017-09-27-en. (opgehaald op: 20-02-2018).

[15] Internet Corporation for Assigned Names en Numbers. *Plan for Continuing the Root KSK Rollover*. 1 feb 2018. URL: https://www.icann.org/en/system/files/files/plan-continuing-root-ksk-rollover-01feb18-en.pdf. (opgehaald op: 20-02-2018).

[16] Internet Corporation for Assigned Names en Numbers. *Root Zone Maintainer Agreement (RZMA)*. 28 sep 2016. URL: https://www.icann.org/en/stewardship-implementation/root-zone-maintainer-agreement-rzma. (opgehaald op: 14-02-2018).

[17] Internet Assigned Numbers Authority. *DNSSEC Information*. URL: https://www.iana.org/dnssec. (opgehaald op: 14-02-2018).

[18] Internet Assigned Numbers Authority. *Domain Name System Security (DNSSEC) Algorithm Numbers*. 10 mrt 2017. URL: https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml. (opgehaald op: 22-02-2018).

[19] Internet Assigned Numbers Authority. *Root KSK Ceremonies*. URL: https://www.iana.org/dnssec/ceremonies. (opgehaald op: 14-02-2018).

[20] Internet Assigned Numbers Authority. *Root Servers*. URL: https://www.iana.org/domains/root/servers. (opgehaald op: 14-02-2018).

[21] Internet Assigned Numbers Authority. *Trust Anchors and Keys*. URL: https://www.iana.org/dnssec/files. (opgehaald op: 14-02-2018).

[22] Root Zone KSK Policy Management Authority. *DNSSEC Practice Statement for the Root Zone KSK Operator*. 1 okt 2016. URL: https://www.iana.org/dnssec/dps/ksk-operator/ksk-dps.txt. (opgehaald op: 13-02-2018).

[23] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. *Ontwerpmemorie van toelichting bij wetsontwerp GDI*. 30 aug 2017. URL: https://www.rijksoverheid.nl/documenten/publicaties/2017/08/30/wetsontwerp-generieke-digitale-infrastructuur-gdi. (opgehaald op: 12-02-2018).

[24] PowerDNS.COM BV. *Changelog for PowerDNS Recursor 4.0.5*. 13 jun 2017. URL: https://doc.powerdns.com/recursor/changelog/4.0.html#powerdns-recursor-4-0-5. (opgehaald op: 21-06-2018).

[25] PowerDNS.com BV. *DNSSEC*. URL: https://www.powerdns.com/dnssec.html. (opgehaald op: 22-02-2018).

[26] Internet Systems Consortium. *A Quick Introduction to Response Rate Limiting*. 12 jun 2013. URL: https://kb.isc.org/article/AA-01000/0/A-Quick-Introduction-to-Response-Rate-Limiting.html. (opgehaald op: 09-02-2018).

[27] C.R. Dougherty. *Multiple DNS implementations vulnerable to cache poisoning*. 8 jul 2008. URL: https://www.kb.cert.org/vuls/id/800113. (opgehaald op: 09-02-2018).

[28] R. Droms. *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. Dec 2003. URL: https://tools.ietf.org/html/rfc3646. (opgehaald op: 13-02-2018).

[29] R. Droms. *Dynamic Host Configuration Protocol*. Mrt 1997. URL: https://tools.ietf.org/html/rfc2131. (opgehaald op: 13-02-2018).

[30] P. Savola F. Baker. *Ingress Filtering for Multihomed Networks*. Mrt 2004. URL: https://tools.ietf.org/html/bcp84. (opgehaald op: 20-02-2018).

[31] M. Gieben. *DNSSEC: The Protocol, Deployment, and a Bit of Development*. Jun 2004. URL: http://ipj.dreamhosters.com/wp-content/uploads/issues/2004/ipj07-2.pdf. (opgehaald op: 22-02-2018).

[32] M. Gleason. *The Ephemeral Port Range*. 2001. URL: https://www.ncftp.com/ncftpd/doc/misc/ephemeral_ports.html. (opgehaald op: 13-02-2018).

[33] Key-Systems GmbH. *RRPproxy Gateways & Features*. URL: https://www.rrpproxy.net/API. (opgehaald op: 21-02-2018).

[34] D. Grant. *A Deep Dive Into DNS Packet Sizes: Why Smaller Packet Sizes Keep The Internet Safe*. 4 mrt 2016. URL: https://blog.cloudflare.com/a-deep-dive-into-dns-packet-sizes-why-smaller-packet-sizes-keep-the-internet-safe/. (opgehaald op: 16-02-2018).

[35] K. Hageman. *The Performance of ECC Algorithms in DNSSEC: A Model-based Approach*. 21 okt 2015. URL: https://essay.utwente.nl/68358/1/hageman_MA_EEMCS.pdf. (opgehaald op: 15-02-2018).

[36] S. Hemminger. *[UDP]: Randomize port selection*. 24 aug 2007. URL: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=32c1da70810017a98aa6c431a5494a302b6b9a30. (opgehaald op: 13-02-2018).

[37] C. Hesselman. *Increasing DNS Security and Stability through a Control Plane for Top-level Domain Operators (paper postprint)*. 19 dec 2016. URL: https://www.sidnlabs.nl/downloads/papers-reports/sidnlabs-commag.pdf. (opgehaald op: 21-02-2018).

[38] P. Hoffman. *Cryptographic Algorithm Identifier Allocation for DNSSEC*. Nov 2010. URL: https://tools.ietf.org/html/rfc6014. (opgehaald op: 08-02-2018).

[39] P. Hoffman. *SMTP Service Extension for Secure SMTP over Transport Layer Security*. Feb 2002. URL: https://tools.ietf.org/html/rfc3207. (opgehaald op: 13-02-2018).

[40] S. Hollenbeck. *Extensible Provisioning Protocol (EPP)*. Aug 2009. URL: https://tools.ietf.org/html/rfc5730. (opgehaald op: 14-02-2018).

[41] IANIX. *Major DNSSEC Outages and Validation Failures*. 9 feb 2018. URL: https://ianix.com/pub/dnssec-outages.html. (opgehaald op: 09-02-2018).

[42] S. Deering J. Mogul. *Path MTU Discovery*. Nov 1990. URL: https://tools.ietf.org/html/rfc1191. (opgehaald op: 16-02-2018).

[43] F. Gont M. Larsen. *Recommendations for Transport-Protocol Port Randomization*. Jan 2011. URL: https://tools.ietf.org/html/bcp156. (opgehaald op: 14-02-2018).

[44] P. Mockapetris. *Domain names - concepts and facilities*. Nov 1987. URL: https://tools.ietf.org/html/rfc1034. (opgehaald op: 09-02-2018).

[45] P. Mockapetris. *Domain names - implementation and specification*. Nov 1987. URL: https://tools.ietf.org/html/rfc1035. (opgehaald op: 19-02-2018).

[46] Stichting Internet Domeinregistratie Nederland. *DNSSEC Policy and Practice Statement .nl*. 10 mrt 2016. URL: https://www.sidn.nl/downloads/procedures/DNSSEC%5C%20Policy%5C%20and%5C%20Practice%5C%20Statement%5C%20.nl.pdf. (opgehaald op: 13-02-2018).

[47] Stichting Internet Domeinregistratie Nederland. *Installatie trust anchor voor nieuwe root KSK*. 12 jul 2017. URL: https://www.sidn.nl/a/veilig-internet/installatie-trust-anchor-voor-nieuwe-root-ksk. (opgehaald op: 20-02-2018).

[48] Stichting Internet Domeinregistratie Nederland. *Over SIDN*. URL: https://www.sidn.nl/t/over-sidn. (opgehaald op: 09-02-2018).

[49] Stichting Internet Domeinregistratie Nederland. *SIDN heeft DNSSEC voor .nl-zone succesvol ingevoerd*. 23 aug 2010. URL: https://web.archive.org/web/20110105065607/https://www.sidn.nl/nieuws/nieuwsbericht/article/sidn-heeft-dnssec-voor-nl-zone-succesvol-ingevoerd/. (opgehaald op: 09-02-2018).

[50] R. Edmonds O. Sury. *Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC*. Feb 2017. URL: https://tools.ietf.org/html/rfc8080. (opgehaald op: 25-04-2018).

[51] D. Senie P. Ferguson. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. Mei 2000. URL: https://tools.ietf.org/html/bcp38. (opgehaald op: 09-02-2018).

[52] R. Rasmussen. *Application Layers - The DNSSEC Chicken and Egg Challenge*. 20 dec 2010. URL: https://www.securityweek.com/application-layers-dnssec-chicken-and-egg-challenge. (opgehaald op: 19-02-2018).

[53] S. Rose. *Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status*. Apr 2013. URL: https://tools.ietf.org/html/rfc6944. (opgehaald op: 26-02-2018).

[54] R. Hinden S. Deering. *Internet Protocol, Version 6 (IPv6) Specification*. Jul 2017. URL: https://tools.ietf.org/html/rfc8200. (opgehaald op: 16-02-2018).

[55] V. Shmatikov S. Son. *The Hitchhiker's Guide to DNS Cache Poisoning*. URL: https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf. (opgehaald op: 14-02-2018).

[56] Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. 22 jan 2018. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile. (opgehaald op: 26-02-2018).

[57] Forum Standaardisatie. *Aanpassing functioneel toepassingsgebieden Internet veiligheidstandaarden*. 11 okt 2017. URL: https://www.forumstandaardisatie.nl/sites/bfs/files/FS%5C%20171011.3E%5C%20Forumadvies%5C%20toepassingsgebieden%5C%20IV-standaarden_3.pdf. (opgehaald op: 12-02-2018).

[58] Forum Standaardisatie. *Lijst open standaarden (verplicht)*. URL: https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht. (opgehaald op: 12-02-2018).

[59] M. StJohns. *Automated Updates of DNS Security (DNSSEC) Trust Anchors*. Sep 2007. URL: https://tools.ietf.org/html/rfc5011. (opgehaald op: 20-02-2018).

[60] Internetstiftelsen i Sverige. *DNSSEC key rollover time!* 30 jun 2017. URL: https://www.iis.se/english/news/dnssec-key-rollover-time/. (opgehaald op: 19-02-2018).

[61] Information Sciences Institute of the University of Southern California. *Internet Protocol*. Sep 1981. URL: https://tools.ietf.org/html/rfc791. (opgehaald op: 16-02-2018).

[62] W. Hardaker V. Dukhovni. *SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Se-*

curity (TLS). Okt 2015. URL: https://tools.ietf.org/html/rfc7672. (opgehaald op: 13-02-2018).

[63] A. Veenman. *Deel .nl-namespace plat; SIDN onbereikbaar*. 29 mei 2008. URL: https://www.ispam.nl/archives/1941/hele-nl-namespace-plat-sidn-onbereikbaar. (opgehaald op: 20-03-2018).

[64] Z. Morley Mao Z. Qian. *Off-Path TCP Sequence Number Inference Attack: How Firewall Middleboxes Reduce Security*. URL: http://www.cs.ucr.edu/~zhiyunq/pub/oakland12_TCP_sequence_number_inference.pdf. (opgehaald op: 14-02-2018).