



APP.3.6 DNS-Server

1. Beschreibung

1.1. Einleitung

Domain Name System (DNS) ist ein Netzdienst, der dazu eingesetzt wird, Hostnamen von IT-Systemen in IP-Adressen umzuwandeln. DNS kann mit einem Telefonbuch verglichen werden, das Namen nicht in Telefonnummern, sondern in IP-Adressen auflöst. Üblicherweise wird über DNS zu einem Hostnamen die entsprechende IP-Adresse gesucht (Vorwärtsauflösung). Ist hingegen die IP-Adresse bekannt und der Hostname wird gesucht, wird dies als Rückwärtsauflösung bezeichnet.

Welche Hostnamen zu welchen IP-Adressen gehören, wird im Domain-Namensraum verwaltet. Dieser ist hierarchisch aufgebaut und wird von DNS-Servern zur Verfügung gestellt. Die Bezeichnung DNS-Server steht im eigentlichen Sinne für die verwendete Software, wird jedoch meist auch als Synonym für das IT-System benutzt, auf dem diese Software betrieben wird.

DNS-Server verwalten den Domain-Namensraum im Internet, werden aber auch häufig im internen Netz einer Institution eingesetzt. Auf den IT-Systemen der Benutzenden sind standardmäßig sogenannte Resolver installiert. Über den Resolver werden die Anfragen an DNS-Server gestellt. Als Antwort liefern die DNS-Server Informationen über den Domain-Namensraum zurück.

DNS-Server können nach ihren Aufgaben unterschieden werden. Dabei gibt es grundsätzlich zwei verschiedenen Typen: Advertising DNS-Server und Resolving DNS-Server. Advertising DNS-Server sind üblicherweise dafür zuständig, Anfragen aus dem Internet zu verarbeiten. Resolving DNS-Server hingegen verarbeiten Anfragen aus dem internen Netz einer Institution.

Der Ausfall eines DNS-Servers kann sich gravierend auf den Betrieb einer IT-Infrastruktur auswirken. Dabei ist nicht das ausgefallene DNS-System an sich problematisch, sondern die DNS-basierten Dienste, die daraus eingeschränkt werden. Unter Umständen sind Webserver oder E-Mail-Server nicht mehr erreichbar oder die Fernwartung funktioniert nicht mehr. Da DNS von sehr vielen Netzanwendungen benötigt wird, müssen laut Spezifikation (RFC 1034) mindestens zwei autoritative DNS-Server (Advertising DNS-Server) für jede Zone betrieben werden.

1.2. Zielsetzung

In diesem Baustein werden die für einen DNS-Server spezifischen Gefährdungen und die sich daraus ergebenden Anforderungen für einen sicheren Einsatz beschrieben.

1.3. Abgrenzung und Modellierung

Der Baustein APP.3.6 *DNS-Server* ist auf jeden im Informationsverbund eingesetzten DNS-Server anzuwenden.

Der vorliegende Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn eine Institution DNS-Server einsetzt. Der Fokus liegt dabei auf der Verfügbarkeit von DNS-Servern und der Integrität der übertragenen Informationen. Außerdem werden Probleme behandelt, die auftreten können, wenn DNS-Server eingesetzt werden.

Allgemeine und betriebssystemspezifische Aspekte eines Servers sind nicht Gegenstand dieses Bausteins. Diese werden im Baustein SYS1.1 *Allgemeiner Server* und in den entsprechenden betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme* behandelt, z. B. SYS.1.3 *Server unter Linux und Unix* oder SYS.1.2.3 *Windows Server*.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.3.6 *DNS-Server* von besonderer Bedeutung.

2.1. Ausfall des DNS-Servers

Fällt ein DNS-Server aus, kann der gesamte IT-Betrieb davon betroffen sein. Da Clients und andere Server der Institution dann nicht mehr in der Lage sind, interne und externe Adressen auf Basis der Hostnamen aufzulösen, können keine Datenverbindungen mehr aufgebaut werden. Auch externe IT-Systeme, z. B. von mobilen Mitarbeitenden, der Kundschaft sowie Geschäftspartnern und Geschäftspartnerinnen, können nicht auf die Server der Institution zugreifen. Dadurch sind in der Regel essenzielle Geschäftsprozesse gestört.

2.2. Unzureichende Leitungskapazitäten

Reichen die Leitungskapazitäten für einen DNS-Server nicht aus, können sich die Zugriffszeiten auf interne und externe Dienste erhöhen. Dadurch sind diese eventuell nur eingeschränkt oder gar nicht mehr nutzbar. Auch kann der DNS-Server dann leichter durch einen Denial-of-Service-(DoS)-Angriff überlastet werden.

2.3. Fehlende oder unzureichende Planung des DNS-Einsatzes

Fehler in der Planung stellen sich oft als besonders schwerwiegend heraus, da leicht flächendeckende Sicherheitslücken geschaffen werden können. Wird der DNS-Einsatz nicht oder nur unzureichend geplant, kann dies zu Problemen und Sicherheitslücken im laufenden Betrieb führen. Sind beispielsweise die Firewall-Regeln, die den DNS-Verkehr steuern, zu freizügig definiert, kann dies unter Umständen einen Angriff zur Folge haben. Sind die Regeln jedoch zu restriktiv formuliert, können legitime Clients keine Anfragen an die DNS-Server stellen und werden beeinträchtigt, wenn sie etwa Dienste wie E-Mail oder FTP benutzen.

2.4. Fehlerhafte Domain-Informationen

Selbst wenn der DNS-Einsatz sorgfältig geplant und somit alle sicherheitsrelevanten Punkte berücksichtigt wurden, ist das nicht ausreichend, wenn semantisch sowie syntaktisch fehlerhafte Domain-Informationen erstellt werden. Dies gilt beispielsweise dann, wenn einem Hostnamen eine falsche IP-Adresse zugeordnet wird, Daten fehlen, nicht erlaubte Zeichen verwendet werden oder die

Vorwärts- und Rückwärtsauflösung inkonsistent sind. Enthalten Domain-Informationen Fehler, funktionieren Dienste, die diese Informationen benutzen, aufgrund der Falschinformationen nur eingeschränkt.

2.5. Fehlerhafte Konfiguration eines DNS-Servers

Sicherheitskritische Standardeinstellungen, selbst konfigurierte sicherheitskritische Einstellungen oder fehlerhafte Konfigurationen können dazu führen, dass ein DNS-Server nicht ordnungsgemäß funktioniert. Ist beispielsweise ein Resolving DNS-Server so konfiguriert, dass er rekursive Anfragen uneingeschränkt entgegennimmt, also sowohl aus dem internen Datennetz als auch aus dem Internet, kann aufgrund der erhöhten Last die Verfügbarkeit des Servers stark beeinträchtigt sein. Zusätzlich könnte er dadurch anfällig für DNS-Reflection-Angriffe werden.

Ebenso besteht bei fehlerhaft konfigurierten DNS-Servern die Gefahr, dass die Zonentransfers nicht auf berechtigte DNS-Server beschränkt sind. Damit kann jeder Host, der die Möglichkeit hat, eine Anfrage an die DNS-Server zu stellen, die gesamten Domain-Informationen dieser Server auslesen. Die so gewonnenen Daten können spätere Angriffe erleichtern.

2.6. DNS-Manipulation

Mit einem DNS-Cache-Poisoning-Angriff wird das Ziel verfolgt, dass das angegriffene IT-System falsche Zuordnungen von IP-Adressen und Namen speichert. Dabei wird ausgenutzt, dass DNS-Server erhaltene Domain-Informationen für einen gewissen Zeitraum im Cache zwischenspeichern. So können sich gefälschte Daten weiträumig verbreiten. Werden dann entsprechende Anfragen an den manipulierten DNS-Server gestellt, liefert dieser als Antwort die gefälschten Daten. Das IT-System, das diese Antwort empfängt, speichert diese zwischen und sein Cache ist somit ebenfalls „vergiftet“. Die gespeicherten Daten haben eine definierte Haltbarkeit (Time-To-Live, TTL). Wird der Resolving DNS-Server nach einer manipulierten Adresse gefragt, so wird er erst dann wieder einen anderen DNS-Server anfragen, wenn die Haltbarkeit abgelaufen ist. So können sich manipulierte DNS-Informationen lange halten, obwohl sie auf dem ursprünglich angegriffenen DNS-Server bereits wieder korrigiert sind. Gelingt es Angreifenden beispielsweise, die Namensauflösung für eine Domain zu übernehmen, indem sie die Einträge so manipulieren, dass ihre DNS-Server befragt werden, sind alle Subdomains automatisch mitbetroffen. DNS-Cache-Poisoning-Angriffe werden oft mit dem Ziel geführt, Anfragen auf bösartige Server umzuleiten.

2.7. DNS-Hijacking

DNS-Hijacking ist eine Angriffsmethode, die verwendet wird, um die Kommunikation zwischen Advertising DNS-Servern und Resolvern über das IT-System der Angreifenden zu leiten. Den Angreifenden ist es mit dieser Man-in-the-Middle-Attacke möglich, die Kommunikation zwischen den Servern abzuhören und aufzuzeichnen. Die weitaus größere Gefahr besteht jedoch darin, dass bei einem erfolgreichen Angriff jeglicher Datenverkehr zwischen den beiden IT-Systemen beliebig verändert werden kann. Wird nach einem erfolgreichen DNS-Hijacking-Angriff vom Resolver eines Clients eine Anfrage an einen DNS-Server gesendet, können Angreifende beispielsweise die Zuordnung von Namen und IP-Adresse ändern. DNS-Hijacking lässt sich auch mit anderen Angriffen kombinieren, zum Beispiel mit Phishing.

2.8. DNS-DoS

Bei einem DoS-Angriff auf einen DNS-Server werden so viele Anfragen an ihn gesendet, dass die Netzverbindung zum DNS-Server bzw. der DNS-Server selbst überlastet wird. In der Regel werden die Anfragen über Botnetze versendet, um die notwendige Datenrate zu erreichen. Ein auf diese Weise überlasteter DNS-Server kann keine legitimen Anfragen mehr beantworten.

2.9. DNS-Reflection

Bei einem DNS-Reflection-Angriff handelt es sich um einen DoS-Angriff, bei dem nicht der DNS-Server, an den die Anfragen gestellt werden, das Ziel ist, sondern das IT-System, das die Antworten empfängt. Dabei wird ausgenutzt, dass bestimmte Anfragen eine verhältnismäßig große Antwortdatenmenge erzeugen. Es ist dabei möglich, einen Verstärkungsfaktor von 100 und mehr zu erreichen. Das bedeutet, dass die Antwort, gemessen in Bytes, mindestens einhundert Mal größer ist als die Anfrage. Durch die Anzahl und Größe der Antworten wird die Netzbandbreite bzw. das empfangende IT-System selbst über seine Leistungskapazität hinaus überlastet. Somit kann jede beliebige technische IT-Komponente das Angriffsziel sein. DNS-Reflection-Angriffe werden durch Open Resolver begünstigt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.6 *DNS-Server* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Zentrale Verwaltung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.3.6.A1 Planung des DNS-Einsatzes (B)

Der Einsatz von DNS-Servern MUSS sorgfältig geplant werden. Es MUSS zuerst festgelegt werden, wie der Netzdienst DNS aufgebaut werden soll. Es MUSS festgelegt werden, welche Domain-Informationen schützenswert sind. Es MUSS geplant werden, wie DNS-Server in das Netz des Informationsverbunds eingebunden werden sollen. Die getroffenen Entscheidungen MÜSSEN geeignet dokumentiert werden.

APP.3.6.A2 Einsatz redundanter DNS-Server (B)

Advertising DNS-Server MÜSSEN redundant ausgelegt werden. Für jeden Advertising DNS-Server MUSS es mindestens einen zusätzlichen Secondary DNS-Server geben.

APP.3.6.A3 Verwendung von separaten DNS-Servern für interne und externe Anfragen (B)

Advertising DNS-Server und Resolving DNS-Server MÜSSEN serverseitig getrennt sein. Die Resolver der internen IT-Systeme DÜRFEN NUR die internen Resolving DNS-Server verwenden.

APP.3.6.A4 Sichere Grundkonfiguration eines DNS-Servers (B)

Ein Resolving DNS-Server MUSS so konfiguriert werden, dass er ausschließlich Anfragen aus dem internen Netz akzeptiert. Wenn ein Resolving DNS-Server Anfragen versendet, MUSS er zufällige

Source Ports benutzen. Sind DNS-Server bekannt, die falsche Domain-Informationen liefern, MUSS der Resolving DNS-Server daran gehindert werden, Anfragen dorthin zu senden. Ein Advertising DNS-Server MUSS so konfiguriert werden, dass er Anfragen aus dem Internet immer iterativ behandelt.

Es MUSS sichergestellt werden, dass DNS-Zonentransfers zwischen Primary und Secondary DNS-Servern funktionieren. Zonentransfers MÜSSEN so konfiguriert werden, dass diese nur zwischen Primary und Secondary DNS-Servern möglich sind. Zonentransfers MÜSSEN auf bestimmte IP-Adressen beschränkt werden. Die Version des verwendeten DNS-Server-Produktes MUSS verborgen werden.

APP.3.6.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.6.A6 Absicherung von dynamischen DNS-Updates (B)

Es MUSS sichergestellt werden, dass nur legitimierte IT-Systeme Domain-Informationen ändern dürfen. Es MUSS festgelegt werden, welche Domain-Informationen die IT-Systeme ändern dürfen.

APP.3.6.A7 Überwachung von DNS-Servern (B)

DNS-Server MÜSSEN laufend überwacht werden. Es MUSS überwacht werden, wie ausgelastet die DNS-Server sind, um rechtzeitig die Leistungskapazität der Hardware anpassen zu können. DNS-Server MÜSSEN so konfiguriert werden, dass mindestens die folgenden sicherheitsrelevanten Ereignisse protokolliert werden:

- Anzahl der DNS-Anfragen,
- Anzahl der Fehler bei DNS-Anfragen,
- EDNS-Fehler (EDNS - Extension Mechanisms for DNS),
- auslaufende Zonen sowie
- fehlgeschlagene Zonentransfers.

APP.3.6.A8 Verwaltung von Domainnamen (B) [Zentrale Verwaltung]

Es MUSS sichergestellt sein, dass die Registrierungen für alle Domains, die von einer Institution benutzt werden, regelmäßig und rechtzeitig verlängert werden. Eine Person MUSS bestimmt werden, die dafür zuständig ist, die Internet-Domainnamen zu verwalten. Falls Dienstleistende mit der Domainverwaltung beauftragt werden, MUSS darauf geachtet werden, dass die Institution die Kontrolle über die Domains behält.

APP.3.6.A9 Erstellen eines Notfallplans für DNS-Server (B)

Ein Notfallplan für DNS-Server MUSS erstellt werden. Der Notfallplan für DNS-Server MUSS in die bereits vorhandenen Notfallpläne der Institution integriert werden. Im Notfallplan für DNS-Server MUSS ein Datensicherungskonzept für die Zonen- und Konfigurationsdateien beschrieben sein. Das Datensicherungskonzept für die Zonen- und Konfigurationsdateien MUSS in das existierende Datensicherungskonzept der Institution integriert werden. Der Notfallplan für DNS-Server MUSS einen Wiederanlaufplan für alle DNS-Server im Informationsverbund enthalten.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.3.6.A10 Auswahl eines geeigneten DNS-Server-Produktes (S)

Wird ein DNS-Server-Produkt beschafft, dann SOLLTE darauf geachtet werden, dass es sich in der Praxis ausreichend bewährt hat. Das DNS-Server-Produkt SOLLTE die aktuellen RFC-Standards

unterstützen. Das DNS-Server-Produkt SOLLTE die Zuständigen dabei unterstützen, syntaktisch korrekte Master Files zu erstellen.

APP.3.6.A11 Ausreichende Dimensionierung der DNS-Server (S)

Die Hardware des DNS-Servers SOLLTE ausreichend dimensioniert sein. Die Hardware des DNS-Servers SOLLTE ausschließlich für den Betrieb dieses DNS-Servers benutzt werden. Die Netzanbindungen sämtlicher DNS-Server im Informationsverbund SOLLTEN ausreichend bemessen sein.

APP.3.6.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.6.A13 Einschränkung der Sichtbarkeit von Domain-Informationen (S)

Der Namensraum eines Informationsverbunds SOLLTE in einen öffentlichen und einen institutionsinternen Bereich aufgeteilt werden. Im öffentlichen Teil SOLLTEN nur solche Domain-Informationen enthalten sein, die von Diensten benötigt werden, die von extern erreichbar sein sollen. IT-Systeme im internen Netz SOLLTEN selbst dann keinen von außen auflösbaren DNS-Namen erhalten, wenn sie eine öffentliche IP-Adresse besitzen.

APP.3.6.A14 Platzierung der Nameserver (S)

Primary und Secondary Advertising DNS-Server SOLLTEN in verschiedenen Netzsegmenten platziert werden.

APP.3.6.A15 Auswertung der Logdaten (S)

Die Logdateien des DNS-Servers SOLLTEN regelmäßig überprüft werden. Die Logdateien des DNS-Servers SOLLTEN regelmäßig ausgewertet werden. Mindestens die folgenden sicherheitsrelevanten Ereignisse SOLLTEN ausgewertet werden:

- Anzahl der DNS-Anfragen,
- Anzahl der Fehler bei DNS-Anfragen,
- EDNS-Fehler,
- auslaufende Zonen,
- fehlgeschlagene Zonentransfers sowie
- Veränderungen im Verhältnis von Fehlern zu DNS-Anfragen.

APP.3.6.A16 Integration eines DNS-Servers in eine "P-A-P"-Struktur (S)

Die DNS-Server SOLLTEN in eine „Paketfilter - Application-Level-Gateway - Paketfilter“- (P-A-P)-Struktur integriert werden (siehe auch NET.1.1 *Netzarchitektur und -design*). Der Advertising DNS-Server SOLLTE in diesem Fall in einer demilitarisierten Zone (DMZ) des äußeren Paketfilters angesiedelt sein. Der Resolving DNS-Server SOLLTE in einer DMZ des inneren Paketfilters aufgestellt sein.

APP.3.6.A17 Einsatz von DNSSEC (S)

Die DNS-Protokollerweiterung DNSSEC SOLLTE sowohl auf Resolving DNS-Servern als auch auf Advertising DNS-Servern aktiviert werden. Die dabei verwendeten Schlüssel Key-Signing-Keys (KSK) und Zone-Signing-Keys (ZSK) SOLLTEN regelmäßig gewechselt werden.

APP.3.6.A18 Erweiterte Absicherung von Zonentransfers (S)

Um Zonentransfers stärker abzusichern, SOLLTEN zusätzlich Transaction Signatures (TSIG) eingesetzt werden.

APP.3.6.A19 Aussonderung von DNS-Servern (S)

Der DNS-Server SOLLTE sowohl aus dem Domain-Namensraum als auch aus dem Netzwerk gelöscht werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.3.6.A20 Prüfung des Notfallplans auf Durchführbarkeit (H)

Es SOLLTE regelmäßig überprüft werden, ob der Notfallplan für DNS-Server durchführbar ist.

APP.3.6.A21 Hidden Master (H)

Um Angriffe auf den primären Advertising DNS-Server zu erschweren, SOLLTE eine sogenannte Hidden-Master-Anordnung vorgenommen werden.

APP.3.6.A22 Anbindung der DNS-Server über unterschiedliche Provider (H)

Extern erreichbare DNS-Server SOLLTEN über unterschiedliche Provider angebunden werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld DNS veröffentlicht:

- BSI-Veröffentlichung zur Cyber-Sicherheit BSI-CS 055: „Sichere Bereitstellung von DNS-Diensten: Handlungsempfehlungen für Internet-Service-Provider (ISP) und große Unternehmen“
- BSI-Veröffentlichung zur Cyber-Sicherheit BSI-CS 121: „Umsetzung von DNSSEC: Handlungsempfehlungen zur Einrichtung und zum Betrieb der Domain Name Security Extensions“
- Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-81-2 „Secure Domain Name System (DNS) - Deployment Guide“ Empfehlungen zum Einsatz von DNS.

Im Request for Comments (RFC) bietet der RFC 1034 „Domain Names - Concepts and Facilities“ weiterführende Informationen zu DNS.