Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: INTERNET-DIENSTLEISTER und UNTERNEHMEN

Sichere Bereitstellung von DNS-Diensten

Handlungsempfehlungen für Internet-Service-Provider (ISP) und große Unternehmen

Das Domain-Name-System (DNS) dient der Umsetzung von Domainnamen in IP-Adressen und umgekehrt. DNS-Server zählen zu den Kernkomponenten der Internet-Infrastruktur. Ein Ausfall oder eine Manipulation eines DNS-Servers kann sich gravierend auf die Funktionsfähigkeit des Internets auswirken. Eine sorgfältige Konfiguration und Absicherung von DNS-Servern ist daher unerlässlich. Diese BSI-Veröffentlichung zur Cyber-Sicherheit beschreibt wesentliche Aspekte, die für einen sicheren und zuverlässigen Betrieb von DNS-Servern umgesetzt sein sollten.

1 Netzanbindung

DNS-Server sollten wie andere, für den Betrieb des Internets kritische Systeme 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“.

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

2 Hardware

Die zum Betrieb der DNS-Server verwendete Hardware sollte ausreichend überdimensioniert sein, um Verkehrsspitzen bewältigen zu können.

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.

Die Hardware sollte dediziert ausschließlich für den Betrieb eines DNS-Servers vorgesehen werden und keine weiteren unzugehörigen Dienste beheimaten.

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

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

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.

4 Konfiguration

4.1 Trennung von autoritativen[1] 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.

4.2 DNS-Resolver

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“[2]). Solche Angriffe sollten erkannt und entsprechende Gegenmaßnahmen ergriffen werden (vgl. Monitoring, weiter unten).

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

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.

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

1 Für Domainzonen verantwortliche DNS-Server
2 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/angriffsmethoden/BSI-CS_042.pdf

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

4.3 Autoritative Server

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)“, sollten deaktiviert oder per TSIG (IETF RFC 2845, „Secret Key Transaction Authentication for DNS“) 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, Secondaries) einer Domain erlaubt sein und über TSIG (Transaction Signatures) abgesichert sein.

4.4 DNSSEC (Domain Name System Security Extensions)

Das DNS-Protokoll weist konzeptionelle Schwachstellen auf. Dies wurde beispielsweise durch die im Sommer 2008 aufgezeigte Designschwäche im DNS-Protokoll erneut deutlich. Dieser Designfehler bewirkt, dass Cache-Poisoning Angriffe (und dadurch weitere Angriffsmethoden) erheblich erleichtert werden. Zur Verbesserung des DNS-Protokolls und zur Erhöhung des künftigen Schutzniveaus sollte DNSSEC umgesetzt werden. Dies umfasst sowohl die

- Signierung und regelmäßige Validierung eigener Zonen als auch eine
- automatische Validierung von DNSSEC-Signaturen anderer Zonen.

Siehe hierzu auch

- IETF RFC 6781, „DNSSEC Operational Practices, Version 2“

4.5 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.

4.6 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.

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 Resource-Records
- Eine Häufung von Anfragen bezüglich nicht existierender Resource-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 (siehe auch Kapitel „Notfallvorsorge“, weiter unten).

6 Zusammenarbeit / Abuse-Handling

Provider sollten untereinander zusammenarbeiten und Auffälligkeiten gegenseitig melden. In Fällen, in denen eigene Server in DNS-Reflection Angriffe eingebunden sind, sollte die Bereitschaft zur Hilfe bei der Aufklärung des Sachverhaltes selbstverständlich sein.

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)
- Andere Hardware
- Andere Software (z. B. bei bekannt werden einer Schwachstelle)

8 Weitere Maßnahmen

Die in BSI-Grundschutz M 4.237 („Sichere Grundkonfiguration eines IT-Systems“) beschriebenen Maßnahmen sollten umgesetzt sein.

Eine ausreichende physische Sicherheit der DNS-Server ist zu gewährleisten. Siehe hierzu u. a.:

- BSI-Grundschutz M 1.58, „Technische und organisatorische Vorgaben für Serverräume“
- BSI-Grundschutz M 2.17, „Zutrittsregelung und -kontrolle“

Weitere Hinweise zur Absicherung von DNS-Systemen finden sich im IT-Grundschutzbaustein B 5.18 "DNS-Server" sowie in den Dokumenten „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)" aus den BSI-Standards zur Internet-Sicherheit.

9 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)

Diese BSI-Empfehlung ist unter Mitwirkung der als Partner der Allianz für Cyber-Sicherheit registrierten Internet-Service-Provider 1&1 Internet AG, Deutsche Telekom und Vodafone entstanden.

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.