Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

Umsetzung von DNSSEC

Handlungsempfehlungen zur Einrichtung und zum Betrieb der Domain Name Security Extensions

Das Domain-Name-System (DNS) dient der Umsetzung von Domainnamen in IP-Adressen und umgekehrt. Das System bildet in der Praxis die Grundlage für nahezu jegliche Art der Internetkommunikation. Ein Ausfall oder eine Manipulation wirkt sich daher erheblich auf die Funktionsfähigkeit des Internet aus. Das Protokoll weist leider einige Schwächen in Bezug auf die Vertrauenswürdigkeit der übermittelten Daten auf. Dies wurde beispielsweise durch die im Sommer 2008 durch Dan Kaminsky aufgezeigte Designschwäche im DNS-Protokoll erneut deutlich. Dieser Designfehler bewirkt, dass Cache-Poisoning Angriffe (und dadurch weitere Angriffsmethoden) erheblich erleichtert werden. Mit der Protokollerweiterung DNSSEC steht ein Verfahren zur Verfügung, mit dem diese Schwächen beseitigt werden können.

Diese BSI-Veröffentlichung fasst wesentliche Aspekte, die bei der Umsetzung und des anschließenden Betriebs von DNSSEC beachtet werden sollten, zusammen.

1 Grundlagen

1.1 Was ist DNSSEC?

DNSSEC (Domain Name System Security Extensions) ist eine sicherheitsbezogene Erweiterung des DNS-Protokolls und ermöglicht, DNS-Daten digital zu signieren. Die Signatur nutzt Mechanismen einer Public-Key-Infrastructure (PKI) unter Verwendung von asymmetrischen Schlüsseln zur Signierung von Daten. Für jeden, der Daten signieren möchte, wird ein Schlüsselpaar erstellt. Dieses besteht jeweils aus einem privaten (geheimen) und einem öffentlichen Schlüssel. Diese werden so generiert, dass die Echtheit von Daten, die mit einem privaten Schlüssel signiert wurde, mit dem zugehörigen öffentlichen Schlüssel geprüft werden kann (auf die mathematischen Hintergründe soll hier nicht eingegangen werden).

Zur Vereinfachung des Validierungsprozesses können die öffentlichen Schlüssel einer Domainzone (z. B. *bund.de*) auch in der darüber geordneten Zone (z. B. *.de*) abgelegt und dort wiederum signiert werden. Auf diese Weise entsteht eine Vertrauenskette, an deren Spitze die Signatur der Root-Zone steht.

Spezifiziert wird DNSSEC u. a. in folgenden RFCs:

- RFC 4033[1], RFC 4034[2], RFC 4035[3], RFC 5155[4]

1 https://tools.ietf.org/html/rfc4033
2 https://tools.ietf.org/html/rfc4034
3 https://tools.ietf.org/html/rfc4035
4 https://tools.ietf.org/html/rfc5155

Praktische Hinweise zum Betrieb werden darüber hinaus in

- RFC 6781[5]

beschrieben.

DNSSEC stellt sicher, dass die Quelle der DNS-Daten korrekt ist und dass die Daten während der Übertragung nicht modifiziert wurden. Es hilft also sicher zu stellen, dass z. B. die Namensauflösung im DNS korrekt durchgeführt wird und zu einem angefragten Domainnamen die korrekte IP-Adresse zurückgeliefert wird. Auch alle weiteren via DNS verbreiteten Daten (z. B. Mailexchange-Records, Domainkeys/DKIM) können auf diese Weise vor Manipulation geschützt werden.

Stellt ein DNS-Client, der DNSSEC-Signaturen verifizieren kann (ein sogenannter "validierender Resolver") eine Anfrage an einen DNS-Server einer DNSSEC-gesicherten Zone, liefert der DNS-Server nicht nur die angefragten Informationen sondern auch deren Signatur zurück. Der validierende Resolver kann dann mit Hilfe des öffentlichen Schlüssels die Integrität der Daten und die Authentizität des DNS-Servers überprüfen.

1.2 Wer muss DNSSEC unterstützen, damit es funktioniert?

DNSSEC muss sowohl auf Seiten des Anbieters (Domaininhaber, DNS-Serverbetreiber, Domain-Registrar) als auch auf Seite des Kunden (Unternehmen, Endanwender, validierender Resolver bei einem Internet-Service-Provider (ISP)) unterstützt werden. Eine DNSSEC-signierte Zone wird nur von einem validierenden Resolver geprüft, nicht-validierende Resolver würden die DNSSEC-Informationen ignorieren bzw. fragen diese erst gar nicht an. Eine nicht signierte Zone kann grundsätzlich nicht validiert werden.

2 DNSSEC für Domaininhaber

Internetdomains haben heute für Unternehmen branchenübergreifend eine herausragende Bedeutung. In vielen Fällen ist eine ungestörte Erreichbarkeit Voraussetzung für die alltäglichen Geschäftsprozesse. Funktionsstörungen können einen erheblichen Imageschaden selbst dann auslösen, wenn für die eigentliche Geschäftstätigkeit die ständige Erreichbarkeit über das Internet eine untergeordnete Bedeutung hat. Zur sicheren Bereitstellung von Domaindienstleistungen hat das BSI die Handlungsempfehlung „Sichere Bereitstellung von Domaindienstleistungen“[6] herausgegeben.

2.1 Ist ein Schutz meiner Domain mit DNSSEC wichtig?

Insbesondere für Nutzer von geschäftskritischen Domains ist die Signierung der von ihnen verwendeten Domaindaten sehr sinnvoll. Manipulationen der Domaindaten können so verhindert werden, der Kommunikationsweg zum Kunden besser geschützt werden.

2.2 Kümmert sich mein Domainregistrar um die DNSSEC-Signierung?

Sofern der Domainregistrar auch mit der Verwaltung der DNS-Daten beauftragt wurde, ist es Aufgabe des Domainregistrars, sich auch um die Schlüsselerzeugung, Signierung der Zonendaten, Neusignierung vor Ablauf der Signaturgültigkeit sowie den regelmäßigen Schlüsselwechsel zu kümmern. Derzeit bietet jedoch noch nicht jeder Domainregistrar diese Dienstleistung an.

5 https://tools.ietf.org/html/rfc6781
6 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-111.pdf, Erscheinungsdatum 30.01.2015

Sofern Sie die DNS-Server zu ihrer Domain selbst betreiben, können Sie auch die Schlüsselverwaltung und Signierung ihrer Domaindaten selbst übernehmen. Den öffentlichen Teil Ihres Schlüssels veröffentlichen sie dann über ihren Domainregistrar in der zu ihrer jeweiligen Domain gehörenden Top-Level-Domain.

Siehe auch nachfolgendes Kapitel 3, DNSSEC für DNS-Serverbetreiber.

2.3 Welche Abläufe sind wichtig, wenn DNSSEC-Schlüssel vom Domaininhaber verwaltet werden?

Wenn der Kunde die DNSSEC-Schlüssel selbst verwaltet, wird er an Dritte nur den öffentlichen Schlüssel herausgeben. Der Kunde muss dementsprechend seine Zonen selbst signieren und diese dann entweder auf seinen Nameservern veröffentlichen oder die signierten Zonen zur Veröffentlichung an seinen DNS-Serverbetreiber weitergeben. Zusätzlich ist in jedem Fall die Veröffentlichung des öffentlichen DNSSEC-Schlüssels über den Domain-Registrar in der zugehörigen Top-Level-Domain erforderlich.

2.4 Was kann man tun, wenn der aktuelle Domainregistrar DNSSEC nicht unterstützt?

Sofern der Domainregistrar zumindest die Weiterleitung öffentlicher DNSSEC-Schlüssel an die jeweilige Top-Level-Domain (TLD) unterstützt, kann der Betrieb der DNS-Server selbst übernommen werden. Da viele TLD-Betreiber (darunter die DENIC als Betreiber der *.de*-Zone) eine direkte Annahme von DNSSEC-Schlüsselmaterial von Domainhabern nicht unterstützen, bleibt, sofern der aktuelle Domainregistrar auch die Weiterleitung von Schlüsselmaterial nicht anbietet, nur der Wechsel des Domain-Registrars.

2.5 Welchen Anbieter soll ich wählen?

Anbieter von Domaindienstleistungen (Domain-Registrare) unterscheiden sich hinsichtlich der angebotenen Dienstleistungen und Schutzmaßnahmen stark voneinander.

Ein auf die Registrierung vieler Domains spezialisierter Registrar bietet häufig Service mit folgenden Eigenschaften:

- hoch automatisiert
- auf das Massengeschäft ausgerichtet
- Korrespondenz via E-Mail
- automatisierte Vorfallsbearbeitung / TT-System
- TLS-geschützter Zugang zur Domain-Konfiguration
- evtl. geschützte WHOIS-Daten
- evtl. Domain-Transferprotektion

Dem gegenüber haben sich andere Anbieter auf Kunden von Domainnamen mit hohem Geschäftswert (sog. High-Profile-Domains) fokussiert, und bieten häufig Service mit folgenden Eigenschaften:

- Qualitätsservice für Kunden von High-Profile-Domains
- Betrachtung von Domainregistrierungen als kritischer Geschäftsprozess
- Schutz vor Ablauf von Domainregistrierungen
- DNSSEC
- Schutz vor Domain-Hijacking
- Verarbeitung von Veränderungen mit Fokus auf geringe Fehlerquote
- persönliche Kundenbetreuung

- Schutz durch Vorgabe, Änderungen nur schriftlich entgegen zu nehmen
- Echtzeit-Monitoring der DNS-Daten, insbesondere auch von WHOIS-Daten
- Hilfestellung bei juristischen Fragestellungen rund um die Domainregistrierung, missbräuchlicher Nutzung und markenrechtlichen Aspekten

Unternehmen sollten daher einen Registrar wählen, der zu dem von ihnen ermittelten Schutzbedarf passt und entsprechende Dienstleistungen anbietet.

Die kurzfristige Erreichbarkeit eines Ansprechpartners im Unternehmen bei Problemen und Störungen durch den Registrar sollte rund um die Uhr sichergestellt sein. Es sollte mit dem Registrar eine detaillierte Vereinbarung getroffen werden, wer bei Domainänderungen zu informieren ist.

3 DNSSEC für DNS-Serverbetreiber

Zum sicheren Betrieb eines DNS-Servers hat das BSI eine separate Empfehlung „Sichere Bereitstellung von DNS-Diensten“[7] veröffentlicht, in der wesentliche Aspekte beschrieben werden, die für einen sicheren und zuverlässigen Betrieb von DNS-Servern umgesetzt sein sollten. Nachfolgend ein Auszug aus dieser Empfehlung:

3.1 Netzanbindung

Da mit dem Betrieb von DNSSEC das Risiko steigt, dass die eigenen Server im Rahmen eines DDoS-Reflektion-Angriffs[8] missbraucht werden, sollten die DNS-Server in separaten Netzsegmenten betrieben werden und über eine breitbandige, robuste und redundante Netzanbindung verfügen.

Zum Schutz vor Angriffen auf DNS-Server unter Ausnutzung von gespooften IP-Adressen sollten gespoofte DNS-Anfragen bereits an den Netzwerk-Grenzen blockiert werden. Siehe hierzu auch IETF BCP-38 / RFC 2827, „Network Ingress Filtering“[9].

Um die korrekte Funktion des DNS-Dienstes in Verbindung mit DNSSEC zu gewährleisten, muss sichergestellt sein, dass auch EDNS-Pakete (DNS-UDP-Pakete > 512 Byte, siehe IETF RFC 2671, „Extension Mechanisms for DNS“[10]) von gegebenenfalls zwischengeschalteten Routern und Paketfiltern korrekt weitergeleitet werden.

3.2 Hardware

Die zum Betrieb der DNS-Server verwendete Hardware sollte ausreichend überdimensioniert sein, um Verkehrsspitzen bewältigen zu können. Die Hardware sollte dediziert ausschließlich für den Betrieb eines DNS-Servers vorgesehen werden und keine weiteren unzugehörigen Dienste beheimaten.

Zur Gewährleistung einer hohen Ausfallsicherheit sollte auf eine ausreichende Hardware-Redundanz (mindestens zwei getrennte DNS-Server) geachtet werden. Durch Realisierung einer räumlichen Trennung und ggf. Nutzung von Anycast-Adressierung kann die Ausfallsicherheit weiter erhöht werden.

3.3 Software

Bei der Auswahl eines geeigneten DNS-Server Produkts (Software) sollte darauf geachtet werden, dass sich das Produkt bereits in der Praxis ausreichend bewährt hat. Weiterhin sollte das Produkt die RFC-Standards zu DNS, darunter

7 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-055.pdf, Erscheinungsdatum 02.04.2013
8 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/anwender/dienste/BSI-CS_096.pdf, Erscheinungsdatum 05.02.2014
9 https://tools.ietf.org/html/rfc2827
10 https://tools.ietf.org/html/rfc2671

- IETF RFC 1034, „Domain Names – Concepts and Facilities“[11]
- IETF RFC 1035, „Domain Names – Implementation and Specification“[12]
- IETF RFC 2181, „Clarifications to the DNS Specification“[13]
- IETF RFC 2671, „Extension Mechanisms for DNS“[14]

erfüllen. Insbesondere sollte auch DNSSEC (s. u.) durch das Produkt vollständig unterstützt werden.

DNS-Server sollten während des Betriebs regelmäßig auf die Aktualität der eingesetzten Software sowie auf die Existenz bekannter Schwachstellen und Sicherheitsverletzungen kontrolliert werden. Geeignete Meldekanäle für Schwachstellen (z. B. entsprechende Mailinglisten) sollten fortwährend überwacht werden. In der Vergangenheit sind mehrfach sicherheitskritische Schwachstellen bei DNS-Server Produkten bekannt geworden, die unter anderem zur Abschaltung des DNS-Dienstes ausgenutzt werden konnten.

3.4 Konfiguration

3.4.1 Trennung von autoritativen[15] und rekursiven DNS-Servern

Die DNS-Server Infrastruktur zur Bereitstellung von autoritativen Domain-Antworten sowie die DNS-Server Infrastruktur zur rekursiven Auflösung von DNS-Einträgen (DNS-Resolver) sollten voneinander getrennt betrieben werden, da sich die Funktionsweisen und daraus resultierend auch die Absicherungsmechanismen grundlegend unterscheiden.

3.4.2 DNS-Resolver

DNSSEC

Die automatische Validierung von DNSSEC-Signaturen anderer Zonen sollte aktiviert sein. Siehe hierzu auch IETF RFC 6781, „DNSSEC Operational Practices, Version 2“[16]

Schutz vor Spoofing / Reduzierung des Missbrauchrisikos für Reflection / Amplification-Angriffe

Zum besseren Schutz vor gespooften DNS-Anfragen sollten DNS-Resolver nicht offen erreichbar („Open Resolver“) betrieben, sondern die Erreichbarkeit auf den eigenen Kundenkreis beschränkt werden (siehe auch BSI-Veröffentlichung zur Cyber-Sicherheit „Zunahme von DDoS-Angriffen durch DNS-Reflection“[17]). Solche Angriffe sollten erkannt und entsprechende Gegenmaßnahmen (vgl. Kapitel 3.7 Notfallvorsorge) ergriffen werden.

Weitere Informationen hierzu auch in IETF RFC 5358, „Preventing Use of Recursive Nameservers in Reflector Attacks“[18].

Schutz vor DNS-Cache Poisoning

Um die Robustheit des Servers gegenüber DNS-Cache-Poisoning Angriffen zu erhöhen, sollte die Port-Randomisierung aktiviert sein.

Die Verkehrsmenge sollte regelmäßig beobachtet werden (siehe auch Monitoring, weiter unten), um Cache-Poisoning Angriffe frühzeitig zu entdecken. Insbesondere bei breitbandig angebunden DNS-Resolvern ist eine Cache-Poisoning Attacke trotz aktivierter Port-Randomisierung weiterhin möglich.

11 https://tools.ietf.org/html/rfc1034
12 https://tools.ietf.org/html/rfc1035
13 https://tools.ietf.org/html/rfc2181
14 https://tools.ietf.org/html/rfc2671
15 Für Domainzonen verantwortliche DNS-Server
16 https://tools.ietf.org/html/rfc6781
17 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/angriffsmethoden/BSI-CS_042.pdf
18 https://tools.ietf.org/html/rfc5358

Zur Risikoreduzierung sollten außerdem Obergrenzen für die Haltezeit von zwischengepufferten Daten (DNS-Cache) festgelegt werden.

Die Validierung von DNSSEC (s. u.) sollte aktiviert sein. In der Anfangsphase sollte die DNSSEC-Validierung überwacht und Validierungsfehlern nachgegangen werden.

3.4.3 Autoritative Server

Signierung und regelmäßige Validierung eigener Zonen

Selbst betriebene DNS-Zonen sollten mit DNSSEC-Signaturen versehen werden und die Gültigkeit regelmäßig überprüft werden.

Es gibt verschiedene Möglichkeiten eine Zone zu signieren. Grundsätzlich sollte unterschieden werden, ob die Zone auf dem Nameserver signiert wird oder im Vorhinein erzeugt, signiert und erst anschließend auf den Nameserver übertragen wird. Eine Signierung auf dem Nameserver setzt das Vorhandensein des privaten Schlüssels auf dem Nameserver voraus, was aus Sicherheitsgründen ggf. nicht erwünscht ist.

DNSSEC wird inzwischen von einer Vielzahl von Softwareprodukten sowohl aus dem freien (Open-Source) als auch aus dem kommerziellen Bereich zur Verfügung.

Zu beachten ist, dass bei einer Erneuerung des Schlüssels (Key-Rollover-Prozedur) unter Einhaltung wichtiger zeitlicher Abstände (siehe RFC 6781, „DNSSEC Operational Practices, Version 2“[19]) die Publizierung des öffentlichen Schlüsselteils in der übergeordnete Zone erfolgen muss. Die Entfernung des bisherigen öffentlichen Schlüssels darf erst dann erfolgen, wenn sichergestellt ist, dass der neue Schlüssel bereits publiziert ist und sich auch bereits auf alle DNS-Server verbreitet hat.

Umgang mit rekursiven Anfragen

Autoritative Server sollten rekursive Anfragen ablehnen und ausschließlich Anfragen nach eigenen Zonen akzeptieren.

Dynamische Updates

Dynamische Updates nach IETF RFC 2136, „Dynamic Updates in the Domain Name System (DNS UPDATE)“[20], sollten deaktiviert oder per TSIG (IETF RFC 2845, „Secret Key Transaction Authentication for DNS“[21]) abgesichert sein, um Manipulationen auszuschließen.

Zonentransfers

Zonentransfers synchronisieren die Domain-Informationen zwischen einem Primary-DNS-Server und einem oder mehreren Secondary DNS-Servern. Zonentransfers sollten nur zur Synchronisation zwischen den autoritativen Servern (Primary, Secondarys) einer Domain erlaubt sein und über TSIG (Transaction Signatures) abgesichert sein.

Verbergen der DNS-Server-Version

Die Version des verwendeten DNS-Servers kann einem Angreifer wertvolle Informationen liefern. Aus diesem Grund sollte die Versionsnummer verborgen werden. Diese Maßnahme erhöht zwar nicht das Sicherheitsniveau des DNS-Servers, erschwert einem Angreifer jedoch die Informationsbeschaffung.

Rechtevergabe

Prozesse von DNS-Servern sollten nur mit den minimal notwendigen Rechten (insbesondere nicht mit Root-Rechten) ausgestattet werden, um die potenziellen Auswirkungen im Fall eines erfolgreichen Angriffs auf den Prozess gering zu halten.

19 https://tools.ietf.org/html/rfc6781
20 https://tools.ietf.org/html/rfc2136
21 https://tools.ietf.org/html/rfc2845

3.5 Monitoring / Überwachung der DNS-Server

Der Betrieb der DNS-Server sollte geeignet überwacht werden. Insbesondere sollten die Logdateien der DNS-Server sowie des unterliegenden Betriebssystems regelmäßig überprüft und ausgewertet werden.

Bei Auffälligkeiten z. B. in Bezug auf die Auslastung (CPU-Last, I/O-Last) sollten umgehend weitere Analysen durchgeführt werden. Unregelmäßigkeiten, deren Feststellung hilfreich zur Eingrenzung der Ursache oder zur Einleitung von Gegenmaßnahmen ist, sind beispielsweise:

- Eine Häufung von Anfragen von bestimmten Quellen
- Eine Häufung von Anfragen bezüglicher bestimmter Ressource-Records
- Eine Häufung von Anfragen bezüglich nicht existierender Ressource-Records
- Eine Häufung von unerlaubten rekursiven Anfragen
- Eine Häufung von (fehlgeschlagenen) Zonentransfers
- Eine Häufung von DNSSEC-Validierungsfehlern

Weiterhin sollte eine regelmäßige Überprüfung/Verifizierung der DNS-Server-Konfiguration durchgeführt werden. Bei Feststellung von Unregelmäßigkeiten sollten die Ursache festgestellt und ggf. entsprechende Gegenmaßnahmen ergriffen werden.

3.6 Wie wird der DS-Eintrag (Hash-Wert des öffentlichen Schlüssels) publiziert?

Der Betreiber der übergeordneten Zone, in der die DS-Records publiziert werden sollen, muss eine entsprechende Möglichkeit zur Verfügung stellen. Falls die übergeordnete Zone eine TLD-Zone ist, fällt diese Zuständigkeit in den Bereich der betreibenden Registry. In den meisten Fällen wird die Möglichkeit, DS-Records für Domains zu publizieren, von den Registries zur existierenden Registry-Registrar-Schnittstelle hinzugefügt. Daher ist es abhängig von der Registry, auf welche Art und Weise DS-Records publiziert werden. Im Regelfall erfolgt die Übermittlung über den mit der Verwaltung der Domain beauftragen Domain-Registrar.

3.7 Notfallvorsorge

Zu einem sicheren Betrieb gehören weitere regelmäßig durchzuführende Maßnahmen der Notfallvorsorge.

Der Ausfall eines DNS-Servers kann sich gravierend auf die Funktionsfähigkeit des Internets auswirken. Funktioniert die Namensauflösung bei Kunden nicht mehr, wird dies in der Regel schnell öffentlich bekannt werden, was bei regelmäßigen oder längeren Ausfällen einen Imageschaden zur Folge haben kann. Gleiches gilt, sofern DNS-Server für Angriffe auf Fremdsysteme missbraucht werden.

Es ist daher ein Konzept zu entwerfen, wie im Falle eines Ausfalls oder Missbrauchs die daraus resultierenden Folgen minimiert werden können. Beim Festlegen der Aktivitäten sollten folgende Aspekte berücksichtigt werden:

- Die Notfallplanung für DNS-Server muss in den existierenden Notfallplan integriert werden.
- Ein Systemausfall kann zu Datenverlusten führen. Daher ist ein Datensicherungskonzept für die Zonendateien zu erstellen.
- Neben dem Notfallplan für den DNS-Server muss auch für das darunterliegende Betriebssystem ein Notfallplan existieren.
- War die Störung das Resultat eines Angriffs, muss die Schwachstelle behoben und dokumentiert werden.
- Es muss ein Wiederanlaufplan erstellt werden, damit das oder die IT-System(e) wieder geregelt hochgefahren werden kann/können.
- Der Notfallplan sollte auf seine Durchführbarkeit getestet werden.

Zu den Maßnahmen, die im Rahmen eines Notfallvorsorgekonzepts vorgesehen werden könnten, zählen:

- Einschränkung von Anfragen (z. B. Bei Missbrauch der Servers)
- Reaktive Filterung von Angriffsverkehr (z. B. Bei Denial-of-Service Angriffen)
- Fluten (Flushen) des DNS-Caches (z. B. bei DNS-Cache-Poisoning Angriffen)
- z. B. Aktivierung eines Hot-Spare / Cold Spare (z. B. bei DoS-Angriffen)
- Nutzung einer alternativen Hardwareplattform
- Nutzung einer alternativen Software (z. B. bei bekannt werden einer Schwachstelle)

3.8 DNS-Monitoring und Testtools

Kostenfrei zugängliche DNS-Monitoring und Testtools stehen unter anderem auf nachfolgenden Webseiten zur Verfügung:

- http://dns.measurement-factory.com/tools/dsc (DSC: A DNS STATISTICS COLLECTOR)
- http://nast.denic.de (Nameserver Predelegation Check Webinterface)
- http://dnscheck.iis.se (Test your DNS-server and find errors)
- https://www.dns-oarc.net/oarc/services/dnsentropy (Web-based DNS Randomness Test)
- https://www.dns-oarc.net/oarc/services/replysizetest (OARC's DNS Reply Size Test Server)
- http://dnsviz.net (A DNS visualization tool)

4 DNSSEC für Anwender

4.1 Kommen Internetnutzer (oder deren Rechner) direkt mit DNSSEC in Berührung?

Üblicherweise erfolgt der Internetzugang eines Anwender-Betriebssystems über einen Zugangsrouter, der einen DNS-Proxy zur Verfügung stellt und die Anfragen an die vom Zugangsprovider mitgeteilten DNS-Server weiterleitet. Die Validierung von DNSSEC-signierten DNS-Daten findet in diesem Fall nicht auf dem Rechner eines Internetnutzers statt, sondern im Idealfall bereits auf den DNS-Servern des Zugangsproviders.

Eine fehlerhafte DNSSEC-Validierung stellt sich für den Anwender als Nicht-Erreichbarkeit der Domain dar. Versierte Internetnutzer können stattdessen einen eigenen DNS-Resolver auf ihren Endgeräten installieren und die DNS-Antworten so eigenständig validieren.

5 DNSSEC für Domain-Registrare

Zur sicheren Bereitstellung von Domaindienstleistungen hat das BSI die Handlungsempfehlung „Sichere Bereitstellung von Domaindienstleistungen“[22] herausgegeben. In Bezug auf DNSSEC empfiehlt das BSI, zumindest die Entgegennahme und Verarbeitung von DNSSEC-Schlüsselmaterial (im DNSKEY- oder DS-Format) zu unterstützen.

Sofern für den Kunden auch der Betrieb von DNS-Servern als Dienstleistung angeboten wird, sollte auch die Signierung der Zonen und der Betrieb der hierzu erforderlichen DNSSEC-Infrastruktur zum angebotenen Portfolio gehören. Diese umfasst:

- Schlüsselimport / -export
- Import / -export von Zonendateien
- Validierung signierter Zonen
- Festlegung von Verfahren und Mechanismen für den Schlüsselwechsel (Key-Rollover) und eine Abschaltung von DNSSEC im Notfall.

22 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-111.pdf, Erscheinungsdatum 30.01.2015

Das beim Registrar eingesetzte Provisionierungssystem sollte eine leichte Verarbeitung auch aller weiteren Resource-Record (RR)-Typen (z. B. TLSA-Einträge zur Nutzung von DANE) ermöglichen.

6 Auf DNSSEC aufsetzende Sicherheitstechnologien

6.1 DNS-Based Authentication of Named Entities (DANE), RFC 6698

Die DANE-Erweiterung ermöglicht die Veröffentlichung von TLS-Zertifikaten im DNS. Dies ermöglicht eine Verbesserung des Schutzniveaus sowohl beim Austausch von E-Mails als auch beim gesicherten Aufruf von Webseiten.

6.1.1 Vertraulichkeit des E-Mail-Verkehrs

Zur Bereitstellung sicherer E-Mail-Dienstleistungen hat das BSI die Handlungsempfehlung „E-Mail-Sicherheit“[23] herausgegeben.

Darin wird auch die Nutzung von DANE empfohlen:
„Das für die verschlüsselte Annahme von E-Mails verwendete Zertifikat oder dessen Hashwert sollte wie im RFC 6698 DNS-Based Authentication of Named Entities (DANE)[24] beschrieben per TLSA-Eintrag im DNS veröffentlicht und per DNSSEC signiert werden.“

6.1.2 Gesicherter Abruf von Webseiten

Beim mit TLS-gesicherten Abruf von Webseiten muss sichergestellt sein, dass der antwortende Server legitimiert ist, die gewünschte Seite auszuliefern. Der Browser prüft daher, ob die Domain im vom Server angebotenen Zertifikat eingetragen ist. Weiterhin wird geprüft, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt wurde.

Die Wirksamkeit der TLS-Sicherung hängt somit davon ab, dass keine der im Browser mit ihrem Zertifikatsanker hinterlegten Zertifizierungsstellen kompromittiert wurde. Mittels DANE ist es möglich, das gültige Zertifikat zu einer Domain zusätzlich im DNS zu hinterlegen, oder alternativ eine Aussage darüber zu treffen, welche CA als Vertrauensanker zulässig ist. Die Nutzung von DANE kann also das derzeitige Schutzniveau erheblich verbessern.

6.1.3 Ausblick

Neben der Hinterlegung von TLS-Zertifikaten wird aktuell an einem Standard zur Hinterlegung des Open PGP-Schlüssels gearbeitet. Dies stellt eine sinnvolle Ergänzung zur Nutzung von Open PGP Schlüsselservern dar.

Auch die Hinterlegung von S/MIME-Zertifikaten wird aktuell in der Fachwelt diskutiert.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

23 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-098.pdf, Erscheinungsdatum 03.06.2014
24 https://tools.ietf.org/html/rfc6698