|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "DNS-Server"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300052 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "DNS-Server" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc82460173)

[Dokumentenhistorie 3](#_Toc82460174)

[Inhaltsverzeichnis 4](#_Toc82460175)

[Allgemeine Festlegungen 6](#_Toc82460176)

[Ziel / Zweck 6](#_Toc82460177)

[Geltungsbereich 6](#_Toc82460178)

[Zuständigkeiten 7](#_Toc82460179)

[Genehmigungs- und Änderungsverfahren 7](#_Toc82460180)

[Aufbau des Dokuments 7](#_Toc82460181)

[Sicherheitsrichtlinie „DNS-Server" 8](#_Toc82460182)

[Basismaßnahmen 8](#_Toc82460183)

[Planung des DNS-Einsatzes (APP.3.6.A1) 8](#_Toc82460184)

[Einsatz redundanter DNS-Server (APP.3.6.A2) 8](#_Toc82460185)

[Verwendung von separaten DNS-Servern für interne und externe Anfragen (APP.3.6.A3) 8](#_Toc82460186)

[Sichere Grundkonfiguration eines DNS-Servers (APP.3.6.A4) 8](#_Toc82460187)

[Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (APP.3.6.A5) 9](#_Toc82460188)

[Absicherung von dynamischen DNS-Updates (APP.3.6.A6) 9](#_Toc82460189)

[Überwachung von DNS-Servern (APP.3.6.A7) 9](#_Toc82460190)

[Verwaltung von Domainnamen (APP.3.6.A8) 9](#_Toc82460191)

[Erstellen eines Notfallplans für DNS-Server (APP.3.6.A9) 9](#_Toc82460192)

[Standardmaßnahmen 9](#_Toc82460193)

[Auswahl eines geeigneten DNS-Server-Produktes (APP.3.6.A10) 10](#_Toc82460194)

[Ausreichende Dimensionierung der DNS-Server (APP.3.6.A11) 10](#_Toc82460195)

[Schulung der Verantwortlichen (APP.3.6.A12) 10](#_Toc82460196)

[Einschränkung der Sichtbarkeit von Domain-Informationen (APP.3.6.A13) 10](#_Toc82460197)

[Platzierung der Nameserver (APP.3.6.A14) 10](#_Toc82460198)

[Auswertung der Logdaten (APP.3.6.A15) 10](#_Toc82460199)

[Integration eines DNS-Servers in eine "P-A-P"-Struktur (APP.3.6.A16) 10](#_Toc82460200)

[Einsatz von DNSSEC (APP.3.6.A17) 11](#_Toc82460201)

[Erweiterte Absicherung von DNS Zonentransfers (APP.3.6.A18) 11](#_Toc82460202)

[Aussonderung von DNS-Servern (APP.3.6.A19) 11](#_Toc82460203)

[Maßnahmen bei erhöhtem Schutzbedarf 11](#_Toc82460204)

[Prüfung des Notfallplans auf Durchführbarkeit (APP.3.6.A20 - A) 11](#_Toc82460205)

[Hidden-Master (APP.3.6.A21 - CIA) 11](#_Toc82460206)

[Anbindung der DNS-Server über unterschiedliche Provider (APP.3.6.A22 - IA) 11](#_Toc82460207)

[Vorausschauende Identifizierung bösartiger Hosts (APP.3.6.bd.A1 - CIA) 12](#_Toc82460208)

# Allgemeine Festlegungen

## Ziel / Zweck

Domain Name System (DNS) ist ein Netzdienst, der dazu eingesetzt wird, Hostnamen von IT-Systemen in IP-Adressen umzuwandeln. 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. DNS kann mit einem Telefonbuch verglichen werden, das Namen nicht in Telefonnummern, sondern in IP-Adressen auflöst. Welche Namen zu welchen IP-Adressen gehören, wird im Domain-Namensraum verwaltet. Dieser ist hierarchisch aufgebaut und wird von DNS-Servern zur Verfügung gestellt. DNS-Server verwalten den Domain-Namensraum im Internet, werden aber auch im internen Netz der <Institution> eingesetzt. Auf den IT-Systemen (DNS-Clients) sind standardmäßig sogenannte Resolver installiert. Darüber werden die Anfragen an DNS-Server gestellt. Als Antwort liefern diese Informationen über den Domain-Namensraum zurück. Die Bezeichnung DNS-Server steht im eigentlichen Sinne für die verwendete Software, wird jedoch meist auch als Synonym für das IT-System selbst benutzt, auf dem die DNS-Software betrieben wird.

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 der Institution.

Ein Ausfall eines DNS-Servers wirkt sich gravierend auf den Betrieb der IT-Infrastruktur aus. Dabei ist nicht direkt das ausgefallene DNS-System problematisch, sondern die daraus resultierende Einschränkung DNS-basierter Dienste. Unter Umständen sind Webserver oder E-Mail-Server oder die komplette SaaS-Lösung der <Institution> nicht mehr erreichbar. Da DNS von sehr vielen Netzanwendungen benötigt wird, müssen laut Spezifikation (RFC 1034) mindestens zwei autoritative DNS-Server (Advertising DNS-Server) für jede DNS-Zone betrieben werden.

In dieser Sicherheitsrichtlinie werden die für einen DNS-Server spezifischen Anforderungen für einen sicheren Betrieb definiert. Die Anforderungen der Sicherheitsrichtlinie beachten hierbei die Vorgaben des BSI Bausteines APP.3.6 „DNS-Server".

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „DNS-Server“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „DNS-Server"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

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

Eine funktionierende Auflösung des öffentlichen und internen Namensraumes der <Institution> ist eine Grundvoraussetzung für viele Anwendungen und damit für einen reibungslosen Betrieb. Es ist aus diesem Grund eine sorgfältige Planung des DNS-Server sicherzustellen. Im Rahmen der Planung ist zunächst festzulegen, wie der Netzdienst DNS aufgebaut werden soll und welche Domain-Informationen schützenswert sind. Es ist ebenfalls zu planen, wie DNS-Server in die Netzinfrastruktur der <Institution> eingebunden werden sollen. Ein weiterer Aspekt, welcher bei der Planung zu berücksichtigen ist, die Erkennung von DNS-Tunnel und wie diese verhindert bzw. begegnet werden. Die getroffenen Entscheidungen sind zu dokumentieren.

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

Selbst betriebene bzw. genutzte Advertising DNS-Server (externe Anfragen) der <Institution> müssen redundant ausgelegt werden. Hieraus ableitend, muss für jeden Advertising DNS-Server mindestens ein zusätzlicher Secondary-DNS-Server betrieben werden. Sofern durch die <Institution> eigene öffentlich erreichbare DNS-Server betrieben werden, sollte der Primary-DNS Server als Hidden-Primary konfiguriert werden. Hierzu ist sich mit dem ISP bzgl. der Möglichkeiten bei der Umsetzung abzustimmen.

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

Advertising DNS-Server (externe Anfragen) und Resolving DNS-Server (interne Anfragen) sind serverseitig zu trennen. Die Resolver der internen IT-Systeme dürfen nur die internen Resolving DNS-Server der <Institution> verwenden, um Namen aufzulösen.

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

Ein Resolving DNS-Server der <Institution> ist so zu konfigurieren, dass der DNS-Server ausschließlich Anfragen aus dem internen Netz der <Institution> akzeptiert. Der Resolving DNS-Server versendet Anfragen via zufällig gewählten Source Ports. Sind der <Institution> DNS-Server bekannt, die falsche Domain-Informationen liefern, ist der Resolving DNS-Server der <Institution> daran zu hindern, Anfragen an diese DNS-Server zu senden. Der Advertising DNS-Server ist so zu konfigurieren, dass er Anfragen aus dem Internet immer iterativ behandelt.

Seitens der <Institution> ist sicherzustellen, dass DNS-Zonentransfers nur zwischen freigegebene Primary- und Secondary-DNS-Server funktionieren. Um Zonentransfers vor einen unerlaubten Zonen-Walk abzusichern, muss der Zonentransfer (Primary und Secondary DNS-Servern) auf deren dedizierten IP-Adressen beschränkt werden. Die Version des verwendeten DNS-Server-Produktes ist vor den Nutzern zu verbergen. Des Weiteren ist sicherzustellen, dass der DNS Server nicht mit Systemrechten betrieben wird.

### Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (APP.3.6.A5)

Die Verantwortlichen für DNS informierten sich regelmäßig bei verschiedenen Quellen über neu bekannt gewordene Schwachstellen zum eingesetzten DNS-Server-Produkt und spielen, sofern erforderlich, werden sicherheitsrelevante Updates zeitnah eingespielt. Vorab wird auf einem Testsystem überprüft, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Solange keine Patches bei bekannten Schwachstellen verfügbar sind, werden andere geeignete Maßnahmen getroffen, um die DNS-Server der <Institution> zu schützen. Bevor ein Patch eingespielt wird, werden die Zonen- und Konfigurationsdateien gesichert.

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

Um dynamische DNS Updates sicher nutzen zu können, dürfen nur legitimierte IT-Systeme der <Institution> Domain-Informationen ändern. Es ist ebenfalls festzulegen, welche Domain-Informationen die IT-Systeme ändern dürfen.

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

Um DNS-Server reibungslos zu betreiben und eventuelle Störungen oder Anomalien festzustellen, werden diese laufend überwacht und sind geeignete Schwellwerte zu hinterlegen. Auch wird überwacht, wie ausgelastet die DNS-Server sind, um rechtzeitig die Leistungskapazität der Hardware anpassen zu können. Darüber hinaus werden alle sicherheitsrelevanten Ereignisse an DNS-Servern geeignet protokolliert.

### Verwaltung von Domainnamen (APP.3.6.A8)

Es ist sichergestellt, dass die Registrierungen für alle Domains, die von der <Institution> verwaltet werden, regelmäßig und rechtzeitig verlängert werden. Es sind Verantwortliche bestimmt, die dafür verantwortlich sind, die Internet-Domainnamen zu verwalten. Sofern ein Dienstleister mit der Verwaltung der Domain beauftragt wird, wird darauf geachtet, dass die <Institution> die Kontrolle über die Domains behält.

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

Es ist sicherzustellen, dass ein aktueller Notfallplan für die internen und externen DNS-Server der <Institution> besteht. Der Notfallplan ist in die bereits vorhandenen Notfallpläne der <Institution> zu integrieren. Im Rahmen der Erstellung des Notfallplanes muss ein Konzept zur Datensicherung der Zonen- und Konfigurationsdateien entwickelt und etabliert in das existierende Datensicherungskonzept der <Institution> integriert werden. Neben der Wiederherstellung muss der der Notfallplan auch einen Wiederanlaufplan für DNS-Server enthalten.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

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

Wird ein DNS-Server-Produkt beschafft, ist darauf zu achten, dass sich mit diesem Produkt alle Betriebs- und Sicherheitsanforderungen geeignet umsetzen lassen. In die Bewertung, welches Produkt beschafft wird, sollte auch die Praxistauglichkeit mit einfliessen und das alle aktuellen RFC-Standards unterstützen werden. Das ausgewählte DNS-Server Produkt sollte den Verantwortlichen dabei unterstützen, syntaktisch korrekte Master Files zu erstellen. Außerdem sollte für das von der <Institution> ausgewählte DNS-Server-Produkt genügend geschultes Personal vorhanden sein.

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

Da die Hardware (Memory, CPU etc.) eines DNS-Servers die Leistung des gesamten Systems beeinflusst, sollte sie ausreichend dimensioniert sein. Auch sollte die Hardware ausschließlich für den Betrieb eines DNS-Servers benutzt werden. Ebenso ist die Netzanbindung der DNS-Server ausreichend zu bemessen.

### Schulung der Verantwortlichen (APP.3.6.A12)

Durch Schulungen der Verantwortlichen für den DNS ist sicherzustellen, dass die Verantwortlichen mit den einzelnen Konfigurationsmöglichkeiten und sicherheitsrelevanten Aspekten der DNS-Server vertraut sind und im Rahmen eines Security Incident schnell unterstützen können.

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

Der Namensraum der <Institution> sind in einen öffentlichen und einen internen Bereich aufzuteilen. Im öffentlichen Teil sind nur solche Domain-Informationen enthalten, die von Diensten der <Institution> benötigt werden bzw. die von Extern erreichbar sein sollen. IT-Systeme im internen Netz erhalten selbst dann keinen von außen auflösbaren DNS-Namen, wenn sie eine öffentliche IP-Adresse besitzen.

### Platzierung der Nameserver (APP.3.6.A14)

Primary und Secondary Advertising DNS-Server sind in unterschiedlichen Netzsegmenten zu integrieren.

### Auswertung der Logdaten (APP.3.6.A15)

Die Logdateien der von der <Institution> betriebenen DNS-Servers sowie des genutzten Betriebssystems sind regelmäßig zu überprüfen und auszuwerten.

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

Die DNS-Server sollten in eine "Paketfilter – Application-Level-Gateway – Paketfilter" (P-A-P) Struktur integriert werden. Der Advertising DNS-Server ist in diesem Fall in einer demilitarisierten Zone (DMZ) des äußeren Paketfilters angesiedelt. Der Resolving DNS-Server ist in einer DMZ des inneren Paketfilters aufgestellt.

### Einsatz von DNSSEC (APP.3.6.A17)

Sofern die DNS-Protokollerweiterung DNSSEC eingesetzt wird, wird sowohl auf Resolving DNS-Servern als auch auf Advertising DNS-Servern diese Funktion aktiviert. Die dabei verwendeten Schlüssel Key-Signing-Keys (KSK) und Zone-Signing-Key (ZSK) sind regelmäßig zu erneuern.

### Erweiterte Absicherung von DNS Zonentransfers (APP.3.6.A18)

Sofern durch den DNS-Server hohe Anforderungen an die Vertraulichkeit und Verfügbarkeit sichergestellt werden müssen, sollte der DNS Zonentransfer mittels Transaction Signature (TSIG) stärker abgesichert werden.

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

Wird ein DNS-Server ausgesondert, werden alle Speichermedien des Servers sicher gelöscht. Außerdem wird der DNS-Server sowohl aus dem Namensraum der Domain als auch aus dem Netzverbund der <Institution> gelöscht.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Prüfung des Notfallplans auf Durchführbarkeit (APP.3.6.A20 - A)

Es sollte seitens der <Institution> regelmäßig überprüft werden, ob der Notfallplan in der aktuellen Version durchführbar ist.

### Hidden-Master (APP.3.6.A21 - CIA)

Um Angriffe auf den primären Advertising DNS-Server der <Institution> zu erschweren, sollte eine Hidden-Master-DNS-Server Anordnung etabliert werden.

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

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

### Vorausschauende Identifizierung bösartiger Hosts (APP.3.6.bd.A1 - CIA)

Durch die Aggregation und Analyse von DNS-bezogenen Informationen soll eine automatisierte Erkennung von Anomalien realisiert werden. Hierdurch soll es möglich sein, verdächtige Domain-Verkehrsspitzen, die für die Angriffsaktivität charakteristisch sind, zu erkennen und dem C2-Verkehr frühzeitig entgegenzuwirken.