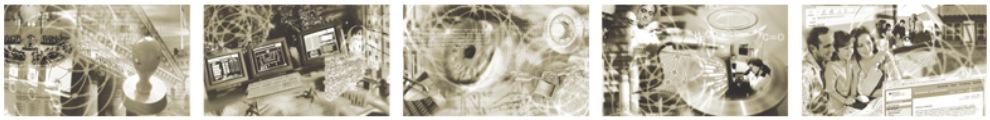
Bundesamt
für Sicherheit in der
Informationstechnik



# Absicherung eines Servers (ISi-Server)

BSI-Leitlinie zur Internet-Sicherheit (ISi-L)

**Vervielfältigung und Verbreitung**

Bitte beachten Sie, dass das Werk einschließlich aller Teile urheberrechtlich geschützt ist.

Erlaubt sind Vervielfältigung und Verbreitung zu nicht-kommerziellen Zwecken, insbesondere zu Zwecken der Ausbildung, Schulung, Information oder hausinternen Bekanntmachung, sofern sie unter Hinweis auf die ISi-Reihe des BSI als Quelle erfolgen.

Dies ist ein Werk der ISi-Reihe. Ein vollständiges Verzeichnis der erschienenen Bände finden Sie auf den Internet-Seiten des BSI.

http://www.bsi.bund.de oder http://www.isi-reihe.de

Bundesamt für Sicherheit in der Informationstechnik
ISi-Projektgruppe
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: isi@bsi.bund.de
Internet: http://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2013

# Inhaltsverzeichnis

1 Leitlinie zur Absicherung eines Servers....4
1.1 Management Summary....4
1.2 Einführung und Überblick....5
1.3 Wesentliche Ergebnisse der Gefährdungsanalyse....6
1.3.1 Vertraulichkeit....6
1.3.2 Integrität....6
1.3.3 Verfügbarkeit....7
1.4 Wesentliche Empfehlungen....8
1.4.1 Sichere Grundarchitektur....8
1.4.2 Grundarchitektur der Infrastruktur mit virtualisierten Komponenten....11
1.5 Fazit....11
2 Literaturverzeichnis....13

# 1 Leitlinie zur Absicherung eines Servers

Die IT-Infrastruktur einer Institution setzt sich aus unterschiedlichen Komponenten zusammen, die über ein Netz miteinander verbunden sind. Grundpfeiler dieser Infrastruktur bilden Server, die u. a. Webinhalte anbieten, den E-Mail-Verkehr regeln oder Informationen in Datenbanken speichern und abrufbar machen.

Die Verfügbarkeit von Servern ist für einen reibungslosen Betrieb essenziell. Aber auch die Vertraulichkeit und die Integrität der verarbeiteten Daten müssen sichergestellt werden. Die Studie *Absicherung eines Servers* [ISi-Server] nimmt sich diesen Themen an und behandelt die grundlegende Absicherung eines Servers, ohne dabei auf bestimmte Anwendungen einzugehen. Die Absicherung von Web- und E-Mail-Servern wird in den Studien [ISi-Web-Server] und [ISi-Mail-Server] behandelt.

## 1.1 Management Summary

Institutionen sind von einer funktionierenden Informationstechnik (IT) abhängig. Dazu zählen nicht nur Arbeitsplatz-PCs, sondern auch Server, die Basisdienste für das Rechnernetz bereitstellen, E-Mail-Austausch ermöglichen, Datenbanken oder Druckerdienste anbieten und vieles mehr.

Angreifer können erheblichen Schaden anrichten, wenn sie es schaffen, die Verfügbarkeit von Servern zu stören oder in Server einzudringen, um dort Daten abzugreifen (Angriff auf die Vertraulichkeit) oder zu manipulieren (Angriff auf die Integrität). Die Verfügbarkeit von Servern kann auch durch technische Defekte bedroht sein, wie den Ausfall von Festplatten oder der Netzverbindung. Server haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Organisation. Daher muss darauf geachtet werden, dass Server nicht durch Schwachstellen in Betriebssystemen und Anwendungen oder durch fehlerhafte Konfiguration solchen Gefährdungen ausgesetzt werden.

Um Server und deren Dienste vor Angriffen und Ausfällen zu schützen, ist die Absicherung sowohl des Betriebssystems als auch der darauf installierten Dienste von entscheidender Bedeutung. Die Studie „ISi-Server“ empfiehlt dazu eine sichere Grundarchitektur, die auf dem Minimalprinzip beruht. Dies bedeutet, dass nur die für den Betrieb notwendigen Dienste installiert bzw. aktiviert sind, um so die Angriffsfläche möglichst gering zu halten.

Dieses Minimalsystem ist von vielen weiteren Systemen abhängig und muss Schnittstellen für Monitoring, Datensicherung, Patch- und Update-Management, Protokollierung, Benutzerverwaltung und Zeitsynchronisation bieten. Je nach Anwendungsfall kann die Anbindung an ein Speichernetz (NAS, SAN) oder die Erweiterung um zusätzliche Komponenten, wie Integritätsprüfung oder Virenschutzprogramm, sinnvoll sein.

Im Serverumfeld ist Virtualisierung eine weitverbreitete Technik, um Hardware-Ressourcen besser auszunutzen. Auf einem Virtualisierungsserver kann eine Vielzahl von Systemen parallel betrieben werden, welche unterschiedliche Dienste anbieten. Beim Einsatz von Virtualisierung sind zusätzliche Sicherheitsaspekte zwischen den Schnittstellen, wie z. B. zwischen Host- und Gastbetriebssystem oder zu unterschiedlichen Netzsegmenten, zu berücksichtigen. Die Studie geht auf die Gefährdungen ein, denen virtuelle Systeme ausgesetzt sind, und beschreibt Maßnahmen, die diese Gefährdungen auf ein akzeptables Restrisiko reduzieren.

## 1.2 Einführung und Überblick

Dieser Abschnitt erläutert kurz die relevanten Begriffe. Abschnitt 1.3 geht auf die wesentlichen Gefährdungen für Serversysteme ein. Empfehlungen zur Absicherung werden in Abschnitt 1.4 dargestellt.

Ein Server setzt sich zusammen aus physischer Hardware, einem Betriebssystem und den Diensten, die der Server anbietet.

Virtualisierung ist im Server-Umfeld inzwischen eine weitverbreitete Technik, um Hardware-Ressourcen besser auszunutzen. Auf einem Virtualisierungsserver kann eine Vielzahl von Systemen parallel betrieben werden, welche unterschiedliche Dienste anbieten.

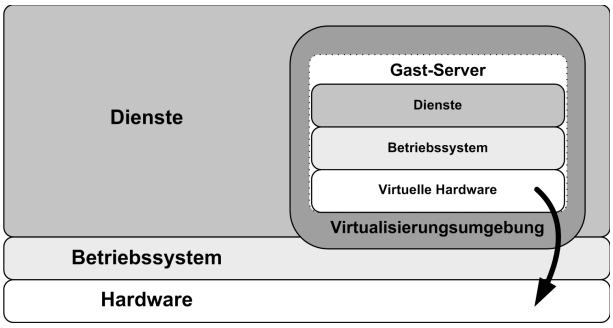



*Abbildung 1.1: Schematischer Aufbau eines Servers*

Nachfolgend werden die Komponenten eines Servers erläutert.

### Hardware

Die Hardware stellt Schnittstellen zur Verfügung, die zur Kommunikation mit der Außenwelt genutzt werden. Zu diesen Hardware-Schnittstellen zählen beispielsweise die Anschlüsse für Monitor, Tastatur, Maus und Netzwerkkarte.

### Betriebssystem

Das Betriebssystem stellt eine Laufzeitumgebung zur Verfügung, die von der installierten Software genutzt wird, um z. B. über das Netz Dienste zur Verfügung zu stellen. Zentraler Bestandteil des Betriebssystems ist der Betriebssystemkern. Zu dessen wesentlichen Aufgaben gehören u. a.:

- die Verwaltung von Betriebsmitteln (z. B. Hauptspeicher, Rechenzeit, Speicherplatz),
- die Steuerung der Ein- und Ausgabegeräte mittels Gerätetreiber,
- die Verarbeitung und Speicherung von Daten,
- die Kontrolle der Benutzerrechte.

Die Administration des Betriebssystems erfolgt über eine Benutzeroberfläche. Diese ist je nach eingesetztem Betriebssystem und dessen Installationsumfang textbasiert (als Kommandozeilen-interpreter) oder als grafische Oberfläche (graphical user interface, GUI) realisiert.

### Dienste

Der Zweck eines Servers ist es, eine Funktion durch einen oder mehrere installierte Dienste über das Netz anzubieten. Solche Dienste können z. B. E-Mail, Web, DNS (Domain Name System) oder

auch DHCP (Dynamic Host Configuration Protocol) sein. Durch die Bereitstellung von Diensten im Netz stehen diese in vorderster Front gegenüber externen und internen Angriffen.

## 1.3 Wesentliche Ergebnisse der Gefährdungsanalyse

Server sind einer Vielzahl von Gefährdungen ausgesetzt, die die Verfügbarkeit, die Integrität und/oder die Vertraulichkeit betreffen. Im Folgenden werden einige dieser Gefährdungen beispielhaft aufgeführt.

### 1.3.1 Vertraulichkeit

Die Gefährdungen durch Entwenden und Ausspähen sind Angriffe auf die Vertraulichkeit von Informationen. Zu den vertraulichen Informationen gehören z. B. Daten aus den Bereichen Forschung und Entwicklung, Gehaltsdaten oder auch Passwörter, die in Institutionen auf unterschiedlichen Servern verarbeitet und gespeichert werden. Die Daten können sich auf Datei-Servern, Datenbank-Servern, E-Mail-Servern, etc. befinden, auf die in der Regel nur eine vorher festgelegte Gruppe von Benutzern nach erfolgreicher Authentisierung zugreifen kann.

Wenn Angreifer Kenntnis von Passwörtern haben, können diese dazu verwendet werden, um sich am Server oder den darauf betriebenen Diensten anzumelden und dadurch Zugriff auf nicht öffentliche Informationen zu bekommen. Durch das Entwenden von Informationen können rechtliche Vorschriften verletzt, Geschäftsgeheimnisse aufgedeckt, der Ruf der Institution und das Vertrauen von Kunden geschädigt werden.

Angreifer können noch auf weitere Arten versuchen an Informationen zu gelangen:

- Durch die Nutzung unsicherer Protokolle können ggf. Anmeldename und Passwort mitgelesen und für weitere Angriffe verwendet werden. Dies betrifft sowohl Administratoren, die den Server über das Rechnernetz administrieren, als auch Benutzer, die sich mit einem Passwort an Diensten anmelden, die der Server zur Verfügung stellt.
- Werden Daten mit hohem Schutzbedarf unverschlüsselt auf Medien gespeichert, auf die ein Angreifer Zugriff hat (z. B. Backup-Medien, externe Speichermedien, etc.), dann können diese leicht entwendet oder kopiert werden.
- Wurden einem Benutzer mehr Rechte zugeteilt, als er für seine eigentliche Aufgabenerfüllung benötigt, dann ermöglicht ihm dies, unberechtigt auf die Daten Dritter zuzugreifen.
- Ein Virtualisierungsserver ist an mehrere Netzsegmente angebunden. Diese Netzsegmente sollen typischerweise voneinander getrennt sein. Durch eine Fehlkonfiguration kann es einem virtuellen IT-System möglich sein, auf mehrere Netzsegmente zuzugreifen und dort Daten abzugreifen.

### 1.3.2 Integrität

In dieser Kategorie können Angriffe auf die Integrität und Authentizität von Informationen eingeordnet werden. Die Integrität und Authentizität von Informationen ist gegeben, wenn sichergestellt werden kann, dass Unbefugte die Daten nicht verändern oder deren Ursprung fälschen können. Gelingt es einem Angreifer auf einen Server zuzugreifen, hat er die Möglichkeit mit den erlangten Rechten sowohl Daten als auch die Software des IT-Systems zu manipulieren.

Die Sicherstellung der Integrität von Daten fängt bereits bei der Installation von Software an. Die Installationsmedien des Betriebssystems oder der auf dem Server betriebenen Dienste müssen von einer vertrauenswürdigen Quelle bezogen werden. Ansonsten besteht die Gefahr, dass diese Daten verändert wurden und ggf. Schadsoftware (wie z. B. Trojaner) eingeschleust wurde, die großen Schaden auf dem Server oder sogar in dem Netz der Zielumgebung anrichten können.

Schadsoftware kann auch im späteren Betrieb, z. B. durch E-Mail-Anhänge oder hochgeladene Dateien auf Web-Servern, in das Netz einer Organisation gelangen. Ohne den Einsatz von entsprechenden Kontrollwerkzeugen wird eine Modifikation von Daten oder auch das Ausspähen und/oder Löschen von Daten durch Schadprogramme häufig nicht erkannt.

Ein weiterer Angriff, der in diese Gefährdungskategorie fällt, ist die Manipulation der Systemuhrzeit des Servers. Verfügt das System nicht über eine genaue Uhrzeit, arbeiten Dienste u. U. nicht mehr korrekt oder beenden sich sogar. Die Manipulation der Systemuhrzeit kann z. B. durch die Kompromittierung des zentralen Zeitgebers erfolgen, der für die Synchronisation der Uhrzeit mit den Serversystemen verwendet wird.

### 1.3.3 Verfügbarkeit

Die Gefährdung der Verfügbarkeit von Hardware, Betriebssystem und Diensten umfasst z. B. das Verhindern der Kommunikation mit Diensten oder auch Hardware-Defekte.

Technisches Versagen kann auf unterschiedlichen Ebenen die Verfügbarkeit des Servers und der darauf betriebenen Dienste beeinflussen. Die Verfügbarkeit einzelner Dienste oder des gesamten Servers kann durch defekte Server-Hardware, einen Ausfall der Energieversorgung oder einen Netzwerkfehler bedroht sein. Neben der Verfügbarkeit ist auch die Konsistenz der Daten bedroht, da der Server bspw. im Falle eines Spannungsverlustes nicht kontrolliert heruntergefahren werden kann und Daten aus dem Arbeitsspeicher nicht mehr auf Datenträger geschrieben werden können.

Ein Angreifer kann auch vorsätzlich die Verfügbarkeit einschränken, indem er Daten löscht, Dienste beendet oder Server herunterfährt. Die Löschung von Daten kann auch versehentlich durch Benutzer durchgeführt werden.

## 1.4 Wesentliche Empfehlungen

Ein Server steht nie alleine, sondern wird in das Netz der Institution eingefügt. Innerhalb der ISi-Server Studie wird nicht auf vorgeschaltete Sicherheitskomponenten eingegangen, da diese bereits von den Grundarchitekturen aus anderen Studien behandelt werden. Die Abbildung 1.2 zeigt z. B. die Grundarchitektur aus [ISi-LANA] in der die Absicherung des Netzes der Institution durch Paketfilter und Application Level Gateway (ALG) erfolgt.

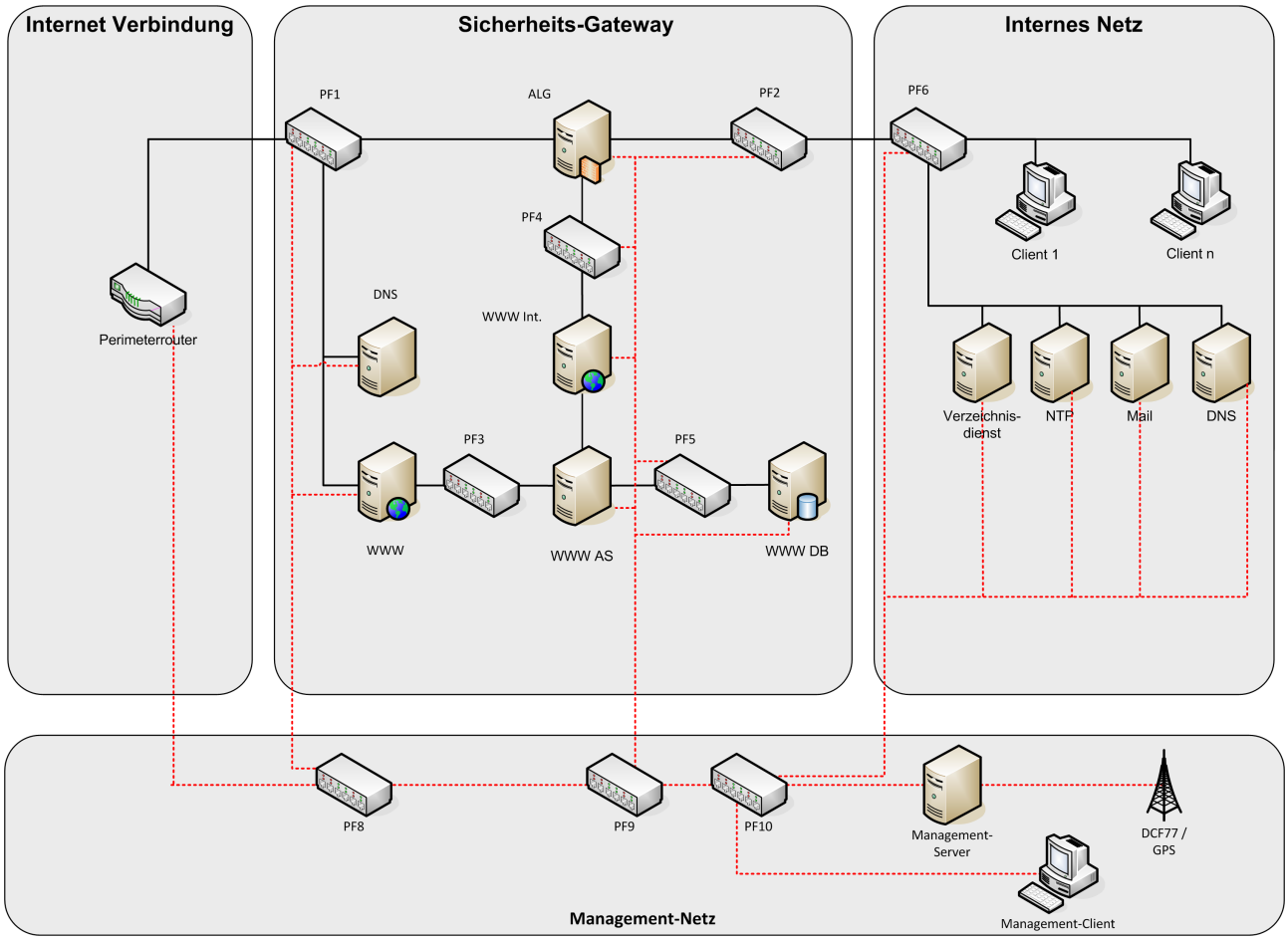



*Abbildung 1.2: Grundarchitektur gemäß ISi-LANA mit Management-Zone*

Die Studie ISi-Server ist auf die Absicherung eines Servers fokussiert. Es wird die Absicherung des Rechnernetzes gemäß [ISi-LANA] vorausgesetzt. In der Studie wird eine Grundarchitektur vorgestellt, die den Gefährdungen aus Abschnitt 1.3 begegnet. Diese Grundarchitektur (siehe auch Abbildung 1.3) umfasst zum einen Konfigurationsempfehlungen für das Betriebssystem, zum anderen zusätzliche Sicherheitskomponenten.

### 1.4.1 Sichere Grundarchitektur

In Abbildung 1.2 sind Server für verschiedene Einsatzzwecke aufgeführt, die sich in unterschiedlichen Sicherheitszonen befinden. Der Einsatzzweck dieser Systeme ist vielfältig und reicht vom Web-Server mit Datenbankanbindung innerhalb der Zone „Sicherheits-Gateway“ bis hin zum NTP-Server für die Zeitsynchronisation in der Zone „Internes Netz“.

Trotz der vielfältigen Einsatzbereiche ist die grundlegende Absicherung des Betriebssystems gleich. Sie basiert auf einem Minimalsystem sowie den Sicherheits-Komponenten, die für den normalen Schutzbedarf installiert werden müssen.

Abbildung 1.3 greift die Architektur eines Servers (siehe auch Abbildung 1.1) auf und ergänzt diese um Sicherheits-Komponenten.

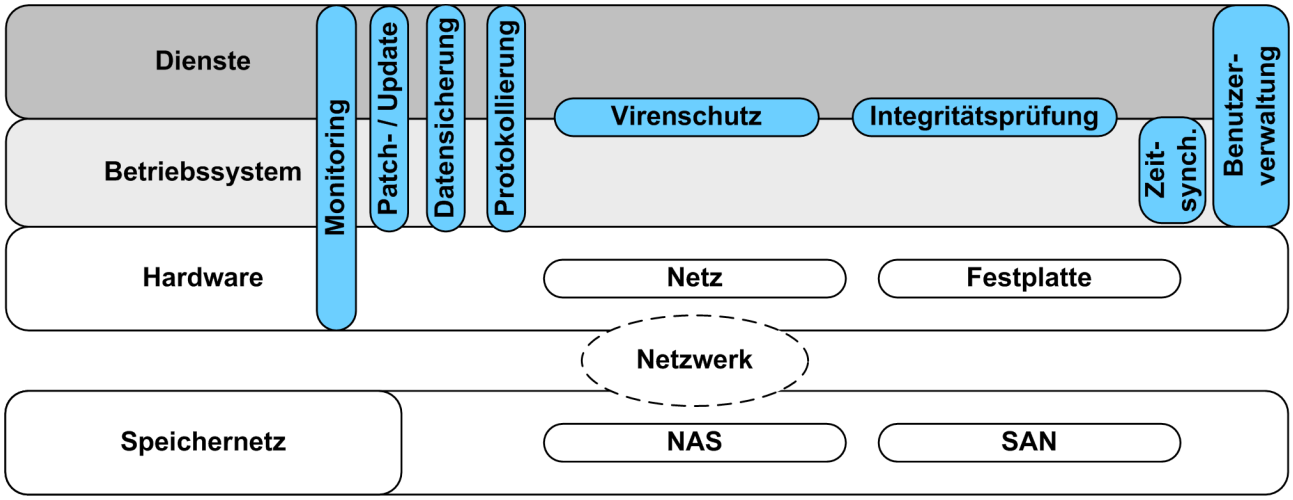



*Abbildung 1.3: Grundarchitektur eines Servers*

### Minimalinstallation des Betriebssystems

Als Schutzkomponente gegen Eindringen und Übernehmen eines Servers durch einen Angreifer dienen in erster Linie die Minimalinstallation und die sichere Grundkonfiguration des Betriebssystems. Ist das Betriebssystem nur mit den benötigten Diensten ausgestattet, dann bietet dies einem Angreifer nur eine geringe Angriffsfläche für mögliche Einbruchsversuche. Schwachstellen im Betriebssystem und in Diensten werden innerhalb des Patch- und Änderungsmanagements durch die Installation von aktuellen Patches und fehlerbereinigter Software auf ein Minimum reduziert.

### Protokollierung

Protokollmeldungen von Betriebssystem und Diensten werden zentral gespeichert und ausgewertet. Treten ungewöhnliche Meldungen auf (z. B. fehlerhafte Anmeldeversuche oder ungeplanter Neustart eines Servers), kann dies ein Hinweis auf Angriffe sein.

### Benutzerverwaltung

Durch die Konfiguration von Benutzerrollen und Gruppenrechten sorgt die Benutzerverwaltung dafür, dass einzelne Benutzer nicht mit mehr Rechten ausgestattet werden, als sie für ihre eigentliche Aufgabenerfüllung benötigen. Wird jeder Benutzer lokal auf einem Server verwaltet, so ist die Gefahr groß, dass Fehler bei der Rechtevergabe vorkommen. Deshalb ist eine zentrale Benutzerverwaltung vorzuziehen. Eine zentrale Vergabe der Berechtigungen verringert die Gefahr von Fehlkonfigurationen. Zusätzlich lässt sich über eine zentrale Benutzerverwaltung sicherstellen, dass alle Passwörter eine ausreichende Komplexität beinhalten, die automatisierten Angriffen standhält.

### Monitoring

Hardware, Betriebssystem und Dienste werden kontinuierlich im Rahmen des Monitorings beobachtet. Ausfälle werden somit erkannt und die verantwortlichen Personen werden alarmiert. Einem Datenverlust wird durch die zentrale Datensicherung vorgebeugt.

### Integritätsprüfung

Hat ein Angreifer Zugriff auf das Betriebssystem, dann kann er die Konfiguration verändern oder Hintertüren in das System einbauen. Hier greift die Integritätsprüfung, die Änderungen an Dateien erkennt und an das zentrale Management meldet, wodurch auf mögliche Angriffe hingewiesen wird.

### Virenschutz

Die Modifikation des Systems durch Schadprogramme wie z. B. Viren oder Trojaner kann sowohl den lokalen Server als auch weitere Server im Netzwerk gefährden. Ein Virenschutzprogramm kann Infektionen erkennen und die Verbreitung von Schadprogrammen frühzeitig verhindern.

### Speichernetz

Reicht der lokal zur Verfügung stehende Speicherplatz nicht aus, dann kann dieser durch externe Speicher, z. B. die Anbindung an ein Speichernetz, erweitert werden.

### Patch- und Änderungsmanagement

Über das Patch- und Änderungsmanagement werden Installation und Aktualisierung der Software für den Server gesteuert. Aktualisierungen schließen häufig Schwachstellen in Betriebssystemen und Anwendungen und sind daher für einen sicheren Betrieb unerlässlich.

### Datensicherung

Um einem Datenverlust vorzubeugen, ist eine regelmäßige Datensicherung unbedingt notwendig.

### Notfallvorsorgekonzept

Ein Notfallvorsorgekonzept stellt die Verfügbarkeit von Servern und Daten sicher, wenn ein Server ausfällt. Es enthält Maßnahmen, welche Aktivitäten im Falle eines Ausfalls durchzuführen sind und wie die Folgen eines Ausfalls minimiert werden können.

### Weiterführende Hinweise

Die auf dem Server installierten Dienste werden über das Netzwerk zur Verfügung gestellt. Daher gelten für die Anbindung dieser Systeme an das Netzwerk die zutreffenden Empfehlungen aus der Studie *Sichere Anbindung von lokalen Netzen an das Internet* [ISi-LANA]. Werden auf dem Server weitere spezifische Dienste betrieben, dann erfordern diese ebenfalls eine weitere Umsetzung von Dienst-spezifischen Schutzmaßnahmen. Diese werden detailliert in anderen Studien behandelt, wie z. B. *Sicherer Betrieb von E-Mail-Servern* [ISi-Mail-Server] oder *Sicheres Bereitstellen von Web-Angeboten* [ISi-Web-Server].

### 1.4.2 Grundarchitektur der Infrastruktur mit virtualisierten Komponenten

Bei den in Abbildung 1.2 dargestellten Komponenten handelt es sich jeweils um dedizierte physische Server. Es gibt jedoch die Möglichkeit, dass einige dieser Komponenten auch auf einem Virtualisierungsserver zusammengefasst werden können. Abbildung 1.4 zeigt diese Grundarchitektur mit virtualisierten Server-Systemen.

In der Grundarchitektur mit virtualisierten Komponenten wurden die folgenden Server zusammengelegt:

- DNS und WWW auf dem Virtualisierungsserver I
- WWW Int. und WWW AS auf dem Virtualisierungsserver II
- Verzeichnisdienst, NTP, Mail und DNS auf dem Virtualisierungsserver III

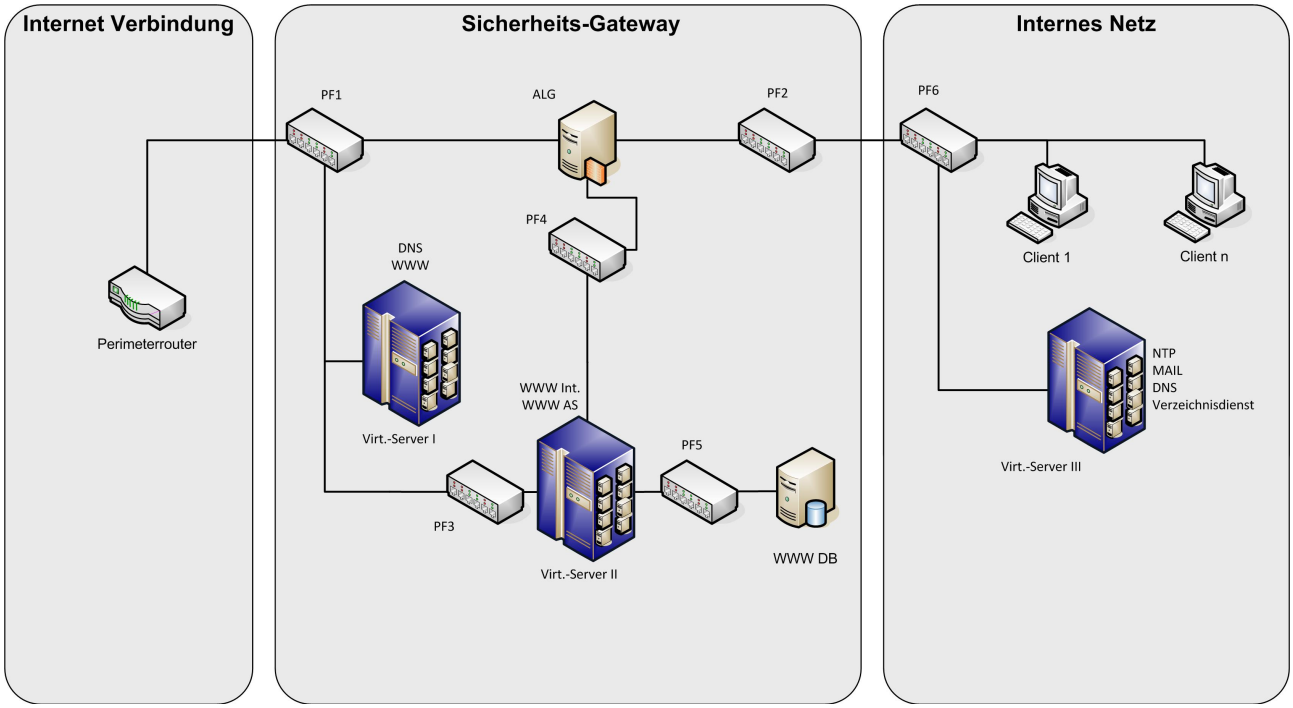



*Abbildung 1.4: Grundarchitektur der Infrastruktur mit virtualisierten Komponenten*

Der Vorteil der Virtualisierung ist, dass mehrere Dienste mit separaten und auch unterschiedlichen Betriebssystemen auf einem Virtualisierungsserver betrieben werden können. Dadurch wird zum einen der Einsatz dedizierter physischer Hardware reduziert, zum anderen reduziert sich die Wahrscheinlichkeit eines Systemausfalls aufgrund defekter Hardware. Der Nachteil ist jedoch, dass bei dem Ausfall des Virtualisierungsservers alle darauf laufenden Betriebssysteme und Dienste betroffen sind. Daher wird in der Grundarchitektur die redundante Auslegung der Hardware für Virtualisierungsserver empfohlen.

## 1.5 Fazit

Server bilden das Rückgrat der IT-Infrastruktur. Sie stellen zentrale Dienste zur Verfügung, auf die Benutzer oder andere Infrastruktur-Komponenten angewiesen sind. Ist ein Server in seiner Funktion beeinträchtigt (z. B. durch einen Ausfall), dann kann dies im schlimmsten Fall die gesamte Arbeitsfähigkeit einer Institution beeinträchtigen.

Die ISi-Server Studie geht auf Gefährdungen ein, denen Server ausgesetzt sind, und zeigt Maßnahmen auf, die diesen Gefährdungen begegnen. Diese Maßnahmen sind Teil einer Grundarchitektur, die durch Konfigurationsempfehlungen für das Betriebssystem und durch Sicherheitskomponenten einen Basisschutz bewirkt. Kern der Grundarchitektur ist ein Minimalsystem, welches nur die Komponenten des Betriebssystems enthält, die für den Betrieb erforderlich sind. Hierdurch wird ein sicheres und robustes Grundsystem erstellt, das eine geringe Angriffsfläche bietet.

Auf diesem Minimalsystem können dann sowohl weitere Sicherheitskomponenten als auch spezifische Dienste installiert werden. Diese Dienste können zu weiterführenden Schutzmaßnahmen führen, die in den fachspezifischen Modulen zu „Dienste und Anwendungen im Internet“ aus der BSI-Schriftenreihe zur Internet-Sicherheit (ISi-Reihe) behandelt werden.

Ergänzt wird die Studie durch Checklisten für unterschiedliche Betriebssysteme, die Empfehlungen für die Phasen Beschaffung, Konfiguration und Betrieb geben. Diese sollen Administratoren, Beratern oder auch Auditoren eine Hilfestellung geben, um die vorgestellte Grundarchitektur umsetzen und prüfen zu können.

# 2 Literaturverzeichnis


[ISi-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Absicherung eines Servers (ISi-Server), 2011, https://www.bsi.bund.de/InternetSicherheit.html

[ISi-Web-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sicheres Bereitstellen von Webangeboten (ISi-Web-Server), 2008, https://www.bsi.bund.de/InternetSicherheit.html

[ISi-Mail-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sicherer Betrieb von E-Mail-Servern (ISi-Mail-Server), 2009, https://www.bsi.bund.de/InternetSicherheit.html

[ISi-LANA] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sichere Anbindung lokaler Netze an das Internet, 2007, https://www.bsi.bund.de/InternetSicherheit.html