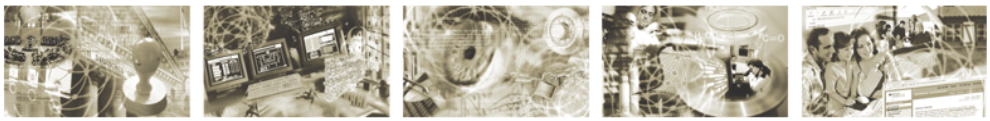
Bundesamt
für Sicherheit in der
Informationstechnik



Absicherung eines Servers (ISi-Server)

BSI-Studie zur Internet-Sicherheit (ISi-S)

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

https://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

Inhaltsverzeichnis

1 Einleitung....6

2 Grundlagen....7

2.1 Aufbau eines Servers....7
2.1.1 Hardware....7
2.1.2 Bauformen....8
2.1.3 Betriebssystem....10
2.1.4 Dienste....11
2.1.5 Einbettung eines Servers in ein Rechnernetz....11

2.2 Benutzer und Rechte....11
2.2.1 Benutzerkonten, Gruppen und Rechte....12
2.2.2 Benutzerverwaltung....12

2.3 Techniken und Komponenten zur Absicherung des Servers....13
2.3.1 Minimalsystem....13
2.3.2 Verschlüsselung von Datenträgern....13
2.3.3 Verschlüsselung von einzelnen Daten....14
2.3.4 TPM (Trusted Platform Module)....14
2.3.5 Virtualisierung....14
2.3.5.1 Virtualisierungstechniken....15
2.3.5.2 Weitere Grundlagen zur Virtualisierung....18
2.3.6 Virenschutzprogramm....19
2.3.7 Ausführungskontrolle....20
2.3.8 Integritätsprüfung....20
2.3.9 Lokaler Paketfilter....20
2.3.10 Fernadministration....20
2.3.11 Monitoring....21
2.3.12 Hardware-Management....22
2.3.13 Protokollierung....22
2.3.14 Speicherschutzmechanismen....23
2.3.15 Speicherrandomisierung....23
2.3.16 Datensicherung....23
2.3.16.1 Arten von Datensicherungen....24

2.4 Verfügbarkeit....24
2.4.1 Berechnung der Verfügbarkeit....25
2.4.2 Verfügbarkeitsklassen....25
2.4.3 Serienschaltung von Komponenten....26
2.4.4 Parallelschaltung von Komponenten....27

2.5 Massenspeicher....29
2.5.1 Local Storage und Direct Attached Storage (DAS)....29
2.5.2 Network Attached Storage (NAS)....29
2.5.3 Storage Area Network (SAN)....29
2.5.3.1 Host Bus Adapter....30
2.5.3.2 Ausfallsicherheit im SAN....30
2.5.3.3 Zugriff auf den Massenspeicher....31
2.5.4 Massenspeicherprotokolle....32
2.5.4.1 SMB / CIFS....32
2.5.4.2 NFS....33
2.5.4.3 iSCSI....33
2.5.4.4 Fibre Channel....34
2.5.4.5 Fibre Channel over Ethernet (FCoE)....34

3 Sichere Grundarchitektur für normalen Schutzbedarf....35

3.1 Überblick....35

3.2 Komponenten der Grundarchitektur....38

3.2.1 Hardware....38
3.2.2 Betriebssystem....38
3.2.3 Sicherheits-Komponenten....39
3.2.4 Benutzerverwaltung....40
3.2.5 Protokollierung....41
3.2.6 Monitoring....42
3.2.7 Integritätsprüfung....42
3.2.8 Datensicherung....43
3.2.9 Aktualisierung des Servers....43
3.2.10 Speichernetz....44
3.2.11 Virenschutzprogramm....45
3.3 Organisatorische Maßnahmen....45
3.4 Netzmanagement....46
3.5 Grundarchitektur der Infrastruktur mit virtualisierten Komponenten....47
4 Komponenten sicher auswählen, konfigurieren und betreiben (normaler Schutzbedarf)....50
4.1 Grundanforderungen an ein sicheres Produkt....50
4.1.1 Übergreifende Aspekte....50
4.1.1.1 Planung....50
4.1.1.2 Auswahl und Bezug der Komponenten....50
4.1.1.3 Lizenzierung....51
4.1.2 Hardware....51
4.1.3 Betriebssystem....52
4.1.4 Dienste....53
4.1.5 Benutzerverwaltung....53
4.1.6 Protokollierung....54
4.1.7 Monitoring....54
4.1.8 Integritätsprüfung....54
4.1.9 Datensicherung....55
4.1.10 Patch- und Änderungsmanagement....55
4.1.11 Speichernetz....55
4.1.12 Virenschutzprogramm....56
4.1.13 Virtualisierung....57
4.2 Sichere Grundkonfiguration und Minimierung der Komponenten....58
4.2.1 Hardware, Firmware und externe Schnittstellen....58
4.2.2 Konfiguration von RAID....58
4.2.3 Betriebssystem....59
4.2.3.1 Installation....59
4.2.3.2 Partitionieren und Formatieren der Festplatte....60
4.2.3.3 Netzkonfiguration....60
4.2.3.4 Deaktivieren von Netzprotokollen....61
4.2.3.5 Sichere Konfiguration des Betriebssystems....61
4.2.4 Dienste....62
4.2.5 Benutzerrechte, -verwaltung und -authentisierung....63
4.2.6 Lokale Protokollierung....64
4.2.7 Monitoring....64
4.2.8 Integritätsprüfung....65
4.2.9 Datensicherung....66
4.2.10 Integration des Betriebssystems in ein Patch- und Änderungsmanagement....66
4.2.11 Anbindung des Speichernetzes....66
4.2.12 Virenschutzprogramm....67
4.2.13 Virtualisierung....67
4.3 Grundvorgaben für einen sicheren Betrieb....69
4.3.1 Organisatorische Aspekte....69
4.3.2 Hardware und Firmware....70
4.3.3 Betriebssystem und Dienste....70

4.3.4 Benutzerrechte, -verwaltung und -authentisierung....70
4.3.5 Protokollierung....71
4.3.6 Monitoring....71
4.3.7 Integritätsprüfung....72
4.3.8 Datensicherung....72
4.3.9 Virtualisierung....73
4.3.10 Virenschutzprogramm....73
4.4 Außerbetriebnahme....74
5 Gefährdungen und Empfehlungen mit Varianten für den normalen und hohen Schutzbedarf....75
5.1 Gefährdungen durch Eindringen und Übernehmen....75
5.1.1 Ausnutzen von Schwachstellen in Diensten....75
5.1.2 Erraten und/oder Manipulation von Passwörtern....77
5.1.3 Unautorisierter Zugriff auf Dienste....78
5.1.4 Zugriff auf verwaiste Benutzerkonten....78
5.1.5 Unbefugter Zugriff auf Schnittstellen zur Fernadministration....79
5.1.6 Einsatz veralteter Software....80
5.2 Gefährdungen durch Entwenden und Ausspähen (Vertraulichkeit)....81
5.2.1 Mitlesen von Administrationstätigkeiten....81
5.2.2 Zugriff auf getrennte Netzsegmente durch fehlerhafte Virtualisierung....82
5.2.3 Unbefugter Zugriff auf lokalen Massenspeicher....83
5.2.4 Unbefugter Zugriff auf das Speichernetz....86
5.2.5 Unbefugter Zugriff auf die Backup-Medien....87
5.2.6 Unbefugter Zugriff auf Daten aufgrund zu umfangreicher Berechtigungen....88
5.2.7 Unerlaubtes Starten von ausführbaren Dateien....89
5.3 Gefährdungen durch Verändern, Täuschen, Fälschen und Betrügen (Integrität und Authentizität)....91
5.3.1 Manipulation von Dateien durch Schadprogramme....91
5.3.2 Manipulation des Boot-Codes oder des Bootloaders durch ein Schadprogramm....93
5.3.3 Manipulation der Systemuhrzeit....93
5.3.4 Manipulation von Dateien....94
5.3.5 Nutzung von kompromittierten Installationsmedien....95
5.4 Gefährdungen durch Verhindern und Zerstören (Verfügbarkeit)....95
5.4.1 Nicht-Verfügbarkeit durch einen Defekt der Hardware oder Ausfall eines Dienstes....95
5.4.2 Datenverlust aufgrund einer defekten Festplatte....96
5.4.3 Ausfall der Energieversorgung....97
5.4.4 Datenverlust durch mangelnde Speicherkapazität....98
5.4.5 Datenverlust durch Löschen oder Ändern von Daten....99
5.4.6 Nicht-Verfügbarkeit des Virtualisierungsservers....99
6 Fazit....101
7 Anhang....102
7.1 Abdeckungsmatrix....102
7.2 Varianten der Grundarchitektur....105
7.2.1 Kleines Unternehmen....106
7.2.2 Mittelgroßes Unternehmen....108
7.2.3 Großes Unternehmen....110
8 Glossar....112
9 Stichwort- und Abkürzungsverzeichnis....124
10 Literaturverzeichnis....127

1 Einleitung

Die Schriftenreihe zur Internet-Sicherheit (ISi-Reihe) befasst sich mit der Sicherheit von Diensten, Netz-Komponenten und den darunterliegenden Rechnernetzen. Sie richtet sich an alle Personen in Behörden und Unternehmen, die sich mit diesem Themenfeld beschäftigen, und bietet ihnen dazu umfassende und aktuelle Informationen. Sie erläutert, mit welchen Gefährdungen zu rechnen ist und gibt Empfehlungen zu vorbeugenden Sicherheitsmaßnahmen, insbesondere unterstützt sie bei der Planung und Realisierung von Netzen und Diensten. Als Ausgangspunkt dient eine sichere Grundarchitektur, die sich mittels Varianten an die individuellen Gegebenheiten anpassen lässt.

Die ISi-Server Studie befasst sich mit der Absicherung der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit von Servern, deren Betriebssystemen und den darauf betriebenen Diensten. Wie in den anderen Modulen der ISi-Reihe wird eine Grundarchitektur vorgestellt, die zur Absicherung eines Servers dient und grundlegenden Vorgaben für Beschaffung, Konfiguration und Betrieb von Hard- und Software-Komponenten gibt. Schwerpunkt der Studie ist die Absicherung des Betriebssystems. Die Absicherung der Dienste, die der Server anbieten soll, wird durch andere Module der ISi-Reihe oder weitere BSI-Publikationen abgedeckt. Es handelt sich um eine übergreifende Studie ohne Fokussierung auf spezifische Betriebssysteme.

Abschnitt 2 beschreibt die Protokolle, Dienste und Technologien, die innerhalb einer Server-Infrastruktur eingesetzt werden. Die hier vermittelten Grundlagen schaffen die nötige Voraussetzung für das Verständnis der nachfolgenden Abschnitte.

Abschnitt 3 stellt eine sichere Grundarchitektur eines Servers für normalen Schutzbedarf vor und beschreibt die Komponenten, die auf einem Server installiert und betrieben werden müssen, um ein Mindestmaß an Sicherheit zu erreichen. Diese Komponenten sorgen dafür, dass Angriffe erkannt und ggf. verhindert werden, im Fehlerfall der Betrieb eines ausgefallenen Servers wiederhergestellt werden kann und der Betrieb der zur Verfügung gestellten Dienste sichergestellt wird.

Abschnitt 4 gibt Empfehlungen, wie die zur Realisierung der Grundarchitektur notwendigen Komponenten sicher ausgewählt, konfiguriert und betrieben werden können.

In Abschnitt 5 werden die Gefährdungen beschrieben, denen ein Server ausgesetzt ist. Zu jeder Gefährdung werden die in den vorigen Abschnitten aufgeführten Maßnahmen zugeordnet, durch die das System abgesichert wird. Darüber hinaus werden dort auch Varianten vorgestellt, die die Grundarchitektur (z. B. für die Realisierung in kleinen Unternehmen) vereinfachen. Zudem wird auf weitere Sicherheitsmaßnahmen eingegangen, die beispielsweise für hohen Schutzbedarf eingesetzt werden können.

Abschnitt 7.1 im Anhang enthält eine Abdeckungsmatrix für den normalen und für den hohen Schutzbedarf, die dem Anwender helfen soll, diejenigen Maßnahmen zu ermitteln, die im Kontext seiner spezifischen Bedrohungslage relevant und angemessen sind.

Abschnitt 7.2 beschreibt Varianten der Grundarchitektur für kleine, mittelgroße und große Unternehmen für den normalen und hohen Schutzbedarf. Sie enthalten Beispiele, wie die Architektur an eine veränderte Unternehmensgröße oder einen veränderten Schutzbedarf angepasst werden kann und welche Konsequenzen dies für die Gefährdungslage hat.

2 Grundlagen

Dieser Abschnitt erläutert die Basistechniken für den sicheren Einsatz eines Servers. Es werden Begriffe und Sicherheitseigenschaften behandelt sowie Techniken und Komponenten beschrieben, die zur Absicherung von Server-Systemen verwendet werden. Diese bilden die Grundlage für das Verständnis der in Abschnitt 3 vorgestellten Grundarchitektur.

2.1 Aufbau eines Servers

Ein Server setzt sich schematisch aus einer Kombination von physischer Hardware, einem darauf aufsetzenden Betriebssystem sowie den darauf betriebenen Diensten zusammen.

Ein Server steht üblicherweise in einem Rechenzentrum und wird über ein Rechnernetz administriert. Systeme, die über das Rechnernetz auf einen Server zugreifen, werden als Clients bzw. Client-Systeme bezeichnet. Dies können aus Sicht des Servers sowohl andere Server als auch Arbeitsplatz-PCs sein.

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 (siehe Abbildung 2.1).

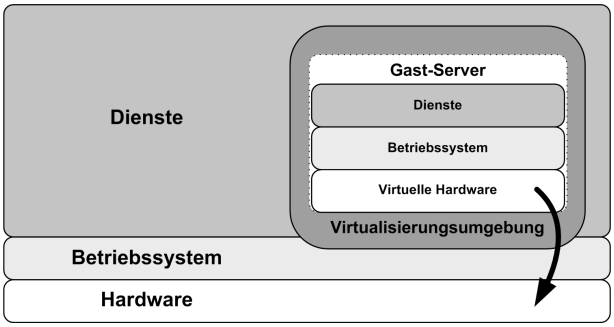


Abbildung 2.1: Schematischer Aufbau eines Servers

Nachfolgend werden die einzelnen Komponenten eines Servers detailliert erläutert.

2.1.1 Hardware

Im Gegensatz zur Standard-PC Hardware für Arbeitsplatz-PCs besteht Server-Hardware oft aus leistungsstärkeren und hochwertigeren Komponenten, die für den Dauereinsatz (24x7) ausgelegt sind. Diese Komponenten umfassen z. B.

- eine oder mehrere CPUs
- eine oder mehrere Festplatten
- einen oder mehrere Netzwerkkarten
- einen oder mehrere Host Bus Adapter (HBA) für die Anbindung von Speichernetzen
- redundante Netzteile
- RAID-Controller

- SCSI- / SAS-Controller
- ein optisches Laufwerk (CD/DVD).

Um dem Ausfall zentraler Komponenten entgegenzuwirken, werden diese im Serverbereich häufig redundant verbaut. Redundanz bezeichnet hier die Vervielfältigung von einzelnen Komponenten, um den Ausfall einer Einzelnen zu kompensieren. Bei modernen Server-Systemen können nahezu alle Bauteile redundant ausgelegt werden (Netzteil, Controller, Festplatten, Arbeitsspeicher, etc.). Diese Komponenten sind in der Regel Hot-Swap fähig (siehe auch Abschnitt 2.4).

Aufgrund der Anzahl und Leistungsfähigkeit der eingebauten Komponenten ist die Wärmeentwicklung innerhalb des Servers deutlich höher als bei einem Arbeitsplatz-PC. Um eine hohe Lebensdauer der Komponenten zu gewährleisten, ist eine ausreichende Lüftung und Kühlung durch Ventilatoren erforderlich. Aufgrund des Kühlungsbedarfs und der im Vergleich zu einem Arbeitsplatz-PC höheren Anzahl an eingebauten Komponenten haben Server auch eine andere Gehäuseform, da durch die Bauform der Luftstrom zur Wärmeabführung beeinflusst wird (siehe auch Abschnitt 2.1.2).

Firmware

Als Firmware wird die Betriebssoftware von elektronischen Komponenten bezeichnet. Analog zu dem Betriebssystem eines Computers, das die Zusammenarbeit aller Komponenten eines Rechners koordiniert, ist die Firmware auf den einzelnen Hardware-Komponenten installiert und sorgt für den korrekten Betrieb der Hardware-Komponente. U. a. sind die folgende Hardware-Komponenten mit Firmware ausgestattet:

- Hauptplatine (engl. Mainboard); der Name der Firmware variiert dort abhängig von der eingesetzten Rechnerarchitektur:
  - BIOS - „Basic Input Output System“ (für x86-Architekturen)
  - EFI - „Extensible Firmware Interface“ (für IA-64-Architekturen)
  - Open Firmware / Open Boot (für nicht-Intel-Architekturen)
- RAID Controller
- Host Bus Adapter (HBA)
- Festplatten
- optische Laufwerke (CD/DVD Laufwerke)
- Netzwerkkarten.

Die jeweiligen Hardware-Hersteller veröffentlichen in unregelmäßigen Abständen neue Firmware-Versionen, die Fehler beheben, neue Funktionen aktivieren oder Sicherheitslücken schließen.

2.1.2 Bauformen

Server-Hardware gibt es in den unterschiedlichen Bauformen als Rackmount Server, Blade Server und ATX Server. Dieser Abschnitt beschreibt die unterschiedlichen Bauformen sowie deren Vor- und Nachteile.

Rackmount Server

Rackmount Server sind Server mit einer Breite von 19 Zoll (48,26 cm), die in besondere Schränke (19-Zoll-Racks) eingebaut werden. Die Höhe der einzelnen Komponenten wird in Höheneinheiten (HE) gemessen und beträgt 1,75 Zoll (4,445 Zentimeter) pro HE. Standard-Racks für Rechenzentren sind etwa 2 Meter hoch und bieten meist einen Netto-Raum von 42 HE, in denen mehrere 19-Zoll-Komponenten übereinander eingebaut werden können. Rackmount Server gibt es in unterschiedlichen Höheneinheiten (meist 1 bis 5 HE).

Vorteile:

- geringere Einbauhöhe als bei ATX Server (siehe unten) möglich
- flexibel bei der Auswahl der Hersteller
- kostengünstiger als Blade Server (siehe unten), wenn nur wenige Server angeschafft werden sollen.

Nachteile:

- Höherer Platzbedarf im Vergleich zu Blade Servern.

Blade Server

Ein Blade Server (auch nur Blade genannt) ist eine separate Einheit eines Servers, die als Einschub in einem 19-Zoll-Rack verwendet wird. Mehrere Blades werden in einem Blade-Gehäuse mittels eines gemeinsamen Busses (Backplane) zusammengeschaltet. Blade Server haben keine eigene Stromversorgung. Diese wird über die Backplane des Blade-Gehäuses zur Verfügung gestellt. Die Lüftung erfolgt auch extern über das Blade-Gehäuse oder das 19-Zoll-Rack. Der Vorteil liegt in der platzsparenden Bauform. So kann z. B. ein Standard 19-Zoll-Rack mit 42 Höheneinheiten bis zu 84 Blade Server aufnehmen. Blade Server besitzen in der Regel nur eine Hauptplatine mit Mikroprozessoren, Arbeitsspeicher sowie optional eine oder mehrere 2,5“ Festplatten, die für das Betriebssystem gedacht sind.

Vorteile:

- Hohe Server-Dichte und geringer Platzbedarf. Im Vergleich zu Rackmount Servern kann hier sogar eine Verdoppelung der Server pro Rack erzielt werden.
- Effizienter Betrieb durch gemeinsam genutzte Komponenten (Stromversorgung, Netzwerkschnittstellen, Speicher).
- Schnelle Erweiterungen durch das Hinzufügen neuer Blades möglich - auch im laufenden Betrieb.
- Niedrigerer Energieverbrauch bezogen auf die Einzel-Komponenten als bei herkömmlichen Servern.

Nachteile:

- Höhere Wärmeentwicklung aufgrund der Packdichte. Dadurch werden leistungsfähigere Lüfter eingesetzt (z. B. als 19-Zoll-Einschub), die einen höheren Lärmpegel haben.
- Gleichzeitig ist aufgrund der Packdichte eine höhere Leistungsaufnahme vorhanden, die häufig den Anschluss an Dreiphasenwechselstrom voraussetzen.
- Da es keine einheitlichen Standards für Blades gibt, ist man bei der Anschaffung und Erweiterung von einem Blade-Hersteller abhängig.

- Falls nur eine geringe Anzahl von Blades betrieben werden soll, sind die Anschaffungskosten in der Regel höher als bei Rackmount Servern oder ATX Servern.

ATX Server

Das ATX-Format (Advanced Technology Extended) ist eine Norm für Gehäuse, Netzteile, Hauptplatinen und Steckkarten. Die Bauform ist ähnlich zu einem Büro-PC in einem Standgehäuse. Diese Server können stehend oder liegend betrieben werden. Mit speziellen Umbau-Kits können sie liegend in ein 19-Zoll-Rack eingebaut werden. Im Gegensatz zu Rackmount Servern ist diese Bauform jedoch mindestens 4 Höheneinheiten hoch (bzw. breit). Die Preise sind vergleichbar mit denen von Rackmount Servern. Ansonsten bestehen dieselben Vor- und Nachteile wie bei Rackmount Servern.

Vorteile:

- Flexibel einsetzbar, sowohl als Stand-Server als auch als Rackmount Server.

Nachteile:

- Aufgrund der Bauhöhe ist die Packdichte meist geringer als bei Rackmount Servern.

Fazit

Generell können alle drei Bauformen in unterschiedlichsten Bereichen eingesetzt werden (z. B. Laborumgebungen, Serverräume, Rechenzentren). Welche Bauform bevorzugt wird, ist abhängig von dem späteren Einsatzbereich und dessen Anforderungen.

2.1.3 Betriebssystem

Das Betriebssystem wird auf der Server-Hardware installiert, betrieben und stellt Schnittstellen zu der darunterliegenden Hardware-Peripherie (Netz, Speicher, RAID-Controller, etc.) zur Verfügung. Es steuert die Ausführung von Diensten und deren Zugriffe auf die Schnittstellen. Zentraler Bestandteil des Betriebssystems ist der Betriebssystemkern. Der Betriebssystemkern (engl. Kernel) ist die erste Komponente, die beim Starten des Betriebssystems geladen wird. Zu den wesentlichen Aufgaben des Betriebssystemkerns gehören:

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

Der Betriebssystemkern stellt Funktionen zur Verfügung, über die auf Hardware und Betriebsmittel zugegriffen werden können. Der Zugriff auf die Hardware erfolgt über Gerätetreiber. Diese werden von dem Betriebssystemhersteller oder ggf. auch von dem Hersteller der Hardware-Komponente zur Verfügung gestellt.

Die Administration des Betriebssystems erfolgt über eine Benutzeroberfläche. Diese kann je nach eingesetztem Betriebssystem und dessen Installationsumfang textbasiert (als Kommandozeileninterpreter) oder als grafische Oberfläche (Graphical User Interface, GUI) bereitgestellt werden.

2.1.4 Dienste

Dienste bieten sowohl lokal als auch über das Rechnernetz Funktionen an, die von Client-Systemen genutzt werden können. Durch das Betriebssystem haben die Dienste Zugriff auf Betriebsmittel wie z. B. Hardware, externe Schnittstellen und Peripheriegeräte. Die Schnittstellen zum Betriebssystem werden über Bibliotheken bereitgestellt, die sowohl vom Betriebssystem als auch von den Diensten mitgeliefert werden können. Die meisten Betriebssysteme bringen bereits eine Vielzahl von Diensten mit, die ggf. vor der Verwendung installiert oder aktiviert werden müssen. Ist der benötigte Dienst nicht Bestandteil des Betriebssystems, dann muss dieser als zusätzliche Software-Komponente installiert werden.

Die Nutzung von Diensten kann in zwei unterschiedlichen Kategorien aufgeteilt werden. Die erste stellt ihren Dienst frei zur Verfügung, wobei die Nutzung ohne Authentisierung des Benutzers möglich ist. Beispiele hierfür sind DNS, DHCP oder NTP. Die zweite Kategorie erfordert hingegen eine Authentisierung des Benutzers vor der Benutzung des Dienstes, um z. B. den Zugriff auf vertrauliche Informationen zu schützen. Beispiele hierfür sind E-Mail (SMTP, POP3, IMAP), SSH oder RDP.

2.1.5 Einbettung eines Servers in ein Rechnernetz

Die Aufgabe eines Servers ist die permanente Bereitstellung von Diensten über das Rechnernetz. Die Anbindung an das Netz findet über Netzwerkkarten statt. Heutzutage erfolgt die physische Anbindung eines Servers überwiegend über Ethernet. Mehrere an das Ethernet angeschlossene Geräte (Server, Arbeitsplatz-PCs, etc.) bilden ein Rechnernetz.

Auf Ethernet bauen die Protokolle auf, die für die Kommunikation zwischen Rechnern in einem Rechnernetz erforderlich sind. Üblicherweise wird hier das Protokoll IP in der Version 4 (IPv4) verwendet und zunehmend auch IPv6 (siehe auch [ISi-LANA]). Über diese Basistechnologie bietet ein Server unterschiedliche Dienste an, die auf offenen oder proprietären Protokollen aufbauen. Diese sind z. B.

- Domain Name Service (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Time Protocol (NTP)
- Hypertext Transfer Protocol (HTTP)
- Lightweight Directory Access Protocol (LDAP).

2.2 Benutzer und Rechte

Um sich als Benutzer oder Administrator an einem Server anzumelden, wird ein Benutzerkonto benötigt. Dem Benutzerkonto sind Berechtigungen zugeordnet, die beschreiben, welche Operationen (lesen, schreiben, ausführen von Dateien) der Benutzer ausführen darf. Konfiguriert werden die Benutzer und Berechtigungen durch eine Benutzerverwaltung, auf die das Betriebssystem zugreift. Nachfolgend werden diese Punkte weiter erläutert.

2.2.1 Benutzerkonten, Gruppen und Rechte

Die Rechte von Benutzern lassen sich in zwei unterschiedliche Rollen aufteilen: die des Anwenders und die des Administrators. Der Anwender greift normalerweise ausschließlich über das Rechnernetz auf Dienste eines Servers zu und ist mit geringeren Rechten ausgestattet als ein Administrator. Administratoren sind für die Konfiguration und Wartung des Servers zuständig und greifen sowohl über das Rechnernetz als auch lokal, über eine Konsole, auf Server zu. Der Verzicht auf Administratorrechte für normale Anwender schützt das Betriebssystem und die Konfiguration des Servers vor versehentlicher, fahrlässiger oder vorsätzlicher Modifikation.

Einige zur Verfügung gestellte Dienste eines Servers verlangen eine Authentisierung des Benutzers, bevor der Dienst genutzt werden kann. Die Authentisierung eines Benutzers durch den Server erfordert ein Benutzerkonto. Es muss entweder lokal auf dem Server vorhanden sein oder kann über eine zentrale Benutzerverwaltung (z. B. Active Directory oder LDAP) zur Verfügung gestellt werden (siehe auch Abschnitt 2.2.2).

Benutzer können außerdem in Gruppen zusammengefasst werden, welche die Berechtigungen für alle Mitglieder dieser Gruppe definieren. Dies erleichtert die Administration, da nicht jeder Benutzer einzeln verwaltet werden muss, sondern einfach einer vorhandenen Gruppe hinzugefügt wird.

Benutzerkonten und Dienste

Die vom Server zur Verfügung gestellten Dienste laufen lokal mit den Rechten eines Benutzers. Wie bei realen Benutzern beschreibt auch hier das Benutzerkonto, welche Rechte ein Dienst hat. Dazu gehören z. B. das Lesen oder Schreiben von Dateien und der Zugriff auf Systemdateien.

2.2.2 Benutzerverwaltung

Benutzerkonten können sowohl lokal auf einem Server als auch von einer zentralen Benutzerverwaltung zur Verfügung gestellt werden. Bei der lokalen Benutzerverwaltung muss auf jedem Server separat das Anlegen von Benutzern sowie die Pflege der Benutzerinformationen, deren Berechtigungen und dessen Gruppenzugehörigkeit vorgenommen werden. Ab einer bestimmten Anzahl von Servern wird dies sehr aufwendig. Daher ist es einfacher und weniger fehleranfällig, die Benutzer zentral zu verwalten.

Eine zentrale Benutzerverwaltung bietet den Vorteil, dass Benutzerkonten nicht auf jedem einzelnen Server angelegt, gelöscht oder die Berechtigungen geändert werden müssen. Dies kann einmal an der zentralen Stelle erfolgen und alle Systeme, die die zentrale Benutzerverwaltung nutzen, haben ebenfalls Zugriff auf diese Änderungen. Meistens wird dies über einen Verzeichnisdienst realisiert. Beispiele für einen Verzeichnisdienst sind Microsoft Active Directory oder das Lightweight Directory Access Protocol (LDAP).

Neben Benutzerinformationen wie Benutzerkennung, vollständiger Benutzername, Passwort, etc. können über eine zentrale Benutzerverwaltung auch Gruppenzugehörigkeiten, die Gültigkeit oder auch das Deaktivieren des Benutzerkontos konfiguriert werden.

Bei der Anbindung der zentralen Benutzerverwaltung ist darauf zu achten, dass die Übermittlung der Daten zwischen dem Server und der Benutzerverwaltung verschlüsselt erfolgt, da hierüber auch die Authentisierungsinformationen (Benutzername und Passwort) übermittelt werden. Bei der Verwendung von LDAP wird z. B. das Passwort unverschlüsselt übertragen. Diese Daten können

von Angreifern durch das Mitlesen der Kommunikation abgefangen werden. In diesem Fall sollte LDAPS oder Secure-LDAP verwendet werden.

2.3 Techniken und Komponenten zur Absicherung des Servers

Dieser Abschnitt beschreibt die Grundlagen eines sicher konfigurierten Betriebssystems, welches auf ein Minimalsystem basiert. Dieses Minimalsystem enthält nur die Komponenten des Betriebssystems, die für den Betrieb erforderlich sind. Nachfolgend werden die Anforderungen an ein Minimalsystem sowie weitere Komponenten vorgestellt, die die Funktionalität des Minimalsystems erweitern bzw. dessen Sicherheit erhöhen.

2.3.1 Minimalsystem

Ein Minimalsystem ist das Ergebnis der Minimalisierung des Betriebssystems und der darauf betriebenen Dienste. Ein Minimalsystem soll eine möglichst geringe Angriffsfläche für Bedrohungen bieten und zeichnet sich durch die folgenden Eigenschaften aus:

- Das Betriebssystem wird nur mit den für den Betrieb notwendigen Komponenten installiert.
- Nur für den Betrieb und für den geplanten Einsatzzweck benötigte Dienste dürfen auf dem Betriebssystem installiert werden.
- Es soll eine Minimierung der zur Verfügung gestellten Schnittstellen erfolgen. Schnittstellen können sowohl physisch als auch über Programme oder Programmbibliotheken (engl. shared libraries) bereitgestellt werden. Nicht benötigte Schnittstellen sind zu deaktivieren oder zu deinstallieren.

Nach der Minimalinstallation folgt die sichere Konfiguration des Betriebssystems. Dies umfasst u. a. die Analyse der laufenden Prozesse, der im Netz zur Verfügung gestellten Programme und der auf dem Betriebssystem installierten Programme. Nicht benötigte Komponenten müssen entfernt oder deaktiviert werden.

2.3.2 Verschlüsselung von Datenträgern

Abhängig von dem eingesetzten Produkt zur Festplattenverschlüsselung können einzelne Partitionen oder auch die gesamte Festplatte inklusive Bootsektor und Systempartition, auf der das Betriebssystem gespeichert ist, verschlüsselt werden. Der Zugriff auf diese Partitionen und damit die Entschlüsselung der Daten erfolgt erst nach der Eingabe eines Passwortes oder Schlüssels.

Eine Verschlüsselung von Datenträgern im Serverbereich kann erforderlich sein, um die Vertraulichkeit von Daten beim Verlust eines Datenträgers zu gewährleisten, z. B. bei Diebstahl eines Datenträgers. Dies ist gerade im Serverbereich sehr einfach, da Festplatten oft als Hot-Swap Komponenten aufgebaut sind und im Betrieb herausgezogen werden können, ohne das Gehäuse eines Servers zu öffnen.

Ein weiterer Grund für die Verschlüsselung von Datenträgern ist der Schutz der Vertraulichkeit von Daten bei der Außerbetriebnahme eines Datenträgers oder eines Servers. Dies kann z. B. der Austausch einer Festplatte bei einem Hardwareschaden im Garantiefall sein, wenn kein Löschen der Daten möglich ist.

2.3.3 Verschlüsselung von einzelnen Daten

Bei der Verschlüsselung von einzelnen Daten wird nicht die gesamte Festplatte verschlüsselt, sondern nur einzelne Bereiche auf der Festplatte (z. B. einzelne Dateien oder Verzeichnisse). Die Verschlüsselung von Daten kann eingesetzt werden, um die Vertraulichkeit bei der Speicherung zu gewährleisten. Sensitive Daten (wie z. B. Passwörter) müssen verschlüsselt auf dem Datenträger hinterlegt werden, damit bei einem Diebstahl nicht auf diese Daten zugegriffen werden kann.

2.3.4 TPM (Trusted Platform Module)

Das Trusted Platform Module (TPM) ist ein fester Bestandteil der Hauptplatine eines Servers, das diesen um Sicherheitsfunktionen erweitert. Das TPM kann unter anderem kryptografische Schlüssel für Public-Key-Verfahren erzeugen und speichern sowie Zufallszahlen generieren. Die gespeicherten, privaten Schlüssel verlassen zu keinem Zeitpunkt das TPM, dadurch sind die privaten Schlüssel vor dem Zugriff durch Dritte oder durch Schadprogramme geschützt.

Ein TPM kann z. B. zur Speicherung der kryptografischen Schlüssel für eine Festplattenverschlüsselung genutzt werden. Abhängig von dem eingesetzten Programm lässt sich damit auch der gesamte Bootvorgang des Betriebssystems kryptografisch absichern. Hierzu werden Prüfsummen der zu ladenden Bestandteile des Bootvorgangs (u. a. Master Boot Record, BIOS, Bootloader) in dem TPM sicher gespeichert (Platform Configuration Registers (PCR)) und können von Dritten später verifiziert werden (Remote Attestation), sodass eine Manipulation der Komponenten ausgeschlossen werden kann.

Ein weiterer Einsatzzweck eines TPMs ist die sichere Hinterlegung eines Schlüssels, der für die Verschlüsselung von Daten verwendet werden kann. Dies wird z. B. zur Speicherung eines privaten Schlüssels einer Zertifizierungsstelle zum Ausstellen von Zertifikaten genutzt.

Um TPM in Betriebssystemen oder Applikationen einzusetzen, muss sichergestellt sein, dass diese die Nutzung eines TPM unterstützen und dass die verwendete Hardware ein TPM besitzt. Nicht alle aktuellen Betriebssysteme bieten z. B. Gerätetreiber für die Verwendung eines TPMs an.

2.3.5 Virtualisierung

Ziel der Server-Virtualisierung ist die Konsolidierung von Hardware, d. h. eine bessere Nutzung von Ressourcen. Dadurch werden Energie und Kosten eingespart.

Bei der Virtualisierung von IT-Systemen werden ein oder mehrere Instanzen des gleichen oder unterschiedlicher Betriebssysteme auf einem physischen Server betrieben. Ein solcher physischer Server wird als Virtualisierungsserver bezeichnet. Ein Virtualisierungsserver stellt eine Ausführungsumgebung für Betriebssysteme zur Verfügung, d. h die Ressourcen, die bei herkömmlichen Rechnern physisch realisiert wurden (Arbeitsspeicher, Prozessor, Festplatten, etc.), werden vollständig oder teilweise emuliert. Das in der virtuellen Maschine ausgeführte Betriebssystem wird Gast-Betriebssystem oder kurz Gastsystem genannt.

Die Gast-Betriebssysteme wissen nicht, dass die Hardware, die sie nutzen, mit anderen Betriebssystemen geteilt wird. Aus der Perspektive des jeweiligen virtuellen Betriebssystems sieht es so aus, als ob es alleine über die vollständigen Ressourcen der darunter liegenden Hardware verfügt.

Die Basis einer Virtualisierungsumgebung ist ein sogenannter Hypervisor oder auch Virtual Machine Monitor (VMM). Der Hypervisor ist für die Kontrolle des Prozessors und aller Ressourcen (Festplattenspeicher, Arbeitsspeicher, Netzwerkkarten, etc.) zuständig und weist diese dem

jeweiligen Gastsystem nach Bedarf zu. Damit wird für eine Kapselung der Gastsysteme gesorgt und unberechtigte oder unverhältnismäßige Zugriffe auf die Ressourcen verhindert. Eine weitere Aufgabe des Hypervisors ist es, die einzelnen Gastsysteme voneinander zu isolieren damit diese sich nicht gegenseitig während des Betriebs stören. Die Isolierung bewirkt weiterhin, dass die Gastsysteme nicht unberechtigt, sondern nur über dafür vorgesehene Mechanismen kommunizieren oder auf die Daten der anderen Gastsysteme zugreifen.

Im folgenden wird kurz auf die unterschiedlichen Virtualisierungstechniken eingegangen.

2.3.5.1 Virtualisierungstechniken

Im Serverbereich werden verschiedene Virtualisierungstechniken unterschieden, diese werden im Folgenden erläutert.

Hypervisorbasierte Virtualisierung

Im Gegensatz zur hostbasierten Virtualisierung wird bei der hypervisorbasierten Virtualisierung der Hypervisor bzw. VMM direkt auf der Hardware ausgeführt. Er umfasst damit auch das Host-Betriebssystem, das allerdings stark für den Einsatz als Virtualisierungsumgebung optimiert ist (siehe Abbildung 2.5). Es ist nicht möglich, normale Anwendungen darauf auszuführen. Wie bei der hostbasierten Virtualisierung können unterschiedliche Betriebssysteme virtualisiert werden. Ebenso „weiß“ das Gastsystem nicht, dass es virtualisiert läuft, d.h. es kann ohne Modifikationen betrieben werden.

Aufgabe des Hypervisor ist die Bereitstellung der virtuellen Maschinen sowie die Zuteilung und Verwaltung der vorhandenen Hardware-Ressourcen. Insbesondere in letztem Punkt zeigt sich der Unterschied zur hostbasierten Virtualisierung: die Zuteilung der Ressourcen wird dort vom Host-Betriebssystem vorgenommen, die Virtualisierungsumgebung hat darauf keinen Einfluss. Die hypervisorbasierte Virtualisierung wird häufig auch als bare-metal-Virtualisierung oder „Virtualisierung Typ 1 bezeichnet.

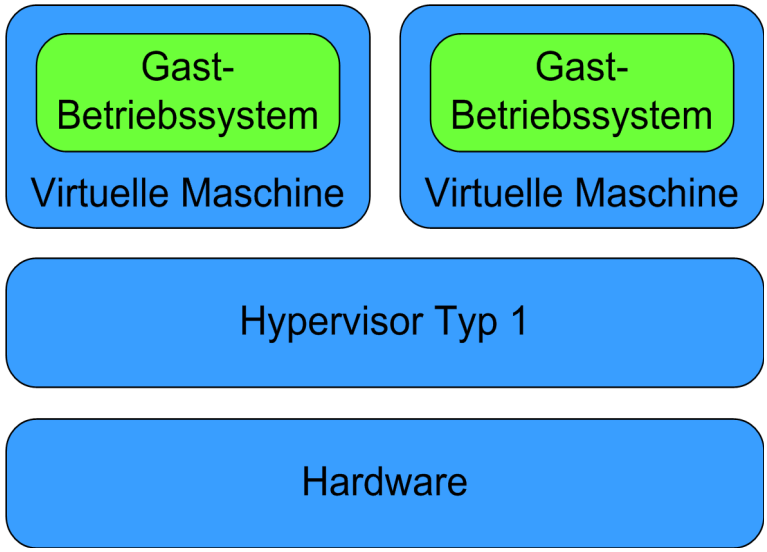


Abbildung 2.2: Schematischer Aufbau eines Hypervisors vom Typ 1

Hostbasierte Virtualisierung

Die hostbasierte Virtualisierung ist hinsichtlich der Gastsysteme flexibler als die Betriebssystemvirtualisierung. Hier ist es möglich, unterschiedliche Betriebssysteme auf einem Host zu betreiben. Bei dieser Lösung wird die Virtualisierungsumgebung bzw. der Hypervisor auf dem Host-Betriebssystem installiert und läuft als normale Anwendung neben anderen Programmen, z. B. Textverarbeitung oder Browser (siehe Abbildung 2.3). Das Gast-Betriebssystem kann ohne Modifikationen, wie die Anpassung von Treibern, in der virtuellen Maschine installiert werden und nutzt seinen eigenen Betriebssystemkern. Anders ausgedrückt verhält es sich genauso, wie wenn es auf physischer Hardware betrieben werden würde.

Obwohl die Hardware-Umgebung in großen Teilen nachgebildet wird, ist eine sehr performante Virtualisierung möglich. Grund hierfür ist, dass die meisten der vom Gast-Betriebssystem abgesetzten Befehle direkt an die Hardware weitergereicht werden können. Nur wenige Befehle, vor allem die, die im privilegierten Raum ausgeführt werden, müssen von der Virtualisierungsumgebung abgefangen und behandelt werden. Beispiele hierfür sind Interrupts oder Zugriffe auf den Arbeitsspeicher.

Vorteil dieser Lösung ist, dass ein schnelles unkompliziertes Aufsetzen der Virtualisierungsumgebung möglich ist. Nachteile sind, dass von einem Absturz des Host-Betriebssystems auch die virtuelle Maschine betroffen ist. Weiterhin ist die Zuteilung der Hardware-Ressourcen an die Virtualisierungsumgebung von dem Host-Betriebssystem abhängig, es kann keine feste Zuteilung vorgenommen werden.

Diese Art der Virtualisierung wird auch als Typ 2-Virtualisierung bezeichnet.

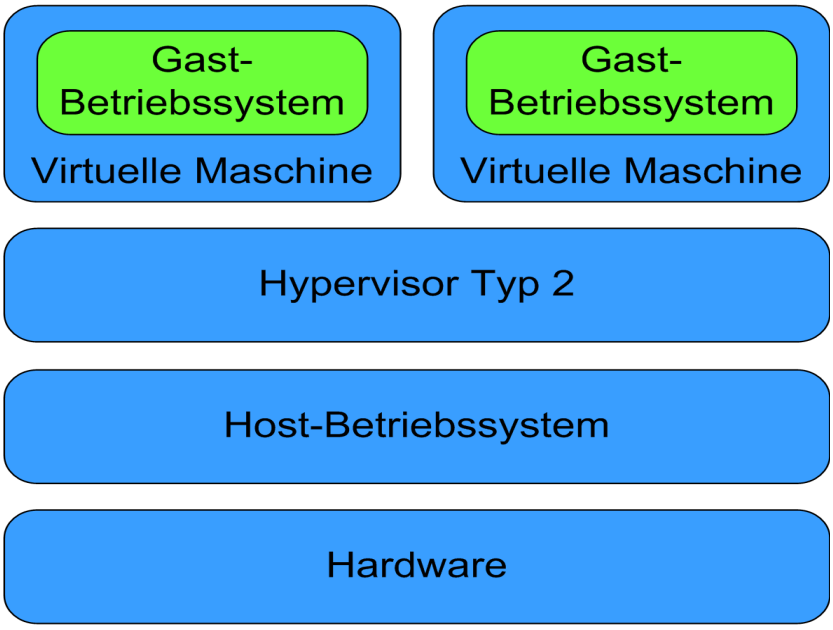


Abbildung 2.3: Hostbasierte Virtualisierung

Betriebssystemvirtualisierung

Bei der Betriebssystemvirtualisierung laufen mehrere isolierte Betriebssystem-Instanzen des Host-Betriebssystems nebeneinander (siehe Abbildung 2.3). Diese virtuellen Instanzen werden meist Container (z. B. bei Sun Solaris) oder auch Jails (z. B. bei FreeBSD) genannt. Sie bekommen ihre Ressourcen wie Dateisystem, IP-Adresse, Hostname und Speicherbereiche vom Host-Betriebssystem zugewiesen. Speicherbereiche und Ein-/Ausgabebereiche der Gastsysteme sind streng getrennt, allerdings nutzen sie den Betriebssystemkern, die Softwarebibliotheken und Hardware-

ressourcen des Host-Betriebssystems. Daraus folgt, dass das Gast-Betriebssystem das gleiche wie das Host-Betriebssystem sein muss.

Diese Form der Virtualisierung ist sehr effizient, da viele Ressourcen wie z. B. der Betriebssystemkern gemeinsam genutzt werden und dadurch nur wenig Befehle von der virtuellen in die physische Umgebung umgesetzt werden müssen. Gleichzeitig ergibt sich daraus auch die Einschränkung, dass es nicht möglich ist, unterschiedliche Betriebssysteme auf einem Virtualisierungsserver einzusetzen. Bei einigen Produkten können allerdings verschiedene Versionen des Betriebssystemkerns des Host-Betriebssystems gleichzeitig genutzt werden. Eine weitere Einschränkung der Betriebssystemvirtualisierung ist, dass bestimmte Hardware-Komponenten nur von einer einzigen Betriebssysteminstanz verwendet werden können (z. B. ISDN-Karten).

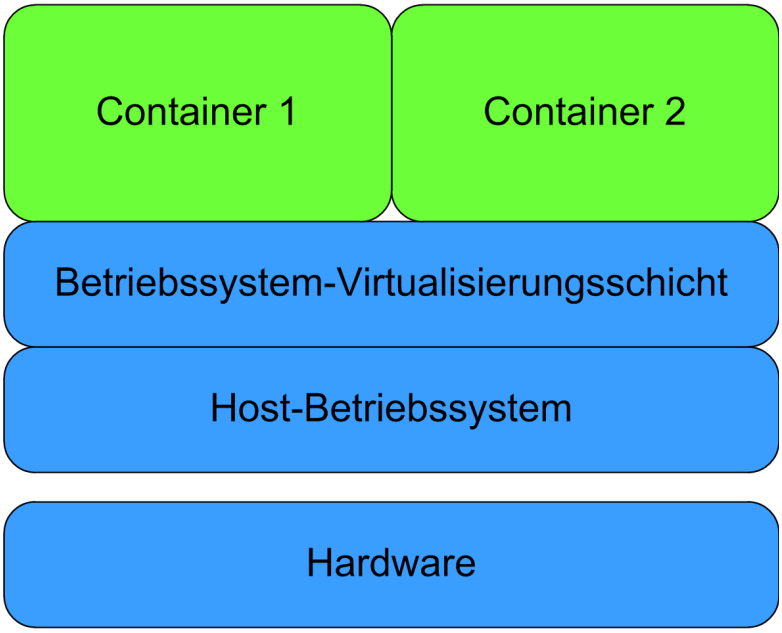


Abbildung 2.4: Schematischer Aufbau der Betriebssystemvirtualisierung

Paravirtualisierung

Wie bei der host- und hypervisorbasierten Virtualisierung können bei der Paravirtualisierung unterschiedliche Betriebssysteme auf einem Host virtualisiert werden. Der wesentliche Unterschied ist, dass eine Anpassung der Gast-Betriebssysteme erfolgen muss. Dies hat zur Folge, dass die Behandlung privilegierter Systemaufrufe der Gastsysteme nicht der Hypervisor übernimmt, sondern durch die Gastsysteme selbst erledigt wird. Zusätzlich zu den Gastsystemen läuft auf dem Virtualisierungsserver ein virtualisiertes privilegiertes Betriebssystem, das Management-Aufgaben in der Virtualisierungsumgebung übernimmt. Die zuvor erwähnte Anpassung der Gastsysteme bewirkt außerdem, dass sie die Treiber des Management-Systems mitbenutzen. Auf diese Weise muss der Hypervisor keine eigenen Treiber für die Gastsysteme bereitstellen.

x86-Prozessoren mit Virtualisierungsunterstützung

Der Einsatz von Prozessoren mit Virtualisierungsunterstützung (Intel-VT oder AMD-V) führt dazu, dass Befehle, die zuvor der Hypervisor abfangen und umsetzen musste, direkt an den Prozessor weitergegeben werden können. Auf diese Weise wird eine performante Virtualisierung erreicht.

Vollständige Virtualisierung oder Emulation

Diese Form der Virtualisierung spielt im Serverbereich keine große Rolle, sie soll jedoch der Vollständigkeit halber kurz erwähnt werden. Die vollständige Virtualisierung gleicht der hostbasierten Virtualisierung mit dem Unterschied, dass eine komplette Hardware-Umgebung nachgebildet wird. Die reale Hardware wird vollständig vor dem Gast-Betriebssystem verborgen. Diese Form der Virtualisierung ist nicht sehr performant, da die Virtualisierungsumgebung aufwendig die Hardware für die Gastsysteme nachbilden muss und Kontextwechsel dementsprechend sehr viel Ressourcen und Zeit kosten.

Kapselung und Isolation der verschiedenen Virtualisierungstechniken

Je stärker die virtuellen IT-Systeme auf dem Virtualisierungsserver isoliert sind, desto eher eignet sich das Virtualisierungsprodukt dazu, unterschiedliche Dienste in den verschiedenen virtuellen IT-Systemen zu betreiben. Die folgenden Grundsätze lassen sich für eine erste Beurteilung heranziehen:

- Auf Virtualisierungsservern mit einer Betriebssystemvirtualisierung ist die Isolierung des Gastsystems im Vergleich zu den anderen Virtualisierungstechniken am geringsten. Daher sollten die virtuellen IT-Systeme den gleichen Dienst anbieten. So sollten auf einem solchen Virtualisierungsserver beispielsweise ausschließlich Web-Server oder ausschließlich Mail-Server, aber keine Mischung aus diesen Gruppen betrieben werden.
- Auf Virtualisierungsservern mit einer Servervirtualisierung (Typ 1 + Typ 2) ist es zulässig, virtuelle IT-Systeme mit unterschiedlichen Diensten zu betreiben. Es können Web-Server und Mail-Server auf einem Virtualisierungsserver in jeweils getrennten virtuellen IT-Systemen bereitgestellt werden.
- Auf Virtualisierungsservern sollten ausschließlich virtuelle IT-Systeme gleichen Schutzbedarfs betrieben werden. Ein Betrieb von Systemen unterschiedlichen Schutzbedarfs auf einem Virtualisierungsserver wird nicht empfohlen. Die Virtualisierung von IT-Systemen mit hohem Schutzbedarf ist im Einzelfall abhängig von den Anwendungen und der eingesetzten Virtualisierungstechnologie.

2.3.5.2 Weitere Grundlagen zur Virtualisierung

Bei dem Einsatz von Virtualisierungstechnologien werden häufig noch weitere Techniken verwendet, die nachfolgend beschrieben werden. Je nach Konfiguration können diese Techniken die Sicherheit eines Virtualisierungsservers stärken oder schwächen. Auf Details zur Konfiguration wird in Abschnitt 4 eingegangen.

Live Migration

Die Live Migration erlaubt es, ein virtuelles IT-System sehr einfach von einem Virtualisierungsserver auf einen anderen zu verschieben. Dies wird z. B. zu Wartungszwecken der Hardware benötigt.

Dynamische Speicherverwaltung

Bei einigen Virtualisierungsprodukten kann den einzelnen virtuellen IT-Systemen in Summe mehr Arbeitsspeicher zugewiesen werden, als auf dem Virtualisierungsserver insgesamt vorhanden ist. Einem einzelnen virtuellen IT-System kann allerdings nicht mehr Speicher zugewiesen werden, als

dem Hypervisor zur Verfügung steht. Um diese sogenannte Überbuchung zu ermöglichen, wird den virtuellen IT-Systemen nicht der gesamte konfigurierte Arbeitsspeicher zugeteilt, sondern nur soviel Arbeitsspeicher, wie in dem Moment von dem virtuellen Betriebssystem benötigt wird.

Snapshots

Einige Virtualisierungsprodukte bieten die Möglichkeit, den Zustand eines virtuellen IT-Systems in Form eines sogenannten Snapshots der virtuellen Festplatte einzufrieren. Werden Änderungen am virtuellen IT-System vorgenommen, nachdem der Snapshot erstellt wurde, dann werden diese Änderungen in eine Differenzdatei geschrieben. Der eigentliche Dateicontainer der virtuellen Festplatte bleibt dabei unverändert. Wird der Snapshot des virtuellen IT-Systems gelöscht, werden die Änderungen in der Differenzdatei auf den Dateicontainer der virtuellen Datenträger angewandt und die Differenzdatei selbst wird gelöscht. Dies bietet den Vorteil, dass Änderungen an dem virtuellen IT-System durchgeführt werden können (z. B. Softwareinstallation oder Konfigurationsänderungen) und diese Änderungen durch Wiederherstellen des ursprünglich erstelltem Snapshots wieder verworfen werden können.

Gastwerkzeuge

Einige Hersteller stellen für die virtuellen IT-Systeme Gastwerkzeuge zur Verfügung. Wie der Name schon sagt, werden Gastwerkzeuge in den Gast-Betriebssystemen installiert und ermöglichen eine deutlich bessere Performanz der virtuellen Maschine. Dies wird durch speziell auf die Virtualisierungsumgebung zugeschnittene Treiber erreicht. Weiterhin ermöglichen die Gastwerkzeuge sehr einfach die Kommunikation zwischen den virtuellen Maschinen sowie zusätzliche Steuerungsmöglichkeiten der virtuellen Maschine durch den Host, beispielsweise das kontrollierte Herunterfahren des Gast-Betriebssystems.

2.3.6 Virenschutzprogramm

Ein Virenschutzprogramm schützt vor den Gefahren durch Schadprogramme, wie beispielsweise Viren, Würmer und Trojanische Pferde, indem diese frühzeitig erkannt und beseitigt werden. Systeme, die direkten Zugriff auf das Internet haben (z. B. SMTP-Server, FTP-Server, Web-Server), sind durch den permanenten Austausch von Daten einer höheren Bedrohung durch Schadprogramme ausgesetzt, als Server aus einem internen Netz (z. B. LDAP, Datenbanken, etc.). Um vor den Gefahren eines Virenbefalls zu schützen, sollte auf diesen Systemen ein Virenschutzprogramm eingesetzt werden.

Eine zentrale Prüfung der eingehenden Daten auf Schadprogramme findet bereits am Application Level Gateway (ALG) und am E-Mail-Server statt (siehe [ISi-LANA], [ISi-Web-Server] und [ISi-Mail-Server]). Es kann jedoch nicht ausgeschlossen werden, dass Schadprogramme diese zentrale Prüfung unbemerkt passieren. Zum Beispiel könnte ein E-Mail-Anhang mit Schadcode, für den zum Zeitpunkt des Empfangs noch keine Signatur verfügbar war und der somit nicht erkannt wurde, an einen weiteren Server (z. B. POP3, IMAP) ausgeliefert werden. In einem solchen Fall bietet die erneute Prüfung auf Schadprogramme auf dem APC und gegebenfalls auf dem File-Server selbst einen zusätzlichen Schutz.

Um die Erkennungsrate zu erhöhen, können auf unterschiedlichen IT-Systemen Virenschutzprogramme eingesetzt werden, die eine jeweils andere Such-Engine verwenden.

2.3.7 Ausführungskontrolle

Die Ausführungskontrolle überwacht ausführbare Dateien daraufhin, ob diese gestartet werden dürfen. Dies erfolgt z. B. über eine sogenannte Whitelist, in der nur zugelassene Programme definiert sind. Sollen Programme gestartet werden, die nicht in dieser Liste eingetragen sind, dann verhindert die Ausführungskontrolle den Start des entsprechenden Programms. Dies soll z. B. verhindern, dass Programme aus nicht vertrauenswürdigen Quellen Schaden an Betriebssystem oder Daten anrichten. Die Ausführungskontrolle wird auch prozessbasierte Integritätsprüfung genannt.

2.3.8 Integritätsprüfung

Die Integritätsprüfung überwacht Änderungen von Dateien, um ungewollte oder durch einen Angreifer beabsichtigte Modifikationen zu erkennen. Der Server wird hierbei auf Veränderungen gegenüber eines zuvor ermittelten Referenzzustandes kontrolliert. Zur Ermittlung des Referenzzustandes werden Prüfsummen von den zu überwachenden Dateien gebildet, die zentral abgelegt werden. Auf den überwachten Systemen ist ein Dienst aktiv, der den Dateizugriff überwacht und bei möglichen Modifikationen die Prüfsumme neu berechnet und mit dem Referenzwert vergleicht. Stimmen diese nicht überein, erfolgt eine Benachrichtigung an das zentrale System, das dann weitere Aktionen (z B. Alarmierung von zuständigen Personen) durchführt.

Die Überwachung der Dateien erfolgt zeitnah. Hierbei werden unterschiedliche Methoden verwendet, um eine Modifikation möglichst schnell zu entdecken. Einige Produkte prüfen die Prüfsummen der Dateien durch sogenanntes Polling, d. h. die Dateien werden regelmäßig in kurzen Abständen hinsichtlich Änderungen überprüft. Andere Produkte bieten eine Überprüfung nahezu in Echtzeit an. Diese Produkte nutzen dieselbe Schnittstelle des Betriebssystems, die z. B. von Virenschutzprogrammen verwendet wird. Über diese Schnittstelle wird die Integritätsprüfung darüber informiert, dass lesend oder schreibend auf eine Datei zugegriffen wurde. Im Falle des schreibenden Zugriffs finden nach dem Schließen der Datei eine Neuberechnung der Prüfsumme und ein Vergleich des Ergebnisses mit der Referenzdatenbank statt. Dies ermöglicht eine effiziente Integritätsüberwachung von Dateien und vermindert die Systemlast des Servers.

2.3.9 Lokaler Paketfilter

Ein lokaler Paketfilter kann als separate Software-Komponente (ähnlich einer Personal Firewall eines Arbeitsplatz-PCs) oder als Bestandteil des Betriebssystems auf einem Server installiert werden. Aufgabe des Paketfilters ist es, unerwünschte Kommunikation zwischen Rechnernetz und Server zu unterbinden. Hierzu werden Regeln definiert, die festlegen, welche Kommunikationsverbindungen erlaubt sind. Daten, die nicht den Regeln entsprechen (z. B. unbekannte Quell-IP-Adresse), werden vom Paketfilter verworfen und nicht weiter verarbeitet. Der lokale Paketfilter muss so konfiguriert sein, dass nur die eingehenden bzw. ausgehenden Verbindungen erlaubt sind, die für die Funktionalität und die Bereitstellung der Dienste des Servers benötigt werden.

2.3.10 Fernadministration

Unter Fernadministration versteht man die Administration von Servern über das Netz. Dies kann sowohl über das lokale Netz als auch über das Internet erfolgen. Weitere Informationen hierzu sind in den Studien [ISi-Fern] und [ISi-LANA] nachzulesen.

2.3.11 Monitoring

Durch das Monitoring von Server-Systemen wird die Verfügbarkeit von Hardware, Betriebssystem und den darauf betriebenen Diensten sichergestellt. Eine zentrale Management-Komponente überprüft hierzu in regelmäßigen Abständen alle konfigurierten Server und Dienste auf korrekte Funktionsweise. Die Kommunikation zu den Systemen, die beobachtet werden, erfolgt über Standardprotokolle oder durch proprietäre Agenten, die auf den Betriebssystemen installiert werden müssen. Nachfolgend werden die verbreitetsten Protokolle aufgeführt. Darüber hinaus gibt es weitere standardisierte und proprietäre Protokolle, die hier aber nicht weiter behandelt werden.

SNMP (Simple Network Management Protocol)

Das Simple Network Management Protocol ist ein Netzprotokoll, das sowohl für das Monitoring als auch für die Steuerung von Netzelementen (Router, Switches, Server, etc.) verwendet werden kann. SNMP ermöglicht u. a.

- das Monitoring von Netz-Komponenten. Hierzu gehören z. B. das Auslesen von Systemvariablen, Temperaturen, Informationen über laufende Prozesse, Speicherausnutzung, etc.
- die Fernsteuerung und Fernkonfiguration von Netz-Komponenten. Mittels SNMP ist es auch möglich, Konfigurationseinstellungen an der überwachten Netz-Komponente vorzunehmen. Dazu gehört z. B. das Setzen von Betriebssystemparametern oder das Ausführen von eigenen Skripten.
- die Fehlererkennung und Fehlerbenachrichtigung. Mit SNMP kann ein Server einem zentralen Monitoring aktiv Ereignisse und Änderungen mitteilen. Dies erfolgt durch das Senden von sogenannten SNMP Traps. Bei einem Monitoring durch Polling (zyklisches Abfragen von Ereignissen) kann z. B. ein kritisches Ereignis nicht rechtzeitig bemerkt werden. Durch die Möglichkeit der Fehlerbenachrichtigung ist eine Echtzeitüberwachung möglich.

SNMP existiert derzeit in drei unterschiedlichen Versionen. Die Versionen 1 und 2 bieten fast keine Sicherheitsmechanismen und sollten nicht mehr eingesetzt werden. SNMPv1 überträgt z. B. Passwörter im Klartext. Erst in Version 3 wurden umfangreiche Sicherheitsmechanismen zur Authentifizierung, Verschlüsselung und Zugriffskontrolle eingeführt.

WBEM (Web Based Enterprise Management)

WBEM ist ein Standard der Desktop Management Task Force (DMTF) für das Netz- und Systemmanagement und wird zur Verwaltung von Netz- und Systemressourcen (z. B. Hardware, Software, Benutzer) eingesetzt. Eine Komponente von WBEM ist das Common Information Model (CIM), welches einheitliche Schnittstellen definiert, über die es möglich ist, auf Geräte und Anwendungen von unterschiedlichen Herstellern zuzugreifen. Dies ermöglicht es z. B. Konfigurationen von Geräten abzufragen oder Einstellungen vorzunehmen und bietet ähnliche Funktionalitäten wie SNMP.

Die Daten werden mittels Extensible Markup Language (XML) kodiert und in der Regel über das Hypertext Transfer Protocol (HTTP) übertragen. Der Einsatz von HTTP bietet den Vorteil, dass auch SSL (HTTPS) zur Verschlüsselung der übertragenen Daten eingesetzt werden kann.

Eine bekannte Implementierung von WBEM ist z. B. die Windows Management Instrumentation (WMI).

2.3.12 Hardware-Management

Heutige Serverhardware bietet Schnittstellen an, um ein Remote-Management durchzuführen. Diese ermöglichen unabhängig vom installierten Betriebssystem auch im heruntergefahrenen Zustand den Zugriff auf das System. Dazu muss das System lediglich an die Spannungsversorgung angeschlossen sein und über eine konfigurierte und angebundene Remote-Management-Schnittstelle verfügen. Über diese Schnittstellen kann z. B. der Hardwarestatus von Komponenten abgefragt oder das System gestartet oder heruntergefahren werden. Eine herstellerübergreifende Schnittstelle wird über das Intelligent Platform Management Interface (IPMI) bereitgestellt.

Mittels IPMI kann sowohl über eine serielle Verbindung als auch über das Netz mit einem Server kommuniziert werden. Diese Schnittstellen können zum Abruf von Informationen über den Hardwarestatus genutzt werden. Unter anderem sind dies folgende Informationen:

- Spannungsversorgung des Netzteils und die zur Verfügung gestellten Spannungswerte
- Status und Temperatur der eingebauten Prozessoren
- Status und Drehzahl der eingebauten Lüfter
- Status der eingebauten Festplatten.

Einige Hersteller bieten auch eigene Schnittstellen an, die sich allerdings in ihrer Bezeichnung von Hersteller zu Hersteller unterscheiden. Herstellerbezeichnungen sind z. B.

- IBM Remote Supervisor Adapter (RSA)
- Hewlett Packard Integrated Lights-Out (HP iLO)
- Dell Remote Access Controller (DRAC)
- Sun System Service Processor (SSP).

Steht für die eingesetzte Hardware eine solche Schnittstelle nicht zur Verfügung, besteht die Möglichkeit durch den Einsatz eines KVM-Switches (Keyboard, Video, Maus) den Zugriff über das Netz auf die Konsole der Hardware zur Verfügung zu stellen. Server werden hierbei über einen KVM-Switch an zentrale Peripheriegeräte angeschlossen, um sich im Falle einer Wartung direkt an der Konsole oder der grafischen Oberfläche anzumelden.

2.3.13 Protokollierung

Sowohl das Betriebssystem als auch die Dienste eines Servers protokollieren lokal wichtige Ereignisse (auch Logging genannt). Diese Ereignisse sind zum einen Statusmeldungen (z. B. über das Starten bzw. Stoppen von Diensten), zum anderen Fehlermeldungen (z. B. über fehlgeschlagene Anmeldeversuche). Um Probleme auf den Servern frühzeitig zu erkennen, sollten die Protokolldaten regelmäßig auf besondere Vorkommnisse hin ausgewertet werden.

Bei einer geringen Anzahl von Systemen kann diese Auswertung noch lokal auf dem Server erfolgen. Bei einer großen Serverlandschaft ist der Aufwand hierfür jedoch zu groß. Daher sollte in großen Umgebungen ein zentraler Protokollierungsserver vorhanden sein, der die Protokollmeldungen aller Systeme sammelt. Die zentrale Speicherung der Protokollmeldungen vereinfacht die Auswertung und die Korrelation von Ereignissen unterschiedlicher Systeme. Bei der Korrelation von Protokollmeldungen ist es besonders wichtig, dass eine Zeitsynchronisation der protokollierenden Systeme erfolgt, damit eine korrekte Auswertung möglich ist.

2.3.14 Speicherschutzmechanismen

Pufferüberläufe (engl. buffer overflow*)* gehören zu den häufigsten Sicherheitsproblemen in aktueller Software. Es sind Softwarefehler, die durch unzureichende Speicherverwaltung entstehen. Zu große Datenmengen werden in einen für die Daten zu kleinen reservierten Speicherbereich (Puffer) geschrieben. Das Programm verhindert nicht, das in solchen Fällen Daten in Speicherbereiche hineingeschrieben werden, die dafür nicht reserviert worden sind. Dadurch können andere Daten und Programme im Speicher beschädigt werden.
Wird dieser Fehler geschickt ausgenützt, können Programme zum Absturz gebracht oder auch beliebiger Programmcode eingeschleust und ausgeführt werden.

Speicherschutzmechanismen (engl. Executable Space Protection, ESP) unterbinden die Ausführung von Programmen aus nicht dafür zugelassenen Bereichen des Arbeitsspeichers. Dazu werden Mechanismen von Prozessoren verwendet (z. B. sogenannte NX-Bit Technologie bei x86-basierten Plattformen; NX steht für No Execute). Diese Technologie sorgt dafür, dass Daten in bestimmten Bereichen des Arbeitsspeichers nicht ausgeführt werden dürfen. Um diese Prozessortechnologie zu nutzen, muss das auf dem Server installierte Betriebssystem dies unterstützen. Die Betriebssystem-Hersteller haben jeweils unterschiedliche Bezeichnungen für diese Technologie. Microsoft nennt dies z. B. Data Execution Prevention (DEP).

Einige Betriebssysteme können diese Speicherschutzmechanismen auch ohne Hardwareunterstützung emulieren. Bei Microsoft heißt dies z. B. Software-DEP. Unter Linux wird dies u. a. durch das Projekt PaX (Page Exec) realisiert.

Es wird empfohlen, einen Prozessor zu verwenden, der Speicherschutzmechanismen in Bezug auf die Hardware unterstützt (s. Abschnitt 4.1.2).

2.3.15 Speicherrandomisierung

Speicherschutzmechanismen (siehe Abschnitt 2.3.14) schützen nicht vollständig gegen Pufferüberläufe. Kennt ein Angreifer den Aufbau des laufenden Programms im Arbeitsspeicher, kann er den Programmfluss durch einen Pufferüberlauf beeinflussen, indem er z. B. vorhandene Daten im Puffer überschreibt. Eine Möglichkeit, dies zu unterbinden ist die Speicherrandomisierung (Address Space Layout Randomization, ASLR). Durch ASLR erfolgt die Zuweisung von Adressbereichen an Programme zufällig. Ein Angreifer kann daher nicht mehr so einfach vorhersehen, wo zur Laufzeit des Programmes Daten abgelegt werden und ist somit auch nicht mehr in der Lage die Speicherbereiche zu manipulieren.

2.3.16 Datensicherung

Neben vielen anderen ist es eine Aufgabe von Server-Systemen, einen zentralen Datenbestand bereitzuhalten und diesen für Anwender, Applikationen oder anderen Servern zur Verfügung zu stellen. Diese Daten können Kundendaten, Personaldaten, Gehaltsdaten, etc. sein. Eine Datensicherung soll einem Verlust der Daten vorbeugen. Durch die Rücksicherung eines Datenbestandes kann im Falle eines Datenverlustes der IT-Betrieb kurzfristig wiederaufgenommen werden.

Die Verfahrensweise der Datensicherung wird von einer großen Zahl von Einflussfaktoren bestimmt. Das eingesetzte Betriebssystem, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Um einem Datenverlust vorzubeugen, ist ein Datensicherungskonzept zu erstellen, das diese Einflussfaktoren berücksichtigt.

2.3.16.1 Arten von Datensicherungen

Es gibt unterschiedliche Möglichkeiten, eine Datensicherung durchzuführen. Nachfolgend werden die in der Praxis am häufigsten vorkommenden Verfahren erläutert.

Vollsicherung

Bei der Vollsicherung (auch Komplettsicherung genannt) werden die zu sichernden Daten komplett auf ein Sicherheitsmedium kopiert. Zur Wiederherstellung der Daten kann auf die letzte Vollsicherung zurückgegriffen werden. Nachteil der Vollsicherung ist, dass diese gerade bei großen Datenbeständen sehr lange dauert, da stets alle Daten komplett auf ein Sicherheitsmedium kopiert werden.

Inkrementelle Sicherung

Das Durchführen einer inkrementellen Sicherung setzt eine Vollsicherung voraus. Bei der inkrementellen Sicherung wird eine Datei nur gesichert, wenn sie sich seit der letzten inkrementellen Sicherung bzw. seit der letzten Vollsicherung verändert hat oder wenn sie neu zu dem Datenbestand hinzugekommen ist. Die Datei wird hierbei komplett auf ein Sicherheitsmedium kopiert. Die Wiederherstellung der Daten erfolgt aus der Vollsicherung und aus allen nachfolgenden inkrementellen Sicherungen (bis hin zum benötigten Wiederherstellungszeitpunkt).

Differenzielle Sicherung

Das Durchführen einer differenziellen Sicherung setzt stets eine vorhandene Vollsicherung voraus. Bei der differenziellen Sicherung werden nur die Daten gesichert, die seit der letzten Vollsicherung hinzugefügt oder geändert wurden. Es wird hierbei stets auf die letzte Vollsicherung aufgesetzt, d. h. zur Wiederherstellung von Dateien werden die Vollsicherung und die letzte differenzielle Sicherung benötigt.

2.4 Verfügbarkeit

Verfügbarkeit bezieht sich auf die Erreichbarkeit und korrekte Funktionsweise eines Server bzw. der darauf betriebenen Dienste. Die Verfügbarkeit wird in Prozent [%] angegeben, woraus sich die maximale Ausfallzeit in Tagen, bezogen auf das gesamte Jahr, berechnen lässt. Zur Steigerung der Verfügbarkeit von Servern und Diensten gibt es unterschiedliche Mechanismen, die nachfolgend vorgestellt werden:

- **Redundanz:** Redundanz bezeichnet das mehrfache Vorhandensein von gleichen oder gleichartigen Komponenten eines Systems. Dies kann sowohl eine Einzel-Komponente sein (z. B. eine Festplatte), als auch der gesamte Server. Fällt eine Komponente im Betrieb aus, kann deren Aufgabe von der redundanten Komponente übernommen werden. Bei modernen Server-Systemen können nahezu alle Bauteile redundant ausgelegt werden. Hierzu gehören u. a Netzteil, Festplatte, Netzwerkkarte und Arbeitsspeicher. Oft sind diese Komponenten Hot-Swap fähig (siehe unten), um einen Austausch im laufenden Betrieb zu gewährleisten.
- **Failover:** Mittels Failover wird sichergestellt, dass bei Nichterreichbarkeit eines Dienstes auf einem System diese Aufgabe von einem anderen (redundanten) System übernommen wird. Dieser Schwenk von einem aktiven System auf ein Ersatzsystem wird als Failover bezeichnet.

- **Loadbalancing:** Kann ein einzelner Server die zu verarbeitenden Anfragen an Dienste nicht mehr alleine performant bearbeiten, dann kann diese Last auf gleichartige Server, die denselben Dienst anbieten, mittels Loadbalancing verteilt werden. Eine Gruppierung einzelner Systeme, die dieselben Dienste anbieten, wird auch als Cluster bezeichnet. Um die einzelnen Server innerhalb des Clusters mit Anfragen zu versorgen, wird davor ein sogenannter Loadbalancer platziert, der die Anfragen auf die im Cluster befindlichen Server verteilt. Loadbalancing erhöht die Verfügbarkeit, wenn mehr Server im Cluster zusammengeführt werden, als für den einwandfreien Betrieb notwendig sind.

Eine weitere Steigerung der Verfügbarkeit lässt sich durch den Einsatz sogenannter Hot-Swap-fähigen Komponenten erreichen. Hot-Swap bezeichnet die Möglichkeit, System-Komponenten im laufenden Betrieb des Server-Systems zu wechseln ohne den Server herunterzufahren. Das auf dem Server installierte Betriebssystem bekommt davon nichts mit und kann ungehindert weiterlaufen und Dienste zur Verfügung stellen. Voraussetzung hierfür ist, dass die Hot-Swap-fähigen Komponenten (z. B. Netzteil, Festplatte oder auch Arbeitsspeicher) redundant auf Hardware-Ebene bereitgestellt werden.

2.4.1 Berechnung der Verfügbarkeit

Die Verfügbarkeit kann sowohl für jede Teil-Komponente als auch für das Gesamtsystem einer IT-Infrastruktur definiert werden und lässt sich anhand des Zeitraums, in der das Gesamtsystem bzw. die Teil-Komponente zur Verfügung steht, definieren.

$$Verfügbarkeit[\%] = \frac{Gesamtzeit - Ausfallzeit}{Gesamtzeit} * 100$$

Die Verfügbarkeit gibt also das Verhältnis von Betriebszeit (Gesamtzeit – Ausfallzeit) zur Gesamtzeit an. Dieser Wert wird mit dem Faktor 100 multipliziert, um die Verfügbarkeit in Prozent anzugeben.

2.4.2 Verfügbarkeitsklassen

Von der Harvard Research Group (HRG) wurden sechs Verfügbarkeitsklassen definiert, welche die minimale Verfügbarkeit und die Ausfallzeit festlegen. Das BSI orientiert sich in seinem Hochverfügbarkeitskompendium (siehe [BSI_HV_KOMP]) an diese definierten Klassen und berücksichtigt dabei gleichzeitig die Anforderungen aus den BSI-Standards 100-[1-3] (siehe [BSI_STANDARDS]). Tabelle 1 zeigt die Verfügbarkeitsklassen aus dem Hochverfügbarkeitskompendium.

Verfügbarkeits-klasse (VK)	*Bezeichnung*	*Minimale Verfügbarkeit*	*Ausfallzeit pro Monat*	*Ausfallzeit pro Jahr*
VK 0	Standard-IT-System ohne Anforderungen an die Verfügbarkeit	~95%	1 Tag	Mehrere Tage
VK 1	Standard-Sicherheit nach IT-Grundschutz bei normalem Verfügbarkeitsbedarf	99,0%	< 8 h	< 88 h
VK 2	Standard-Sicherheit nach IT-Grundschutz bei erhöhtem Verfügbarkeitsbedarf	99,9%	< 44 min	< 9 h
VK 3	Hochverfügbar IT-Grundschutz für spezifische IT-Ressourcen; 100-3	99,99%	< 5 min	< 53 min
VK 4	Höchstverfügbar	99,999%	< 26 s	< 6 min
VK 5	Disaster-Tolerant	max. Verfügbarkeit	0	0

Tabelle 1: Verfügbarkeitsklassen und ihre Ausfallzeiten

Für den Betrieb von IT-Systemen können diese Verfügbarkeitsklassen als Vorgabe für die Mindestverfügbarkeit festgelegt werden, die die eingesetzten Komponenten zu erfüllen haben. Um die Gesamtverfügbarkeit zu ermitteln, muss jedoch immer das Gesamtsystem aller verwendeten Komponenten betrachtet werden. Die nächsten Abschnitte 2.4.3 und 2.4.4 beschreiben die Auswirkung von unterschiedlichen Architekturmodellen auf die Verfügbarkeit.

2.4.3 Serienschaltung von Komponenten

In einer Serienschaltung werden Einzel-Komponenten in Reihe hintereinander geschaltet. Aus diesem Grund ergibt sich eine Abhängigkeit der Einzel-Komponenten. Fällt eine der Komponenten aus, ist die Gesamtverfügbarkeit des Systems nicht mehr gegeben (siehe Abbildung 2.5).

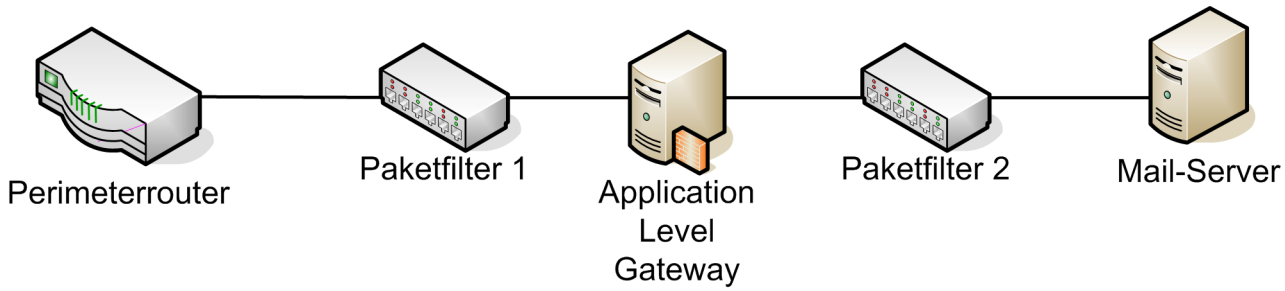


Abbildung 2.5: Serienschaltung von Komponenten

Die Verfügbarkeit des Gesamtsystems errechnet sich aus dem Produkt der Einzelverfügbarkeiten. Daraus ergibt sich, dass die Gesamtverfügbarkeit stets kleiner ist als die kleinste Einzelverfügbarkeit einer Komponente.

$$Gesamtverfügbarkeit[V_{gesamt}] = \prod_{i=1}^{n} Einzelverfügbarkeit_i$$

Beispiel

Gegeben seien die folgenden Einzelverfügbarkeiten (bezogen auf Abbildung 2.5):

- Perimeterrouter: 0,999
- Paketfilter: 0,995
- Application Level Gateway: 0,998
- Mail-Server 0,991

Die Gesamtverfügbarkeit ist demnach:

$$V_{Gesamt} = 0{,}999 * 0{,}995 * 0{,}998 * 0{,}995 * 0{,}991 = 0{,}978$$

In Prozent ausgedrückt, hat das Gesamtsystem eine Verfügbarkeit von 97,8%. Bezogen auf die Einzel-Komponenten genügen diese dem normalen Schutzbedarf (VK1). Die Gesamtverfügbarkeit des Systems reicht dafür jedoch nicht aus, da in der VK1 eine Verfügbarkeit von 99% gefordert wird.

Falls die Verfügbarkeit in einem solchen Fall nicht durch technische Maßnahmen gesteigert werden kann, muss einem Ausfall durch ergänzende organisatorische Maßnahmen vorgebeugt werden. In jedem Fall muss ein Notfallvorsorgekonzept (siehe Abschnitt 3.3) erstellt werden, in dem Maßnahmen für einen Ausfall (Monitoring der Komponenten, Backup, Ersatzgeräte, etc.) beschrieben werden.

2.4.4 Parallelschaltung von Komponenten

In einer Parallelschaltung sind Komponenten redundant angeordnet. Das Gesamtsystem ist verfügbar, solange mindestens eine der redundanten Komponenten verfügbar ist. Die redundanten Komponenten arbeiten hierbei unabhängig voneinander (siehe Abbildung 2.6).

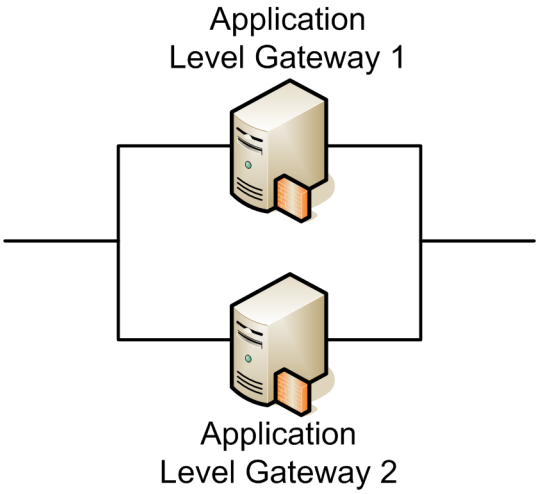


Abbildung 2.6: Parallelschaltung von Komponenten

Die Gesamtausfallzeit in einer Parallelschaltung ergibt sich aus dem Produkt der Einzelausfallzeiten. Hieraus ergibt sich:

$$Einzelausfallzeit = 1 - Einzelverfügbarkeit$$

$$Gesamtausfallzeit = \prod_{i=1}^{n} Einzelausfallzeit_i$$

Die Gesamtverfügbarkeit einer Parallelschaltung kann demnach wie folgt berechnet werden:

$$Gesamtverfügbarkeit\,[V_{gesamt}] = 1 - \prod_{i=1}^{n} (1 - Einzelverfügbarkeit_i)$$

Beispiel

Gegeben seien die folgenden Einzelverfügbarkeiten (bezogen auf Abbildung 2.6):

- Application Level Gateway: 0,998

Die Gesamtverfügbarkeit ist demnach:

$$V_{gesamt} = 1 - ((1 - 0{,}998) * (1 - 0{,}998)) = 0{,}999996$$

In Prozent ausgedrückt, hat das Gesamtsystem eine Verfügbarkeit von 99,9996%, dies entspricht Verfügbarkeitsklasse 4.

2.5 Massenspeicher

Reicht die lokale Speicherkapazität von Server-Systemen nicht aus, müssen externe Speichermedien eingebunden werden. Ein weiterer Grund zur Anbindung von externem Massenspeicher ist, dass eine gemeinsame Datenhaltung (z. B. von mehreren Virtualisierungsservern, die in einem Cluster betrieben werden) benötigt wird, um z. B. eine Inkonsistenz von Daten zu verhindern. Externe Massenspeicher können unterschiedlich realisiert werden. Nachfolgend werden die wichtigsten Speichertechnologien erläutert.

2.5.1 Local Storage und Direct Attached Storage (DAS)

Die einfachste Möglichkeit Massenspeicher an Server-Systeme anzubinden, ist über die lokalen Schnittstellen, die auf dem Mainboard zur Verfügung gestellt werden. Dies sind im Serverbereich meist SAS (Serial Attached SCSI) - oder SATA (Serial Advanced Technology Attachement) - Schnittstellen. Hierfür wird keine externe Hardware benötigt und die maximale Schreib- und Lesegeschwindigkeit des lokalen Festplatten- bzw. RAID-Controllers kann genutzt werden. Die Anbindung des lokalen Massenspeichers wird als Local Storage bezeichnet.

Falls ein Server lokal nicht über genügend Festplattenkapazität verfügt, kann diese einfach durch externe Festplatten erweitert werden, welche Direct Attached Storage (DAS) genannt werden. Diese werden in einem externen Gehäuse über die physischen Schnittstellen SATA, SAS oder Fibre Channel angebunden. Auf DAS-Systeme kann (wie bei lokalen Festplatten) immer nur ein Server zugreifen.

2.5.2 Network Attached Storage (NAS)

Das Konzept von Network Attached Storage (NAS) basiert auf einer zentralen Datenhaltung. Das NAS-System ist wie ein Server mit Festplatten ausgestattet und stellt diesen Speicher über das Netz zur Verfügung. Die Festplatten werden mit einem „normalen“ Dateisystem, wie z. B. NTFS, ext3, etc., formatiert. Die Server, die den Speicher nutzen wollen, greifen über ein Netzdateisystem auf die zur Verfügung gestellten Freigaben zu, als ob es sich dabei um ein lokales Dateisystem handelt. Die verbreitetsten Netzdateisysteme sind SMB (Server Message Block), das darauf aufbauende CIFS (Common Internet File System) und NFS (Network File System).

2.5.3 Storage Area Network (SAN)

Ein SAN bezeichnet ist ein Speichernetz, welches eine Vielzahl von Festplatten enthält und diese als Datenspeicher für andere Server zur Verfügung stellt. Diese Zusammenfassung von Festplatten wird auch als Festplattensubsystem bezeichnet. Diese speziellen Speichernetze sind für eine hochperformante Übertragung großer Datenmengen konzipiert worden. Die Übertragungstechnologien, die dort verwendet werden, sind meist Fibre Channel (siehe Abschnitt 2.5.4.4) und zunehmend iSCSI (Internet Small Computer System Interface, siehe Abschnitt 2.5.4.3).

Bevor der SAN-Speicher von einem Server genutzt werden kann, muss dieser zuerst mit einem Dateisystem formatiert werden (z. B. mit NTFS, ext3, ZFS, UFS, etc.). Erst nach dem Formatieren kann der Speicher eingebunden und darauf wie auf eine lokale Festplatte zugegriffen werden. Ein SAN ist damit eine Erweiterung von Direct Attached Storage (DAS). Während bei DAS nur ein einzelner Server auf den Speicher zugreifen kann, ermöglicht ein SAN die Anbindung mehrerer

Server an ein oder mehreren Speichersystemen. Der Zugriff auf das SAN erfolgt entweder über normale Netzwerkkarten oder Host Bus Adapter (HBA, siehe Abschnitt 2.5.3.1).

2.5.3.1 Host Bus Adapter

Host Bus Adapter sind für die Anbindung eines Rechnersystems an ein SAN zuständig und ersetzen den lokalen Festplatten-Controller, der normalerweise für die Anbindung einer Festplatte zuständig ist. Je nach verwendeter Speichertechnologie kann ein HBA eine normale Netzwerkkarte sein (z. B. bei iSCSI) oder eine dedizierte Hardwarekarte (z. B. bei Fibre Channel). Die physische Anbindung an das SAN erfolgt entweder über Kupfer- oder Glasfaserkabel.

Es gibt HBAs, die bereits Teile des verwendeten Speicherprotokolls (iSCSI oder Fibre Channel) in Hardware implementiert haben, um einen höheren Datendurchsatz zu erzielen. Hierbei werden Teile des Protokolls (z. B. Berechnung von Prüfsummen) nicht von der CPU des Servers berechnet, sondern auf dem HBA.

Gleiches gilt für Massenspeicherprotokolle, die auf TCP/IP aufbauen (z. B. iSCSI – siehe Abschnitt 2.5.4.3 oder FcOE – siehe Abschnitt 2.5.4.5). Hier gibt es ebenfalls spezielle HBAs, die Teile des TCP/IP-Protokolls implementiert haben, um z. B. die Prüfsummen der TCP- und IP-Schicht auf dem HBA zu berechnen. Hierbei spricht man von sogenannten TCP Offload Engines (TOE). Der Einsatz solcher Karten reduziert die CPU-Belastung des Hosts. Durch die Auslagerung von rechenintensiven Operationen von der Host CPU auf den HBA kann der Datendurchsatz gesteigert werden.

Der Begriff HBA wird im Folgenden für Hardware genutzt, die zur Anbindung an das SAN dient. Dies können sowohl normale Netzwerkkarten sein als auch HBAs, die bereits Teile des Speicherprotokolls implementiert haben.

2.5.3.2 Ausfallsicherheit im SAN

Ausfallsicherheit bei SAN-Speichernetzen erreicht man durch Multipathing. Hierunter versteht man die Möglichkeit, über mehrere Host Bus Adapter eines Servers dasselbe Festplattensubsystem zu erreichen. Die HBAs sollten über unterschiedliche Netz-Komponenten angebunden werden, um beim Ausfall einer einzelnen Komponente einen Totalausfall vorzubeugen. Fällt einer dieser Pfade aus, kann auf das Festplattensubsystem noch über einen anderen Pfad zugegriffen werden. Die Implementierung von Multipathing kann sowohl im Treiber des HBAs oder auch auf Betriebssystemebene durch spezielle Software erfolgen. Dies wird im Betriebssystem oft im Zusammenhang mit dem Begriff Multipath I/O (MPIO) verwendet.

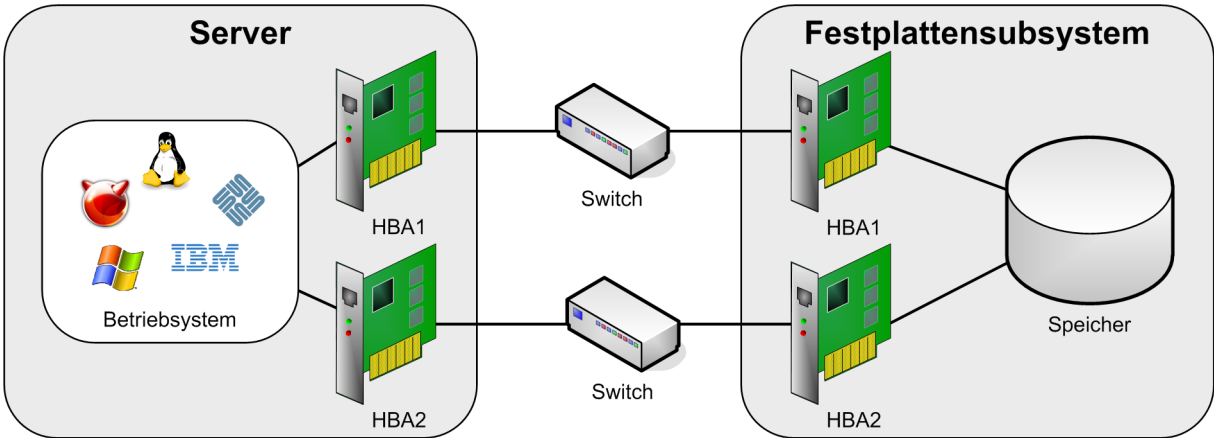


Abbildung 2.7: Multipathing

Beim Multipathing unterscheidet man noch zwischen den beiden Betriebsmodi Aktiv/Passiv und Aktiv/Aktiv. Bei Aktiv/Passiv gibt es einen primären HBA, über den die Datenübertragung stattfindet. Beim Ausfall dieses HBAs übernimmt ein anderer dessen Aufgabe. Beim Betriebsmodi Aktiv/Aktiv erfolgt der Datentransfer auf allen zur Verfügung stehenden HBAs. Im Fehlerfall übernehmen die noch betriebsfähigen HBAs den Datentransfer. Im Falle einer Aktiv/Aktiv-Konfiguration können die redundanten Pfade auch zur Lastverteilung genutzt werden.

2.5.3.3 Zugriff auf den Massenspeicher

Im Folgenden werden einige Begriffe und Namen erläutert, die im Rahmen der Konfiguration von Massenspeicher verwendet werden.

WWN

Die interne Verwaltung und Zuordnung der Geräte in einem Fibre Channel SAN erfolgt über World Wide Names (WWN). Der WWN ist eine 64 Bit lange Adresse für Fibre Channel-Komponenten, die weltweit einmalig vergeben wird. Sie sind vergleichbar mit den MAC-Adressen von Ethernet-Netzadaptern.

- **Beispiel:** 210000E08B02DE2F

Der WWN wird noch einmal unterteilt zwischen dem World Wide Node Name (WWNN) und dem World Wide Port Name (WWPN). Eine Fibre-Channel-Komponente kann über mehrere Ports verfügen, die jeweils über einen eindeutigen WWPN verfügen. Der WWN ist jedoch für eine Fibre-Channel-Komponente nur einmal vorhanden.

IQN

Das Äquivalent der WWN in einem Fibre-Channel SAN ist bei einem iSCSI SAN der IQN (iSCSI Qualified Name). Der Aufbau dieses Bezeichners beginnt mit der Bezeichnung „iqn“ gefolgt von Informationen wie Datum, Domainnamen sowie ein optionaler Teil, der frei vergeben werden kann (z. B. mit dem Servernamen).

- **Beispiel:** iqn.2000-04.com.qlogic:qle4060c.yk10ny04tbjn.1

LUN

Mit Hilfe der Logical Unit Number (LUN) wird eine Zugriffssteuerung in einem SAN realisiert, über die eine feste Verknüpfung zwischen Server- und logischer Speichereinheit gebildet wird. Eine LUN bildet die kleinste adressierbare Einheit in einem Speichernetz. Der physische Speicher des Festplattensubsystems wird dabei in mehrere logische Festplatten unterteilt, auf die mittels der LUN von einem Client aus zugegriffen werden kann.

LUN Masking

Mittels LUN Masking ist es möglich, die Sichtweise von LUNs in einem SAN auf bestimmte Hosts einzuschränken. Dadurch kann man in iSCSI oder Fibre-Channel Netzen konfigurieren, welcher Rechner welches Massenspeichersystem sehen darf. LUN Masking wird auf dem HBA oder auf dem Controller des Massenspeichers konfiguriert.

SAN Zoning

Mit SAN Zoning wird eine logische Zugriffskontrolle innerhalb eines SANs ermöglicht (vergleichbar mit einem VLAN), welches bei Fibre Channel Switchen verwendet wird. Eine Möglichkeit SAN Zoning zu implementieren, ist auf der Port-Ebene von Fibre Channel Switchen (sog. Port Zoning). Hierbei werden Gruppen von Ports konfiguriert, die miteinander kommunizieren dürfen, um den Zugriff von Servern auf den Massenspeicher einzuschränken. Eine weitere Möglichkeit von SAN Zoning ist das WWN Zoning. Beim WWN Zoning wird konfiguriert, welche WWNs von Server und Massenspeicher miteinander kommunizieren dürfen.

2.5.4 Massenspeicherprotokolle

Der Zugriff auf die vorgestellten Speichertechnologien über das Netz wird durch Massenspeicherprotokolle ermöglicht. Unter Massenspeicherprotokolle fallen in diesem Zusammenhang auch Netzdateisysteme, die für den Zugriff auf den Massenspeicher verwendet werden. Nachfolgend sollen die verbreitetsten Massenspeicherprotokolle erläutert werden.

2.5.4.1 SMB / CIFS

SMB und CIFS werden meistens von Windows Systemen verwendet, wobei CIFS eine Weiterentwicklung von SMB ist und heutzutage am verbreitetsten ist. Unter Windows (Desktop und Serverprodukte) ist dieses Protokoll bereits integraler Bestandteil des Betriebssystems. Die meisten Linux- / Unix-Systeme haben ebenfalls Schnittstellen integriert, um SMB / CIFS einzubinden.

Der Zugriff auf SMB / CIFS kann optional mit einer Authentisierung erfolgen. Das Protokoll bietet die folgenden Authentisierungsverfahren an:

- LAN Manager (LM)
- NT LAN Manager (NTLM)
- NT LAN Manager Version 2 (NTLMv2) und
- Kerberos.

Aufgrund von Sicherheitslücken in den älteren Versionen werden fast ausschließlich NTLMv2 und Kerberos eingesetzt. SMB / CIFS bietet jedoch bis heute keine Möglichkeit der Verschlüsselung.

Da das Protokoll auf TCP/IP aufbaut, können für Verschlüsselung andere Mechanismen, wie z. B. SSL oder IPSec, verwendet werden.

2.5.4.2 NFS

NFS ist ein von Sun Microsystems entwickeltes Protokoll, das den Zugriff auf Dateien in einem Netz ermöglicht. Dieses Dateisystem wird hauptsächlich in Linux- / Unix-Umgebungen verwendet. Dieses Netzdateisystem gibt es inzwischen in vier verschiedenen Versionen. NFSv1 und NFSv2 unterstützen dabei ausschließlich UDP; NFSv3 unterstützt UDP und TCP; NFSv4 unterstützt nur noch TCP.

Die einzige Möglichkeit der Authentisierung bei NFS war bis einschließlich Version 3 nur anhand der IP-Adresse des anfragenden Clients. In NFSv4 wurden unterschiedliche Authentisierungsmechanismen aufgenommen, u. a. Kerberos. Verschlüsselung war ebenfalls nicht in früheren Protokollversionen vorgesehen. Erst durch den Einsatz von TCP in NFSv3 konnte durch andere Mechanismen (SSH-Tunnel, IPSec, etc.) eine Verschlüsselung der Verbindung realisiert werden. In der Protokollversion 4 wurde Verschlüsselung ebenfalls berücksichtigt.

2.5.4.3 iSCSI

iSCSI ist eine Übertragungstechnologie, die zum Einsatz in einem SAN verwendet werden kann. Es verpackt SCSI-Kommandos zum Lesen oder Schreiben bestimmter Blöcke in TCP/IP-Pakete und übermittelt sie via Ethernet an Speichergeräte. Der Zugriff über iSCSI ist transparent und erscheint auf Serverseite wie ein Zugriff auf eine lokale Festplatte.

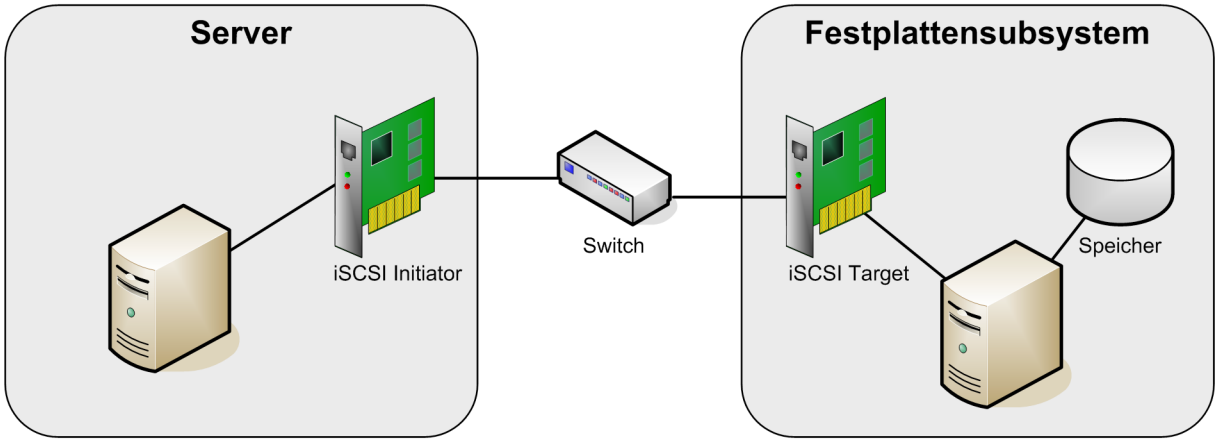


Abbildung 2.8: Komponenten einer iSCSI-Verbindung

Eine iSCSI-Verbindung wird über die beiden Komponenten iSCSI Initiator und iSCSI Target errichtet. Der iSCSI Initiator ist der Server, der den Speicher nutzen will. Das iSCSI Target ist das Festplattensubsystem, das den Speicher zur Verfügung stellt (siehe Abbildung 2.8). Die Verbindung dieser beiden Komponenten erfolgt über die Ethernet-Infrastruktur (Netzwerkkabel, Router bzw. Switch). Bei iSCSI können bereits vorhandene Netz-Komponenten (Router, Switches, Netzwerkkarten) zum Aufbau des Speichernetzes genutzt werden, sodass nicht zwingend eine neue Infrastruktur angeschafft werden muss. Da iSCSI auf der Ethernet-Technologie basiert, ist die Übertragungsgeschwindigkeit hierüber festgelegt. Üblich ist derzeit eine Datenübertragungsrate von 1, 2, 4, 8 oder 10 Gbit/s.

2.5.4.4 Fibre Channel

Fibre Channel spezifiziert sowohl eine Übertragungstechnologie als auch ein Protokoll, das große Datenmengen übertragen kann. Als Übertragungsmedium können Kupferkabel oder Lichtwellenleiter (LWL) verwendet werden. Bei beiden Übertragungsmedien wird das Fibre Channel Protokoll verwendet. Bei der Entwicklung des Protokolls stand die Effizienz zur Übertragung großer Datenmengen im Vordergrund, daher ist Fibre Channel nach einem eigenen Schichtenmodell aufgebaut und orientiert sich nicht am OSI-Referenzmodell. Der Aufbau eines Speichernetzwerkes mittels Fibre Channel erfordert die Anschaffung dedizierter Netz-Komponenten, da diese Technologie nicht mit der in Firmen meist vorhandenen Ethernet-Technologie kompatibel ist. Die Datenübertragungsraten liegen derzeit bei 1, 2, 4, 8 und 10 Gbit/s.

2.5.4.5 Fibre Channel over Ethernet (FCoE)

Da die Anschaffung einer komplett neuen Infrastruktur für die Verwendung von Fibre Channel sehr kostenintensiv ist, wurde das Protokoll weiterentwickelt. In 2009 ist das Protokoll Fibre Channel over Ethernet (FCoE) verabschiedet worden, das die Verwendung des Fibre Channel Protokolls in bestehenden Ethernet Infrastrukturen ermöglicht. Hierbei werden Fibre Channel Pakete direkt in Ethernet Pakete verpackt.

Um FCoE nutzen zu können, wurden einige Erweiterungen an Ethernet vorgenommen. Diese Erweiterungen können Serverseitig bereits im Protokolltreiber des Betriebssystems implementiert werden, was jedoch zu einer erhöhten CPU-Belastung führt. Alternativ gibt es besondere Netzwerkkarten, welche diese Prokollerweiterungen bereits in Hardware implementiert haben, sogenannte Converged Network Adapter (CNA). Um FCoE auf bestehende Ethernet-Netze umsetzen zu können, müssen die dort verwendeten Switche ebenfalls diese Erweiterungen (Convergence Enhanced Ethernet, CEE) unterstützen. Die Datenübertragungsrate wird von der darunterliegenden Ethernet-Technologie bestimmt. Üblich ist derzeit eine Datenübertragungsrate von 1, 2, 4, 8 oder 10 Gbit/s.

3 Sichere Grundarchitektur für normalen Schutzbedarf

Im vorigen Abschnitt wurden die Grundlagen beschrieben, die für das Verständnis zur Absicherung von Servern benötigt werden. Dieser Abschnitt stellt die Grundarchitektur eines sicheren Servers vor und beschreibt die Hard- und Software-Komponenten, die ein sicherer Server enthalten muss, um dem normalen Schutzbedarf hinsichtlich der Schutzwerte Vertraulichkeit, Verfügbarkeit und Integrität zu genügen.

3.1 Überblick

Bei der Grundarchitektur geht es um die grundlegende Absicherung eines Servers. In dieser Studie liegt der Fokus auf den technischen Aspekten. Sie berücksichtigt organisatorische und infrastrukturelle Aspekte nur am Rande. Die letzten beiden Punkte werden durch Maßnahmen der IT-Grundschutz-Kataloge abgedeckt (siehe [BSI_GSK]). Es wird z. B. davon ausgegangen, dass der betriebene Server in einer physisch gesicherten Umgebung steht, die über eine Zutrittskontrolle verfügt. Zu den technischen Aspekten gehören die sichere Konfiguration des Betriebssystems und die Installation von spezieller Software, die der Absicherung des Servers dient. Die Empfehlungen zur Absicherung bewegen sich auf Betriebssystem-Ebene.

Der hier beschriebene Server dient als Grundlage für unterschiedliche Einsatzzwecke. Nach Installation der entsprechenden Anwendungen oder Dienste, kann er sowohl im Intranet als Verzeichnisdienst oder Mail-Server als auch in der Zone „Sicherheits-Gateway“ als Web-Server oder externer DNS-Server eingesetzt werden (siehe Abbildung 3.1).

Die Absicherung der Anwendungen oder Dienste, die auf dem Server laufen (z. B. Web-Server, DBMS, File-Server, etc.), wird in dieser Studie nicht betrachtet. Diese werden detailliert von anderen Studien behandelt (siehe hierzu z. B. [ISi-Mail-Server] oder [ISi-Web-Server]).

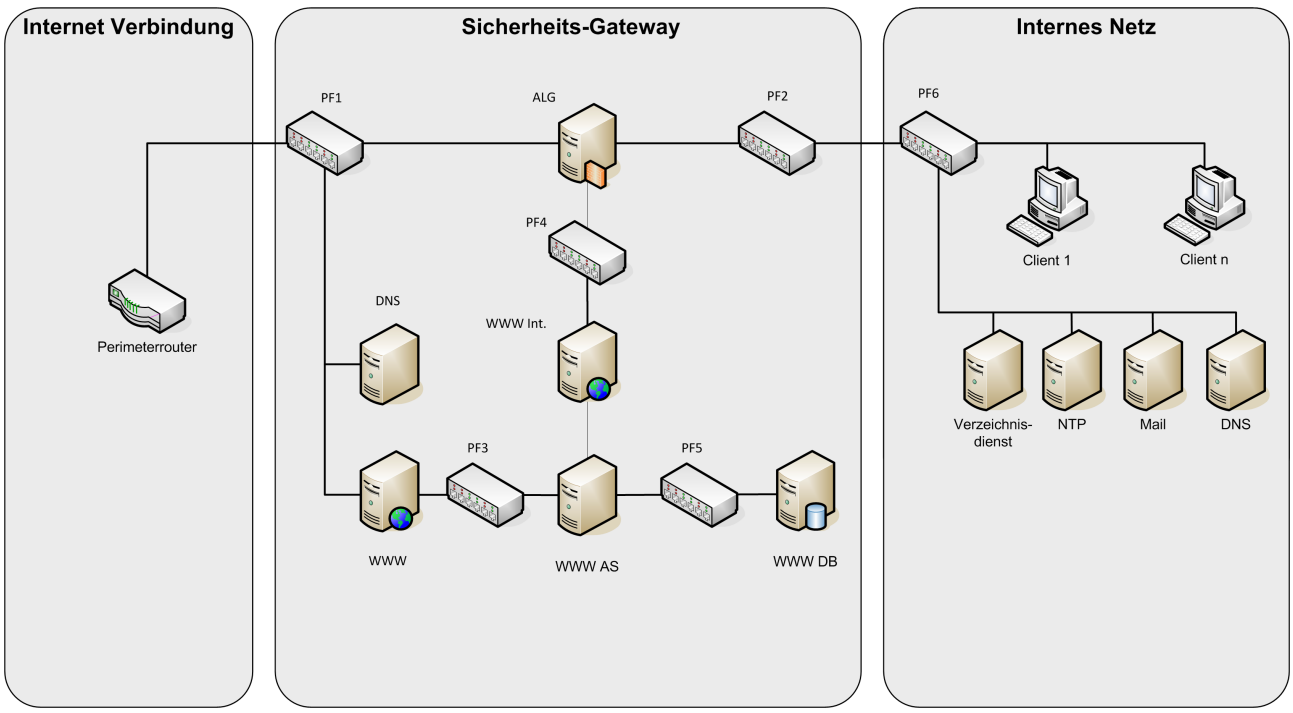


Abbildung 3.1: Grundarchitektur für den normalen Schutzbedarf

Für diese Studie wird davon ausgegangen, dass in der Institution bereits ein abgesichertes Netz vorhanden ist, z. B. nach ISi-LANA. Die Abbildung 3.1 zeigt z. B. die Grundarchitektur aus [ISi-LANA] in der die Absicherung der Server durch Paketfilter und Application Level Gateway (ALG) erfolgt. Aufgrund der vorgelagerten Paketfilter wird die Installation einer lokalen Firewall auf dem Server nicht zwingend gefordert, kann jedoch als Erweiterung installiert werden.

Die Grundarchitektur deckt hinsichtlich der Verfügbarkeit der Server-Systeme den normalen Schutzbedarf ab. Eine redundante Auslegung von einzelnen Komponenten oder kompletten Server-Systemen wird innerhalb der Grundarchitektur nicht gefordert, es wird jedoch auf die Erstellung eines Notfallvorsorgekonzeptes eingegangen, um einem etwaigen Ausfall vorzubeugen. Eine Ausnahme bzgl. Redundanz bilden virtualisierte Komponenten, die in Abschnitt 3.5 behandelt werden.

In Abbildung 3.1 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. Diese Sicherheits-Komponenten werden in den nächsten Abschnitten vorgestellt.

Sicherheits-Komponenten

Abbildung 3.2 greift die Architektur eines Servers (siehe auch Abbildung 2.1) auf und ergänzt diese um geforderte und optionale Sicherheits-Komponenten.

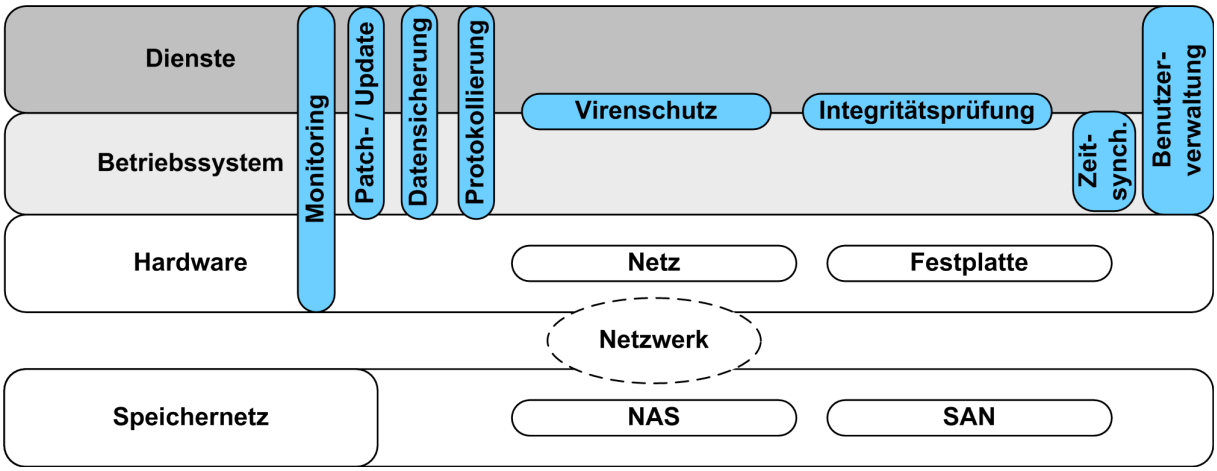


Abbildung 3.2: Schematischer Aufbau der Grundarchitektur eines Servers

Die Basis des Servers ist die Hardware, auf der das Betriebssystem installiert wird. Die Hardware stellt dem Betriebssystem die Schnittstellen zu Netz und Festplatte zur Verfügung. Das Betriebssystem bietet eine Laufzeitumgebung, in die weitere Software installiert wird. Weitere Software sind zum einen Sicherheits-Komponenten (Integritätssicherung, Monitoring, etc.), zum anderen die Dienste, die ein Server anbieten soll (Web-Server, Datenbank-Managementsystem etc.). Der Fokus dieser Studie liegt auf den Sicherheits-Komponenten, diese werden im weiteren Verlauf des Abschnitts beschrieben.

Die Aufgabe der **Integritätsprüfung** innerhalb der Grundarchitektur ist es, die Betriebssystem-relevanten Dateien zu überwachen. Die Integritätsprüfung erkennt inhaltliche Änderungen der Konfigurationsdateien und auch Änderungen an den Zugriffsberechtigungen dieser Dateien.

Es ist vorgesehen, dass sämtliche Daten auf dem Server-System von dem **Virenschutzprogramm** auf möglichen Virenbefall hin untersucht werden.

Details hierzu sind unter Abschnitt 3.2.11 beschrieben. **Protokolliert** wird sowohl der Fund von Schadprogrammen (vom Virenschutzprogramm) als auch Änderungen an Konfigurationsdateien oder Zugriffsrechten (von der Integritätsprüfung).

Die Verfügbarkeit von Hardware, Betriebssystem und den darauf betriebenen Diensten wird über das Monitoring überwacht. Fällt eine Hardware-Komponente oder ein Dienst aus, erfolgt eine Alarmierung an das zentrale Monitoring. Diese alarmiert dann die Administratoren, damit diese Gegenmaßnahmen einleiten, um die Verfügbarkeit des Server-Systems wiederherzustellen.

Um eine zentrale Pflege von Benutzern und Berechtigungen zu ermöglichen, ist die Benutzerverwaltung des Betriebssystems an eine zentrale **Benutzerverwaltung** angebunden. Will ein Administrator sich am Betriebssystem anmelden, erfolgt die Authentisierung über die Benutzerverwaltung, wobei erfolgreiche und fehlgeschlagene Anmeldungen protokolliert werden. In der Benutzerverwaltung sind auch Informationen für die Zugriffskontrolle hinterlegt (z. B. Zugriffsrechte und Gruppenzugehörigkeit des Benutzers). Bevor ein Benutzer auf Daten oder Ressourcen zugreifen kann, überprüft die Zugriffskontrolle die Berechtigung eines Benutzers anhand der Zugriffsrechte. Werden die Zugriffsberechtigungen nicht erfüllt, wird der Zugriff auf die Daten verweigert.

Das Betriebssystem und ggf. auch die zu verarbeitenden Daten werden auf der lokalen Festplatte gespeichert. Sollen größere Datenmengen gespeichert oder verarbeitet werden, kann ein externes Speichernetz verwendet werden. Auf diesem **Speichernetz** können Server- oder Client-Systeme gemeinsam zugreifen, um z. B. Daten auszutauschen oder zu verarbeiten.

Um die Ausfallsicherheit und/oder die Performance des Gesamtsystems zu erhöhen, können RAID-Systeme (mit Ausnahme von RAID-0) eingesetzt werden.

Um eine korrekte Funktionsweise von Diensten zu gewährleisten, ist es häufig erforderlich, dass diese über eine genaue Uhrzeit verfügen. Dies erfolgt in der Grundarchitektur über eine zentrale **Zeitsynchronisation** (z. B. über NTP). Eine korrekte Uhrzeit ist ebenfalls für die Protokollierung relevant, um z. B. Fehlermeldungen zwischen mehreren Systemen nachzuvollziehen.

Die **Datensicherung** eines Servers sorgt dafür, dass bei einem Datenverlust eine Wiederherstellung der Daten aus dem Backup möglich ist. So kann der IT-Betrieb schnell wieder aufgenommen werden.

Um Sicherheitslücken oder Fehler in Betriebssystem und Diensten vorzubeugen, ist der Server an ein **Patch- und Änderungsmanagement** angebunden, das die Installation von Sicherheitsupdates und fehlerbereinigter Software durchführt. Hierdurch werden potenzielle Schwachstellen reduziert und die Systemstabilität (und dadurch die Verfügbarkeit) des Servers gesteigert.

Die hier beschriebenen Zusammenhänge zwischen den einzelnen Grund-Komponenten eines Server-Systems geben nur einen Überblick über den Aufbau einer sicheren Grundarchitektur eines Servers. Diese Komponenten werden in den nächsten Abschnitten weiter erläutert.

3.2 Komponenten der Grundarchitektur

In diesem Abschnitt werden die bereits kurz vorgestellten Komponenten der Grundarchitektur im Detail beschrieben.

3.2.1 Hardware

Im Gegensatz zu Arbeitsplatz-PCs besteht Server-Hardware aus leistungsstärkeren und hochwertigeren Komponenten, die für den Dauereinsatz (24x7) ausgelegt sind. Dies führt zu einer erhöhten Wärmeentwicklung, daher sind die Gehäuse mit mehreren Lüftern versehen, die für die Abfuhr der Wärme sorgen und eine Überhitzung verhindern. Weiterhin ist für eine ausreichende Klimatisierung der Räumlichkeiten zu sorgen, in denen die Server betrieben werden (siehe hierzu auch [BSI_GSK_KLIMA]).

In der Grundarchitektur für den normalen Schutzbedarf wird kein redundanter Aufbau von Servern und dessen Hardware gefordert. Durch die Erstellung eines Notfallvorsorgekonzeptes werden jedoch organisatorische und technische Maßnahmen zur Sicherung der Verfügbarkeit ergriffen, um bei einem Ausfall von Server, Diensten oder Daten eine kurzfristige Wiederaufnahme des Betriebs zu gewährleisten (siehe auch Abschnitt 3.3).

Externe Schnittstellen und Peripheriegeräte

Die externen Schnittstellen eines Servers bieten u. a. die Möglichkeit, Geräte zur Administration des Betriebssystems anzuschließen (Peripheriegeräte wie Monitor, Tastatur, Maus). Des Weiteren hat ein Server die üblichen Schnittstellen, die auch ein Arbeitsplatz-PC haben kann:

- USB-Anschlüsse
- CD/DVD-ROM oder auch CD/DVD-Brenner
- Netzanschluss zur Stromversorgung
- eine oder mehrere Netzwerkkarten.

Nicht benötigte physische Schnittstellen brauchen nicht deaktiviert werden, da Server-Systeme üblicherweise in Rechenzentren oder Rechnerräumen mit Zutrittskontrolle stehen, zu denen nur autorisiertes Personal Zutritt hat.

3.2.2 Betriebssystem

Das Betriebssystem muss als Minimalsystem installiert und konfiguriert werden, um eine möglichst geringe Angriffsfläche für potenzielle Bedrohungen zur Verfügung zu stellen. Bei einem Minimalsystem werden nur benötigte Komponenten und Dienste installiert. Nicht benötigte Komponenten und Dienste sind zu deaktivieren oder zu deinstallieren. Nach der Installation dürfen nur berechtigte Personen Zugriff auf den Server haben. Dies sind z. B. Administratoren, Applikationsverantwortliche, Datenbankadministratoren etc. Endbenutzer haben in der Regel kein Benutzerkonto auf diesen Systemen. Nach der Installation des Betriebssystems sind die in der Grundarchitektur beschriebenen Sicherheits-Komponenten zu installieren und konfigurieren. Dies wird in Abschnitt 4 beschrieben.

3.2.3 Sicherheits-Komponenten

Um den Server nach der Minimalinstallation gemäß der vorgestellten Grundarchitektur aus Abbildung 3.2 abzusichern, bedarf es der Installation zusätzlicher Programme, welche die erforderlichen Sicherheits-Komponenten zur Verfügung stellen. Abbildung 3.3 stellt die, innerhalb der Grundarchitektur, benötigten Sicherheits-Komponenten aus der Sicht des Betriebssystems dar und erweitert diese um weitere Dienste, die nachfolgend beschrieben werden.

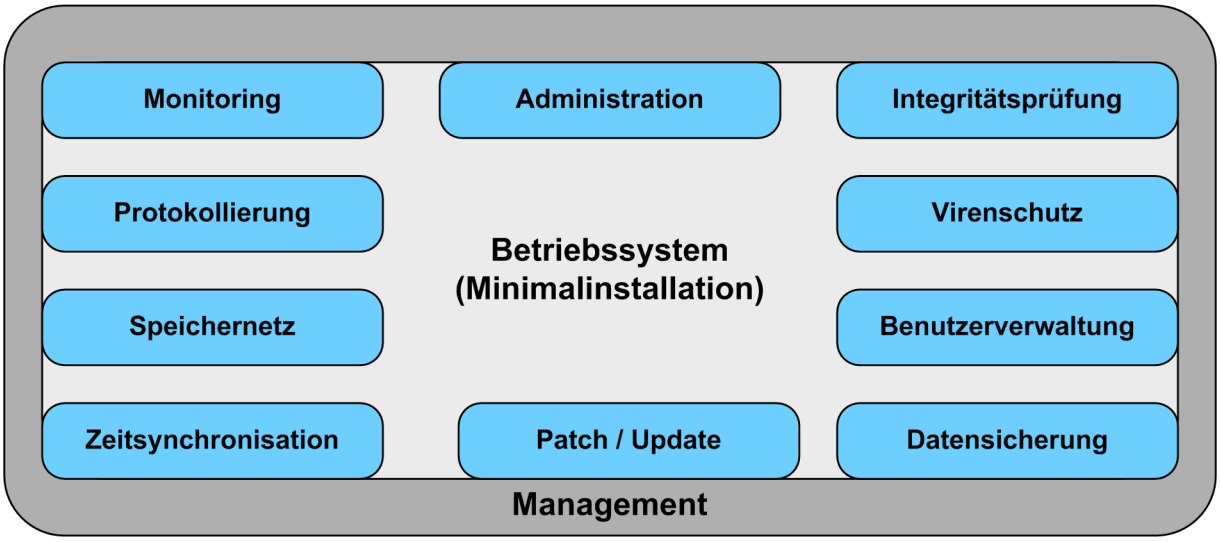


Abbildung 3.3: Dienste und Schnittstellen des Betriebssystems

- Ein Dienst zur Administration:
  Dieser ermöglicht Administratoren die lokale oder auch entfernte Anmeldung am Betriebssystem, um Installations- und Wartungsaufgaben durchzuführen.
- Ein Dienst für das Monitoring:
  Dieser Dienst kommuniziert mit dem zentralen Monitoring und informiert u. a. über den Hardwarestatus, den Speicherverbrauch und den Status der laufenden Dienste.
- Ein Dienst für die Protokollierung:
  Dieser Dienst nimmt die lokal protokollierten Meldungen entgegen und leitet diese zur Auswertung an den zentralen Protokollierungsserver weiter.
- Ein Dienst zur Zeitsynchronisation:
  Dieser Dienst aktualisiert in regelmäßigen Abständen die lokale Uhrzeit des Servers mit der Uhrzeit der zentralen Zeitquelle.
- Ein Dienst für das Patch- und Änderungsmanagement:
  Dieser Dienst kommuniziert mit der zentralen Softwareverteilung, berichtet über aktuell installierte Software und deren Versionsstände, nimmt Installationsaufträge für neue Software und Updates entgegen und führt diese aus.
- Ein Dienst zur Durchführung der Datensicherung:
  Dieser Dienst kommuniziert mit der zentralen Datensicherung und sichert die lokalen Daten nach den vorgegebenen Zeitintervallen.
- Ein Dienst für die Kommunikation mit der zentralen Benutzerverwaltung:
  Dieser Dienst nimmt die lokalen Authentisierungsanfragen entgegen, leitet diese zur Verifikation an die zentrale Benutzerverwaltung weiter und informiert die anfragenden Dienste und Programme über die Rückmeldung der Benutzerverwaltung.

- Ein Dienst zur Überwachung der Systemintegrität:
  Änderungen an den zu überwachenden Objekten werden über diesen Dienst dem zentralen Management für die Integritätsprüfung mitgeteilt.
- Ein Dienst zur Kommunikation mit dem Speichernetz:
  Dieser Dienst kann ggf. bereits im Betriebssystemkern integriert sein und stellt das Protokoll zur Verfügung, mit dem auf das Speichernetz zugegriffen werden kann.
- Einen Dienst zur zentralen Kommunikation mit dem Virenschutzprogramm:
  Dieser Dienst kommuniziert mit dem zentralen Management des Virenschutzprogramms und tauscht darüber u. a. aktuelle Virensignaturen oder Konfigurationseinstellungen aus und informiert über möglichen Virenbefall.

Die hier aufgeführten Dienste sollen Teil einer Basisinstallation des Betriebssystems sein. Darauf aufbauend werden noch die Dienste installiert, die für die eigentliche Aufgabenerfüllung des Servers benötigt werden. Für die zusätzlich installierten Dienste können sich noch Anforderungen ergeben, die durch zusätzliche Maßnahmen abgesichert werden müssen. Als Beispiel für server-spezifische Dienste wird hier auf die folgenden Studien der ISi-Reihe verwiesen:

- Sicheres Bereitstellen von Webangeboten (ISi-Web-Server) und
- Sicherer Betrieb von E-Mail-Servern (ISi-Mail-Server).

Für alle auf dem Server betriebenen Dienste gilt: Der Betrieb eines Dienstes mit Administrator-rechten ist wenn möglich zu vermeiden. Dies verringert die Auswirkungen, falls eine Schwachstelle der Dienst-Software ausgenutzt wird.

3.2.4 Benutzerverwaltung

Für die Grundarchitektur wird eine zentrale Benutzerverwaltung gefordert. Die zentrale Benutzer-verwaltung kann mittels eines Verzeichnisdienstes (Active Directory, LDAP, etc.) implementiert werden. Beim Anlegen von Benutzern ist darauf zu achten, dass der Benutzer nur die Rechte besitzt, die zur Erfüllung seiner Aufgaben notwendig sind. Um eine lokale Administration bei einem Ausfall der zentralen Benutzerverwaltung zu ermöglichen, muss darauf geachtet werden, dass lokale Administrationskonten angelegt werden.

In der Variante 5.1.4.A wird eine lokale Benutzerverwaltung beschrieben, die bei Bedarf z. B. bei kleinen Unternehmen (siehe auch Abschnitt 7.2.1) ebenfalls genutzt werden kann.

Rollenbasierte Rechtevergabe

Für den Betrieb wird eine rollenbasierte Rechtevergabe empfohlen. Dies ermöglicht die Konfiguration von Berechtigungen für Mitarbeiter mit gleichartigen Aufgaben, damit nicht die Berechtigungen eines jeden Mitarbeiters separat konfiguriert werden müssen. Dies kann z. B. unter Windows mittels Gruppenrichtlinien im Active Directory und unter Linux / Unix mittels RBAC (Role Based Access Control) umgesetzt werden.

Authentisierung

Innerhalb der Grundarchitektur wird die Authentisierung mindestens mittels Benutzername und Passwort gefordert. Passwörter bieten eine einfache Möglichkeit anhand einer Identität (der Benutzerkennung) und Wissen (das Passwort) eine Zugangsüberprüfung durchzuführen. Zur Ver-wendung von Passwörtern auf den Server-Systemen innerhalb der Grundarchitektur müssen klare

Regeln in einer Passwortrichtlinie definiert werden. Die Vorgaben werden in Abschnitt 4.2.5 behandelt.

Um die Passwortrichtlinien umzusetzen, müssen diese auf dem Betriebssystem oder der zentralen Benutzerverwaltung konfiguriert werden. Dies hat den Vorteil, dass die Passwörter automatisch von dem Betriebssystem bzw. der Benutzerverwaltung bei deren Erstellung geprüft werden. Eine manuelle Überprüfung der Passwörter hinsichtlich der Richtlinien ist dadurch nicht notwendig. Zusätzlich zu der Passwortrichtlinie ist darauf zu achten, dass Passwörter von dem Betriebssystem oder der zentralen Benutzerverwaltung verschlüsselt abgelegt werden.

3.2.5 Protokollierung

In der Grundarchitektur wird eine zentrale Protokollierung innerhalb eines Management-Netzes gefordert, um eine detaillierte Analyse bei Fehlerfällen oder Angriffen vornehmen zu können. Die lokale Protokollierung eines Servers protokolliert alle sicherheitsrelevanten Ereignisse und leitet diese an den zentralen Protokollierungsserver weiter. Die Vorgaben zur Protokollierung werden in Abschnitt 4.2.5 behandelt.

Zusätzlich zu der zentralen Protokollierung wird empfohlen die Protokolldaten auch lokal auf dem Server zu speichern, um diese z. B. bei der Analyse von Problemen schnell heranziehen zu können und um eine redundante Speicherung zu haben. Um Vorkommnisse frühzeitig zu erkennen, ist darauf zu achten, dass eine regelmäßige Überprüfung der Protokolldaten durchgeführt wird.

Nachfolgend werden einige Beispiele relevanter Ereignisse aufgeführt, die protokolliert werden sollen:

- die erfolgreiche und die fehlgeschlagene Anmeldung am Server
- die Verweigerung des Zugriffs auf Dateien aufgrund fehlender Rechte
- das erfolgreiche und das fehlgeschlagene Einspielen von Updates
- das manuelle oder automatische Starten und Beenden von Systemdiensten und Anwendungen
- die Meldung kritischer Systemzustände (z. B. nicht genügend Speicherplatz auf der Festplatte oder Speicherfehler)

Bei der Erfassung von Systemereignissen werden die folgenden Informationen gespeichert:

- das Ereignis selbst
- Datum und Uhrzeit des Auftretens
- Verursacher (Prozess, falls möglich auch der zugehörige Benutzer)
- weitere ereignisspezifische Informationen (z. B. die Datei, auf die der Zugriff verweigert wurde).

Bei allen Protokollierungsmaßnahmen sind die geltenden datenschutzrechtlichen Bestimmungen genau einzuhalten, da die erfassten Daten potenziell die Privatsphäre lokaler Netzteilnehmer oder externer Kooperationspartner berühren. Daher sind die Grundsätze des Datenschutzes − zum Beispiel das Wesentlichkeitsprinzip (Datensparsamkeit) und die Zweckbindung − schon bei der Planung und Durchführung von Protokollierungsmaßnahmen umfassend zu berücksichtigen.

3.2.6 Monitoring

Über das Monitoring wird die Verfügbarkeit des Servers überwacht. Das Monitoring hat zentral zu erfolgen, um eine einfache Auswertung und Alarmierung im Fehlerfall zu ermöglichen. Um möglichst frühzeitig den Ausfall von Software- oder Hardware-Komponenten festzustellen, wird das Monitoring dieser Komponenten innerhalb der Grundarchitektur gefordert. Bei dem Monitoring eines Server-Systems müssen mindestens die folgenden Dinge überwacht werden:

- Hardware:
  - Temperatursensoren (CPU, Gehäuse, etc.), um einer Überhitzung und dadurch dem Ausfall von Hardware-Komponenten vorzubeugen.
  - Funktionsweise von Lüftern, Festplatten, Netzteilen, etc. Dies ist gerade bei redundanten Komponenten zwingend notwendig, da häufig der Ausfall einer Komponente nicht auffällt, da die Zweite den Betrieb übernimmt.
- Betriebssystem:
  - Speicherbedarf des Systems (Arbeitsspeicher, Festplattenspeicher). Zu wenig Speicherplatz kann zu einem unerwünschten Systemverhalten führen (z. B. unerwartetes Beenden von Prozessen oder Fehlermeldungen, die nicht auf das Problem hinweisen).
    Wenn kein ausreichender Arbeitsspeicher vorhanden ist, verlangsamt sich die Bearbeitungszeit des Betriebssystems, da immer wieder Teile des Arbeitsspeichers auf die Festplatte ausgelagert bzw. von der Festplatte eingelesen werden müssen.
  - Netz- und CPU-Auslastung des Systems. Um einer Überlastung des Systems vorzubeugen, muss die Auslastung von Netz und CPU überwacht werden. Bei Anzeichen von Überlastung müssen ggf. weitere Systeme angeschafft werden. Anzeichen von Überlastung kann z. B. eine ständig hohe CPU-Auslastung oder die Größe und Nutzung der Auslagerungsdatei sein.
  - Monitoring der zur Verfügung gestellten Dienste. Die zur Verfügung gestellten Dienste müssen auf ihre Funktionalität hin überwacht werden. Ein einfaches Überwachen auf Vorhandensein eines Prozesses reicht nicht aus, da ein Dienst z. B. aufgrund eines Softwarefehlers noch läuft, jedoch keine Daten mehr verarbeiten kann (Aufhängen eines Dienstes). Dies betrifft auch die Anzahl laufender Prozesse und Dienste, die von dem Server angeboten werden.
  - Korrekte Funktion der Zeitsynchronisation. Hierbei wird die Systemzeit des zu überwachenden Servers mit der Referenzzeit verglichen, um eine evtl. nicht korrekte oder fehlende Zeitsynchronisation zu erkennen.
  - Regelmäßige Durchführung der Datensicherung.

3.2.7 Integritätsprüfung

Die Integritätsprüfung soll für die Überwachung aller Betriebssystem-relevanten Daten genutzt werden, damit unerlaubte oder ungewollte Änderungen erkannt werden. Hierzu gehören u. a. die folgenden Daten:

- Konfigurationsdateien
- Treiber
- dynamische Bibliotheken (engl. shared libraries)

- Kernel-Module
- Konfigurationseinträge in der Windows Registry, etc.

Viele Hersteller von Integritätsprüfungen bieten spezielle Standardprofile an, um diese Verzeichnisse und Pfade zu überprüfen. Diese sollen bevorzugt verwendet werden, da diese Profile auch sich häufig ändernde Dateien bzw. Registrierungsschlüssel berücksichtigen und diese von der Integritätsprüfung ausschließen. Auf diese Weise wird False Positive-Meldungen vorgebeugt.

3.2.8 Datensicherung

Um einem Datenverlust vorzubeugen, ist es erforderlich, eine Datensicherung für die auf dem Server gespeicherten Daten einzurichten. Eine Datensicherung gewährleistet, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wieder aufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen. Es gilt dabei zu unterscheiden, ob nur Teile des Betriebssystems (z. B. Konfigurationsdateien) oder eine Vollsicherung des gesamten Systems erfolgen soll. Es müssen alle Dateien gesichert werden, die für eine Inbetriebnahme eines identischen Servers auf einem neu installierten System benötigt werden. Die Anforderungen an die Datensicherung eines Servers müssen in einem Datensicherungskonzept beschrieben werden, welches die nachfolgenden Punkte behandeln muss:

- Art und Umfang der Datensicherung (Voll-, inkrementell oder differenzielle Sicherung; siehe 2.3.16.1).
- Welche Daten von welchen Systemen gesichert werden sollen.
- Wie häufig und wann Daten gesichert werden sollen (stündlich, täglich, wöchentlich, etc.).
- Wie schnell in einem Schadensfall die Rekonstruktion der Daten zu erfolgen hat.
- Wie hoch das zu sichernde Datenvolumen ist und wie groß dieses Datenvolumen zukünftig anwächst.
- Welche Aufbewahrungsfrist die Datensicherung hat. Ggf. gibt es rechtliche Vorgaben bzgl. der Aufbewahrungsfristen, die es zu berücksichtigen gilt. Nach Ablauf der Aufbewahrungsfrist sind die Daten zu löschen.
- Ob Vertraulichkeitsanforderungen für die gesicherten Daten zu berücksichtigen sind. Ggf. muss die Datensicherung verschlüsselt gespeichert werden.
- Welche Datensicherungsmedien verwendet werden sollen (Festplatte, Band, DVD, etc.).

Für die Grundarchitektur wird eine regelmäßige Vollsicherung mit aufbauender inkrementeller Datensicherung des gesamten Systems empfohlen. Je nach Anwendungsfall und Anforderungen kann jedoch eine andere Sicherung eingesetzt werden. Das Datensicherungskonzept muss für die Gewährleistung einer funktionierenden Datensicherung die Restaurierbarkeit der Daten mittels praktischer Übungen zwingend vorsehen.

3.2.9 Aktualisierung des Servers

Das Betriebssystem und die darauf installierten Dienste sind stets aktuell zu halten, um die Stabilität und Sicherheit des Server-Systems zu gewährleisten. Hersteller bringen kontinuierlich Updates heraus, die Fehler korrigieren, neue Schnittstellen bereitstellen oder Sicherheitslücken schließen. Die Aktualisierung des Servers ist Teil des Patch- und Änderungsmanagements.

Aufgabe des Patch- und Änderungsmanagement ist es, Veränderungen an Betriebssystem, Diensten, Infrastruktur, Dokumentationen, Prozessen und Verfahren zu steuern und zu kontrollieren. Dies betrifft sowohl ein Update von Software-Komponenten (z. B. durch Sicherheitspatches) als auch die Einführung von neuen Applikationen.

Innerhalb der Grundarchitektur wird die regelmäßige Aktualisierung von Software-Komponenten und Betriebssystem bzgl. Sicherheitspatches und Updates gefordert. Das Einspielen dieser Aktualisierungen sollte über eine zentrale Softwareverteilung durchgeführt werden.

Durch ein Update von Software können Schwachstellen beseitigt oder Funktionen erweitert werden. Ein Update ist insbesondere dann notwendig, wenn Schwachstellen bekannt werden, die Auswirkungen auf den sicheren Betrieb haben, wenn Fehlfunktionen auftreten oder eine funktionale Erweiterung aus sicherheitstechnischen oder fachlichen Erfordernissen notwendig wird.

Bevor eine Aktualisierung der Software vorgenommen wird, müssen die Funktionalität, die Interoperabilität und die Zuverlässigkeit der neuen Komponenten genau geprüft werden. Dies geschieht in einer separaten Testumgebung, bevor das Update in den produktiven Einsatz übernommen wird.

Die Häufigkeit der Aktualisierung hängt von den veröffentlichten Sicherheitsempfehlungen der Hersteller ab. Auf verschiedenen Herstellerseiten werden (auch betriebssystemunabhängige) Sicherheitsempfehlungen ausgegeben. Die verantwortlichen Administratoren sollten diese über Newsletter, RSS-Feeds, etc. abonnieren und regelmäßig prüfen.

3.2.10 Speichernetz

Ein Speichernetz ist innerhalb der Grundarchitektur eine optionale Komponente (siehe Abbildung 3.2) und kann bei Bedarf implementiert werden. Dies kann z. B. der Fall sein, wenn mehrere Server auf dieselben Daten zugreifen müssen (z. B. Virtualisierungsserver innerhalb eines Hochverfügbarkeitsclusters). Bei der Verwendung eines Speichernetzes ist folgendes zu berücksichtigen:

- In der Grundarchitektur wird keine Authentisierung für den Zugriff auf ein Speichernetz gefordert. Bei hohem Schutzbedarf hat jedoch eine Authentisierung zu erfolgen (siehe Variante 5.2.4.A).
- Die Datenübertragung zwischen dem Speichersystem und dem zugreifenden System ist in der Regel unverschlüsselt. Sind erhöhte Anforderungen an die Vertraulichkeit der Daten gestellt, dann muss eine Verschlüsselung der Kommunikationsstrecke eingesetzt werden (siehe Variante 5.2.4.B).
- Bei dem Einsatz eines SAN wird innerhalb der Grundarchitektur ein dediziertes Speichernetz gefordert, um das eigentliche Betriebsnetz nicht mit erhöhtem Datenverkehr zu belasten.
- NAS-Systeme befinden sich in der Regel in demselben Netzsegment wie die zugreifenden Benutzer, da diese Systeme häufig als zentraler DatenServer (FileServer) eingesetzt werden. Im Gegensatz zu einem SAN werden hierbei wesentlich weniger Daten über das Netzwerk ausgetauscht, sodass hierfür kein dediziertes Speichernetz gefordert wird.

3.2.11 Virenschutzprogramm

Der Einsatz eines Virenschutzprogramms innerhalb der Grundarchitektur ist abhängig von der Anwendung bzw. dem Dienst, der vom Server angeboten wird. Die folgenden Hilfestellungen sollen bei der Entscheidung über den Einsatz eines Virenschutzprogramms behilflich sein:

- Systeme, die für den Dateiaustausch oder die Dateiablage zuständig sind, müssen ein Virenschutzprogramm installiert haben, um die Verbreitung von Schadsoftware zu unterbinden.
- Innerhalb der Grundarchitektur gemäß [ISi-LANA] (siehe Abbildung 3.1) wird durch das ALG (Application Level Gateway) bereits eine Virenprüfung vorgenommen. Für Systeme, die vor dem ALG platziert sind, wird der Einsatz eines Virenschutzprogramms empfohlen, da ansonsten kein Schutz vor Schadsoftware gegeben ist. Für Systeme hinter dem ALG kann dies als Ergänzung eingesetzt werden.

Wird auf ein Virenschutzprogramm verzichtet, muss eine Einzelfallbetrachtung der Risiken erfolgen. Dies trifft z. B. auf Server-Systeme zu,

- die keinen Datenaustausch mit anderen Systemen vornehmen oder
- auf denen CPU-intensive Programme laufen (z. B. für Berechnungen) oder

auf denen Dienste laufen, die einen hohen Datendurchsatz erfordern.

3.3 Organisatorische Maßnahmen

Wie bereits in Abschnitt 3.1 erwähnt, wird für die Grundarchitektur keine redundante Auslegung einzelner Komponenten oder kompletter Server gefordert. Innerhalb der Grundarchitektur soll durch ein Notfallvorsorgekonzept die Verfügbarkeit von Diensten und Servern sichergestellt werden. Ein Notfallvorsorgekonzept enthält vorbeugende Maßnahmen, die den Schaden oder die Eintrittswahrscheinlichkeit von Risiken reduzieren sowie Maßnahmen, um ein schnelles und sinnvolles Reagieren auf einen Vorfall zu ermöglichen. Dort sind die direkt für die Bewältigung eines Notfalls benötigten Informationen wie beispielsweise Kontaktinformationen von Verantwortlichen und Handlungsanweisungen beschrieben.

Für die IT-Infrastruktur ist ein entsprechendes Konzept für die Prozesse, Systeme und Maßnahmen zu erstellen und umzusetzen. In diesem werden die für den Notbetrieb vorgesehenen Notprozesse, aber auch die Wiederanlaufphase, die Prozesse für die Rückführung und die Nacharbeiten betrachtet und die Vertraulichkeit und Integrität der Prozesse sowie der verarbeiteten Informationen für jeden Zwischenschritt sichergestellt. Für Wiederherstellungs- bzw. Wiederanlaufpläne kann dies beispielsweise bedeuten, dass eine bestimmte Reihenfolge der Arbeitsschritte eingehalten werden muss. So darf z. B. die Wiederherstellung vertraulicher Daten in einer Anwendung erst erfolgen, wenn die Netzsicherheit u. a. durch ein vollständig wiederhergestelltes Sicherheits-Gateway gewährleistet ist.

Die IT-Grundschutz-Kataloge (siehe [BSI_GSK]) geben hierzu weiterführende Hinweise hinsichtlich der Organisation, Infrastruktur, Rollentrennung und Sensibilisierung. Weitere Informationen sind ebenfalls dem BSI-Standard 100-4 für das Notfallmanagement [BSI_STD_100-4] zu entnehmen.

3.4 Netzmanagement

Das Management der Server-Systeme erfolgt über das Managementnetz (siehe [ISi-LANA], Abschnitt 4.4). Abbildung 3.4 zeigt den Aufbau eines solchen separaten Netzes. Alle Server der jeweiligen Segmente „Internet Verbindung“, „Sicherheits-Gateway“ und „Internes Netz“ werden aus der Management-Zone administriert. Das Managementnetz ist ein durch separate Paketfilter abgesichertes Netz und dient ausschließlich zur Administration und Wartung der eingesetzten Systeme.

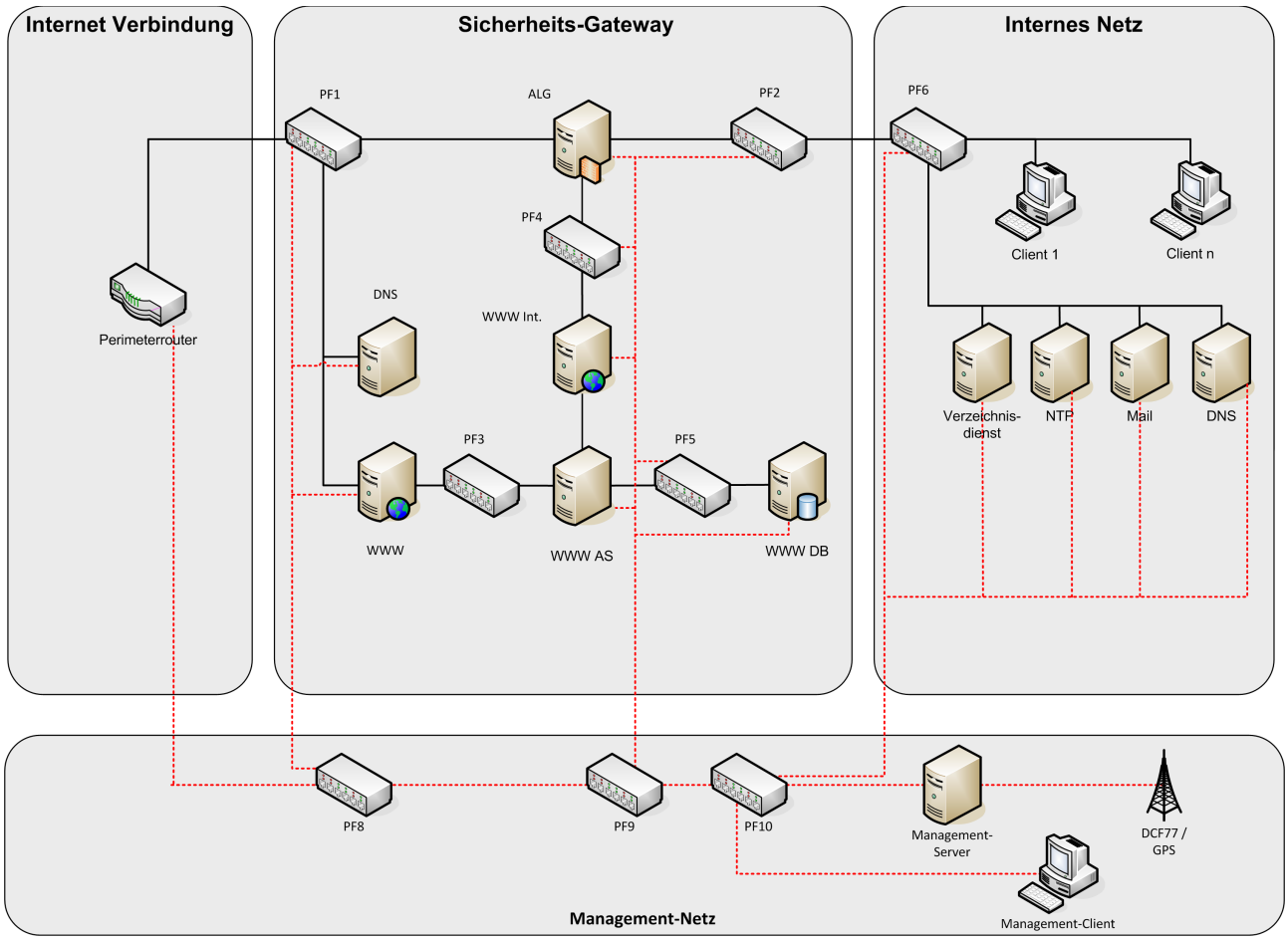


Abbildung 3.4: Grundarchitektur mit Management-Zone

Durch die Management-Zone erfolgt eine vollständige Trennung zum Produktionsnetz, in dem die Nutzdaten verarbeitet werden. Hierdurch wird eine Erhöhung der Sicherheit erzielt, weil ein separates Netz die Angriffsmöglichkeiten auf das Netzmanagement durch Abhören, Eindringen oder Denial-of-Service-Attacken erschwert. Die Administration aus einem separaten Netz heraus wird auch Out-of-Band Management genannt.

Eine Aufgabe der Management-Zone ist es, alle Management-Daten zentral zu sammeln und zu verarbeiten. Hierzu gehören die Daten der Integritätsprüfung, Virenscanner, Daten des Monitorings, Protokollierung der Systeme, etc. Durch die zentrale Datenhaltung der Überwachungsdaten, kann eine effizientere Analyse der Daten erfolgen, da nicht jedes System einzeln analysiert werden muss. Für eine Auswertung und Analyse der Daten ist es wichtig, dass die Uhren aller Server-Systeme synchronisiert werden. Dies kann von einem vertrauenswürdigen Server aus dem Internet oder auch lokal erfolgen und z. B. mittels des Network Time Protocols (NTP) zur Verfügung gestellt werden.

Um eine höhere Verfügbarkeit des NTP-Dienstes zu erhalten, ist es auf jeden Fall notwendig eine lokale hochgenaue Zeitquelle einzusetzen, da bei einem Ausfall des Internetzugangs keine Zeitsynchronisation mehr möglich wäre. Diese lokale Zeitquelle kann z. B. mit DCF77 oder GPS realisiert werden.

In Abschnitt 3.2 wurden bereits die Sicherheits-Komponenten Monitoring, Protokollierung und Zeitsynchronisation vorgestellt, die sich auch in der Abbildung 3.4 wiederfinden. Der Server für die Protokollierung und das Monitoring (in der Abbildung allgemein MGMT-Station genannt) befindet sich in der Zone „Management-Netz“. Dort werden alle Protokolldaten gespeichert und auf besondere Vorkommnisse hin analysiert sowie die Verfügbarkeit und die korrekte Funktion der IT-Infrastruktur überwacht. Ebenfalls in derselben Zone untergebracht ist die Quelle zur Zeitsynchronisation, die in der Abbildung als DCF-77 Signal aufgeführt ist. Durch entsprechende Freischaltungen von Regeln auf den Paketfiltern können die Server der IT-Infrastruktur das Zeitsignal aus der Zone „Management und Überwachung“ abrufen.

3.5 Grundarchitektur der Infrastruktur mit virtualisierten Komponenten

Bei den in Abbildung 3.1 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 3.5 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

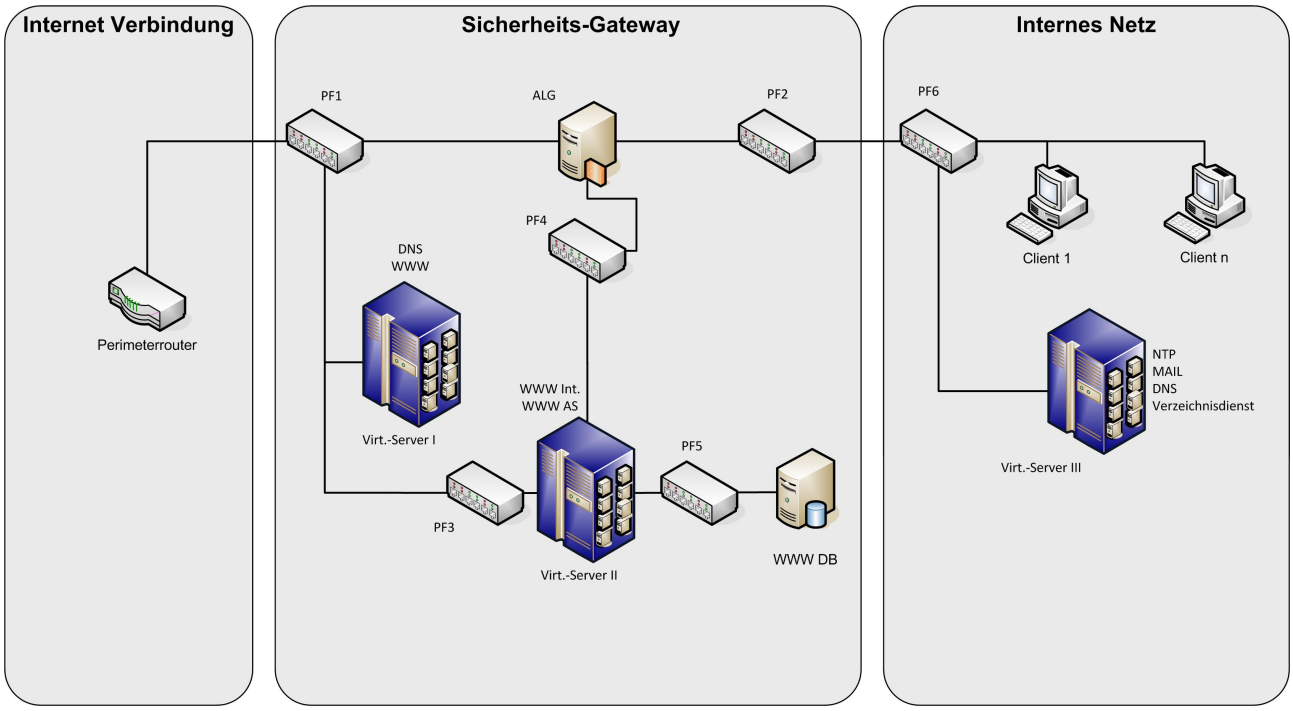


Abbildung 3.5: Grundarchitektur mit virtualisierten Komponenten

Virtualisierung bietet den Vorteil, 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. Nachteilig ist jedoch, dass bei dem Ausfall des Virtualisierungsservers alle darauf laufenden Betriebssysteme und Dienste betroffen sind, sodass dies oft größere Auswirkungen auf andere Systeme hat, als bei dem Einsatz einzelner Server-Systeme. Daher wird in der Grundarchitektur die redundante Auslegung der Hardware für Virtualisierungsserver empfohlen. Der redundante Aufbau einer virtualisierten Umgebung setzt in der Regel den Einsatz eines zentralen Speichernetzes (SAN oder NAS) voraus, auf dem die Betriebssysteme, Konfigurationsdaten und Statusinformationen gespeichert sind. In Abbildung 3.5 ist aufgrund der Übersichtlichkeit auf den redundanten Aufbau der Virtualisierungsserver und des Speichernetzes verzichtet worden.

Der Einsatz redundanter Server kann auch zur Lastverteilung zwischen den einzelnen Server-Systemen genutzt werden. Die meisten Virtualisierungsprodukte bieten heutzutage die Möglichkeit, die Auslastung auf mehrere Server zu verteilen. Hierzu werden die betriebenen virtuellen Maschinen auf die einzelnen Virtualisierungsserver aufgeteilt, um die zur Verfügung stehenden Ressourcen (Arbeitsspeicher, CPU, etc.) besser auszunutzen.

Um dedizierte physische Systeme auf einem Virtualisierungsserver zusammenzuführen, müssen die folgenden Hinweise beachtet werden:

- Nur Komponenten aus demselben Netzsegment dürfen innerhalb der Grundarchitektur auf einem Virtualisierungsserver zusammengelegt werden. Mit Netzsegment ist jeweils der Bereich gemeint, der von zwei Paketfiltern getrennt wird. Als Variante wird auch die Virtualisierung von Komponenten aus unterschiedlichen Netzsegmenten beschrieben (siehe Variante 5.2.2.A).
- Jeder Paketfilter muss mit einer eigenen physischen Netzwerkkarte an den Virtualisierungsserver angebunden werden, um eine ausreichende Isolation der Netze sicherzustellen.
- Systeme aus unterschiedlichen Schutzzonen (Internet-Verbindung, Sicherheits-Gateway und Internes-Netz) dürfen nicht zusammen auf einem System virtualisiert werden.
- Es dürfen nur Server mit normalem Schutzbedarf auf demselben Virtualisierungsserver betrieben werden. Die Virtualisierung von IT-Systemen mit hohem Schutzbedarf ist im Einzelfall abhängig von den Anwendungen und der eingesetzten Virtualisierungstechnologie (siehe Variante 5.2.2.B).

Des weiteren muss das Virtualisierungsprodukt eine ausreichende Kapselung und Isolation des virtuellen Betriebssystems von dem Host-Betriebssystem ermöglichen. Hiermit ist das Einschränken bzw. Deaktivieren von Schnittstellen zwischen virtueller Maschine und Virtualisierungsserver gemeint sowie zwischen den virtuellen Maschinen. Einige Virtualisierungsprodukte bieten die Installation von Gastwerkzeugen an, die unterschiedliche Schnittstellen zwischen Gast und Host zur Verfügung stellen. Diese Schnittstellen können bei einem Angriff auf das Gast-System ggf. zur Kompromittierung des Host-Systems ausgenutzt werden. Werden Gastwerkzeuge für den Betrieb des Servers benötigt, dann ist darauf zu achten, dass nur die benötigten Schnittstellen installiert und aktiviert werden. Schnittstellen, die es z. B. ermöglichen, von dem Host-Betriebssystem aus Skripte im virtuellen IT-System auszuführen, dürfen nicht aktiviert werden.

Weitere Punkte, die bei dem Einsatz von Virtualisierung beachtet werden sollen:

- Bei der Datensicherung ist darauf zu achten, dass sowohl die Daten des Virtualisierungsservers als auch die Daten der virtualisierten Betriebssysteme gesichert werden.

- Bei der Live Migration von virtuellen Maschinen ist darauf zu achten, dass ein virtuelles Betriebssystem nach der Migration nicht an ein anderes Netz angebunden wird.
- Für das Betriebssystem des Virtualisierungsservers gelten auch alle Anforderungen, die in der Grundarchitektur in Abschnitt 3.2 und 3.4 aufgeführt sind (Minimalisierung, Monitoring, Zeitsynchronisation, Anbindung an eine zentrale Benutzerverwaltung, etc.).
- Werden aus Verfügbarkeitsgründen mehrere Virtualisierungsserver eingesetzt, muss jeder einzelne Virtualisierungsserver Zugriff auf die virtuellen Maschinen haben. Daher müssen die virtuellen Maschinen auf einem zentralen Speichernetz abgelegt werden, auf das jeder der Virtualisierungsserver Zugriff hat.
- Für einen Virtualisierungsserver müssen unterschiedliche Netze konfiguriert werden, die jeweils eine andere Verwendung haben. Eine Übersicht der zu konfigurierenden Netze ist in Abschnitt 4.2.13 beschrieben.

Üblicherweise greifen bei der Verwendung eines Speichernetzes unterschiedliche Systeme auf den zur Verfügung gestellten Speicherplatz zu. Dies können Server sein, die unterschiedliche Aufgaben haben (Virtualisierungsserver, Datenbankserver, etc.), die sich in demselben oder auch in unterschiedlichen Netzsegmenten befinden. Der Zugriff von Servern mit unterschiedlichen Aufgaben auf dieselbe Speichereinheit ist zu vermeiden, damit die dort gespeicherten Daten nicht unbeabsichtigt von anderen Systemen gelöscht oder verändert werden. Die logische Trennung von Daten auf unterschiedliche Speichereinheiten kann durch die von Massenspeichertechnologien zur Verfügung gestellten Mechanismen erfolgen. Diese Mechanismen sind z. B.:

- die Konfiguration einer erforderlichen Authentisierung bei dem Einsatz von NAS-Systemen
- die Bereitstellung von unterschiedlichen Freigaben (bzw. Laufwerken) für unterschiedliche Server bei dem Einsatz von NAS-Systemen
- die Separierung der Daten unterschiedlicher Server auf einzelne LUNs bei dem Einsatz eines SAN
- die Verwendung von LUN Masking bei dem Einsatz eines SANs
- die Verwendung von SAN Zoning bei dem Einsatz von Fibre Channel innerhalb des SANs.

4 Komponenten sicher auswählen, konfigurieren und betreiben (normaler Schutzbedarf)

Im vorherigen Abschnitt wurde die Grundarchitektur einer sicheren Server-Infrastruktur vorgestellt, ohne dabei im Detail auf die Umsetzung einzugehen. Dieser Abschnitt gibt umfassende Empfehlungen, wie die in der Grundarchitektur enthaltenen Komponenten sicher ausgewählt, konfiguriert und betrieben werden können. Der Aufbau des Abschnitts orientiert sich dabei am Lebenszyklus eines Server-Systems.

- In Abschnitt 4.1 werden die Sicherheitsanforderungen bei der Auswahl und Beschaffung der Server-Komponenten beschrieben.
- In Abschnitt 4.2 wird auf die Installation und die Minimierung des Betriebssystems sowie auf die sichere Konfiguration der einzelnen Komponenten eingegangen.
- In Abschnitt 4.3 wird beschrieben, auf was beim sicheren Betrieb eines Server-Systems zu achten ist.
- In Abschnitt 4.4 wird die Außerbetriebnahme beschrieben.

Einige Punkte sind in den Abschnitten als „Optional“ aufgeführt, da sie nicht innerhalb der Grundarchitektur aus Abschnitt 3 gefordert werden, aber bei Bedarf umgesetzt werden können.

4.1 Grundanforderungen an ein sicheres Produkt

Die Grundanforderungen an ein sicheres Produkt gliedern sich in allgemeine, nicht auf spezielle Produkte oder Komponenten beschränkte Eigenschaften sowie spezifische Anforderungen, die das Betriebssystem, die Hardware oder die darauf installierten Dienste betreffen. Der Abschnitt 4.1.1 geht dabei auf die allgemeinen Aspekte ein. Die Abschnitte 4.1.2ff behandeln dann die spezifischen Anforderungen an den einzelnen Komponenten.

4.1.1 Übergreifende Aspekte

Dieser Abschnitt beschreibt die übergeordneten Anforderungen, die generell gelten und die im Vorfeld der weiteren Planung zu beachten sind.

4.1.1.1 Planung

Im Rahmen der Planung wird zunächst entschieden, welcher Dienst auf dem Server zum Einsatz kommen soll. Daraus ergeben sich Anforderungen an das Betriebssystem, die Hardware und ggf. des einzusetzenden Speichernetzes. In der Planungsphase muss zusätzlich entschieden werden, ob der angebotene Dienst auf dedizierter Hardware oder auf einer virtualisierten Plattform betrieben werden soll.

4.1.1.2 Auswahl und Bezug der Komponenten

Die anzuschaffenden Hard- und Software-Komponenten sollten direkt vom Hersteller oder von einem autorisierten Fachhändler bezogen werden, da diese für eine etwaige Garantieabwicklung

verantwortlich sind und Wartungsverträge ebenfalls über den Fachhandel bzw. Hersteller abgeschlossen werden müssen.

Wird Software von der Webseite des Herstellers heruntergeladen, so ist diese mit den auf der Herstellerseite bereitgestellten Informationen (z. B. Prüfsumme oder Signatur der Datei) zu vergleichen, um Manipulationen an der Datei auszuschließen.

Bei der Auswahl sollten neuere Produkt-Versionen gegenüber älteren bevorzugt werden, da diese oft neue oder verbesserte Sicherheitsmechanismen enthalten und Fehler der Software behoben wurden. Neuere Versionen haben meistens eine längere Herstellerunterstützung bzgl. Updates.

Es sollten Produkte der Hersteller bevorzugt werden, die eine dauerhafte Versionspflege gewährleisten sowie zeitnah auf bekannt gewordene Sicherheitsschwachstellen reagieren und Patches bereitstellen. Dies gilt sowohl für die Software als auch für die Firmware bei Hardware-Komponenten.

Bietet das zu verwendende Produkt kryptografische Funktionen an, die auch im Betrieb eingesetzt werden, dann müssen diese auf der Basis standardkonformer, kryptografisch starker Algorithmen mit ausreichender Schlüssellänge realisiert sein. Die vom BSI empfohlenen Verschlüsselungsalgorithmen und Schlüssellängen müssen von dem Produkt unterstützt werden[1].

4.1.1.3 Lizenzierung

Der Einsatz eines Betriebssystems bzw. der darauf betriebenen Dienste ist häufig einer Lizenzierung unterworfen. Ohne Lizenzierung sind einige Produkte nicht oder nicht im vollen Umfang einsetzbar. Bei Serverbetriebssystemen beinhaltet die Lizenzierung oft die Aktualisierung von Betriebssystemversionen und Sicherheitsupdates. Einige Produkte verfügen auch über zeitlich beschränkte Lizenzierungen. Wird diese Lizenz nicht innerhalb einer bestimmten Zeit verlängert, dann stellen diese Produkte ihren Dienst ein oder stehen nur noch eingeschränkt zur Verfügung. Daraus ergibt sich eine Beeinträchtigung der Verfügbarkeit des Dienstes.

Folgende Dinge sollten bei der Lizenzierung berücksichtigt werden.

- Lizenzen sollten unabhängig von der Hardware des darunterliegenden Systems sein, um einen schnellen Austausch des Servers bei einem Hardware-Defekt zu gewährleisten.
- Lizenzen sollten unbefristet gültig sein. Für einige Programme (z. B. Virenschutzprogramm) ist dies typischerweise nicht möglich, sodass befristete Lizenzen akzeptiert werden müssen.

4.1.2 Hardware

Bei der Auswahl der Hardware sind die folgenden Anforderungen zu beachten:

- Um die Leistungsfähigkeit zu ermitteln, müssen die folgenden Aspekte berücksichtigt werden:
  - Die benötigte Rechenleistung der CPU. Ggf. müssen mehrere CPUs eingesetzt werden.
  - Bei der Größe des Arbeitsspeichers sind die Vorgaben des Betriebssystemherstellers und des Herstellers des zu installierenden Dienstes zu beachten.

1 Die Bundesnetzagentur (www.bundesnetzagentur.de) veröffentlicht regelmäßig auf Basis der Angaben des BSI im Bundesanzeiger eine Übersicht über Kryptoalgorithmen, die zur Erzeugung von Signaturschlüsseln, zum Hashen von Daten und zur Prüfung und Erzeugung von digitalen Signaturen als geeignet angesehen werden. Entsprechende aktuelle Informationen sind auch unter http://www.bsi.bund.de/esig/kryptoalg.htm zu finden.

  - Wenn von dem System öfter größere Datenmengen über das Netz transferiert werden, muss eine hochperformante Netzanbindung vorhanden sein. Evtl. muss hierzu gesonderte Hardware eingesetzt werden, die einen höheren Datentransfer garantiert (z. B. bei dem Einsatz von Jumbo-Frames).
  - Sind hohe Anforderungen bzgl. der Performanz oder Ausfallsicherheit von Festplatten vorhanden, dann muss ein RAID-System eingesetzt werden.
- Zukünftige Erweiterungen der Hardware (zusätzliche Festplatten, spätere Anbindung eines externen Massenspeichers, nachträgliches Aufrüsten des Arbeitsspeichers, etc.) sind zu berücksichtigen.
- Bei der Auswahl des Massenspeichers müssen die Anforderungen der zu betreibenden Dienste und Anwendungen berücksichtigt werden. Soll z. B. Speicherplatz auch für Arbeitsplatz-PCs bereitgestellt werden, empfiehlt sich hier der Einsatz eines NAS-Speichers. Soll der Speicher nur von einem oder mehreren Servern genutzt werden (z. B. innerhalb eines Clusters), dann empfiehlt sich der Einsatz eines SAN.
- Die eingesetzten Server-Systeme müssen ein Out-of-Band-Management unterstützen. In-Band-Konfigurierbarkeit muss deaktiviert werden können (Ausführliche Erläuterungen hierzu sind in [ISi-LANA] zu finden.).
- Die eingesetzte Hardware ist mit einer ausreichenden Anzahl von Netzwerkschnittstellen auszustatten. Dies ist insbesondere bei dem Einsatz von Virtualisierungsservern notwendig, da hier mehrere Netze mit unterschiedlichen Zwecken angebunden werden müssen (siehe auch Abschnitt 3.5).
- Es wird empfohlen, einen Prozessor zu verwenden, der Speicherschutzmechanismen (siehe Abschnitt 2.3.14) in Bezug auf die Hardware unterstützt.

Für den Anbieter, über den die Hardware bezogen wird (Fachhandel oder Hersteller), gelten zusätzliche Anforderungen. Diese werden häufig im Rahmen eines Wartungsvertrages geregelt.

- Für die Grundarchitektur ist bei normalem Schutzbedarf eine Erreichbarkeit des Anbieters an Werktagen innerhalb der Arbeitszeit ausreichend.
- Der Anbieter muss eine sichere Versorgung mit Ersatzgeräten gewährleisten. Auch hier genügt für die Grundarchitektur bei normalem Schutzbedarf eine Erreichbarkeit innerhalb der regulären Arbeitszeit.

Hinweis: Darüber hinaus sollte in einem Notfallvorsorgekonzept festgelegt werden, wie auf einen Hardwareausfall, z. B. am Wochenende, zu reagieren ist (z. B. Vorhalten von Ersatzgeräten).

4.1.3 Betriebssystem

Bei der Auswahl des Betriebssystems muss geprüft werden, ob die Dienste, die der Server anbieten soll, darauf lauffähig sind. Des Weiteren sollte das Betriebssystem die folgenden Anforderungen erfüllen:

- Bei der Auswahl des Betriebssystems muss auf Kompatibilität mit der darunterliegenden Hardware geachtet werden. Einige Betriebssysteme setzen eine spezielle Hardware voraus (z. B. Intel, Sparc, Power-PC, etc.).
- Es sollte eine entfernte Administration des Betriebssystems (z. B. über SSH oder RDP) möglich sein. Alternativ kann ein KVM-Switch eingesetzt werden, um eine entfernte Administration durchzuführen.

- Die auf dem Server zur Verfügung gestellten Dienste müssen auf der eingesetzten Version des Betriebssystems lauffähig sein. Dies betrifft z. B. spezielle Funktionen oder Bibliotheken, die von den Diensten benötigt werden.
- Das Betriebssystem muss eine zentrale Protokollierung unterstützen.
- Es muss möglich sein, das Betriebssystem zu minimieren, d.h. nicht benötigte Betriebssystem-Komponenten müssen sich bei der Installation abwählen oder im Nachhinein deinstallieren lassen.
- Das Betriebssystem muss eine dedizierte Rechtevergabe unterstützen, sodass den Benutzern die Berechtigungen zugewiesen werden können, die sie benötigen.
- Die Benutzerverwaltung des Betriebssystems muss eine Anbindung an eine zentrale Benutzerverwaltung unterstützen (z. B. Verzeichnisdienst).
- Sollen externe Speichertechnologien genutzt werden (DAS, NAS, SAN), müssen diese vom Betriebssystem unterstützt werden. Dies betrifft sowohl die Verwendung des Dateisystems als auch die Treiber für die Hardware, die für den Zugriff auf das Speichernetz notwendig sind (z. B. für iSCSI oder Fibre Channel).
- Das Betriebssystem muss Sicherheitsmechanismen wie Speicherschutzmechanismen (s. Abschnitt 2.3.14) und Speicherrandomisierung (s. Abschnitt 2.3.15) unterstützen.
- Um den Betrieb sicherzustellen, muss das Monitoring des Betriebssystems und den darauf installierten Diensten möglich sein.
- Der Hersteller des Betriebssystems muss fortlaufend Updates und Sicherheitspatches bereitstellen. Diese müssen nach Möglichkeit mit einer Herstellersignatur versehen sein, um die Authentizität und Integrität der Updates zu gewährleisten.

4.1.4 Dienste

Bei der Auswahl von Diensten steht in der Regel die Funktionalität im Vordergrund. Stehen mehrere funktional gleichwertige Alternativen zur Verfügung, so sollen Dienste bevorzugt werden, die zusätzlich die folgenden Anforderungen erfüllen:

- Der Dienst muss eine zentrale Protokollierung unterstützen.
- Wird der Dienst in geeigneter Funktionalität von dem Betriebssystem bereitgestellt, sollte dieser verwendet werden. Dies hat den Vorteil, dass die Aktualisierung des Dienstes über die Mechanismen des Betriebssystems erfolgt.

4.1.5 Benutzerverwaltung

Innerhalb der Grundarchitektur sollte eine zentrale Benutzerverwaltung (z. B. über einen Verzeichnisdienst) genutzt werden. Diese Benutzerverwaltung muss die nachfolgenden Anforderungen unterstützen:

- Das Einrichten von Benutzer- und Gruppenrechten muss möglich sein.
- Das Deaktivieren und Löschen von Benutzerkonten muss möglich sein.
- Die eingesetzte Benutzerverwaltung muss kompatibel mit den eingesetzten Betriebssystemen sein (z. B. mit dem vom Betriebssystem genutzten Authentisierungsverfahren).

- Die Vorgaben für Passwörter aus Abschnitt 4.2.5 müssen umgesetzt werden können.
- Bei der Authentisierung mittels Passwörtern dürfen diese nicht im Klartext übermittelt werden.
- Die im Verzeichnisdienst gespeicherten Benutzerdaten müssen sich mit geringem Aufwand anpassen lassen, um auf organisatorische Änderungen (Team-Wechsel, Ausscheiden eines Benutzers) zeitnah zu reagieren.

4.1.6 Protokollierung

Innerhalb der Grundarchitektur muss eine zentrale Protokollierung im Management-Netz erfolgen. Die Meldungen von Betriebssystemen und den darauf betriebenen Diensten sind hierzu an den zentralen Protokollierungsdienst weiterzuleiten. Dabei sind die folgenden Anforderungen zu berücksichtigen:

- Die zentrale Protokollierung muss alle eingesetzten Betriebssysteme unterstützen.
- Es muss ausreichend Speicherplatz für die zentrale Protokollierung bereitgestellt werden. Das zu erwartende Log-Aufkommen der anzubindenden Server-Systeme ist hierzu grob abzuschätzen.
- Da durch das Protokollieren sehr detailliert nachvollzogen werden kann, welche Aktivitäten ein Administrator auf einem Server ausgeführt hat, müssen unbedingt die rechtlichen Rahmenbedingungen, insbesondere zum Datenschutz, beachtet werden. Bereits bei der Planung von Protokollierungsmaßnahmen ist daher die Personalvertretung oder/und der Betriebsrat mit einzubeziehen.

In der Grundarchitektur wird empfohlen, den zentralen Protokollierungsserver in der Zone „Management-Netz“ zu betreiben.

4.1.7 Monitoring

Die folgenden Anforderungen werden an Produkte für das Monitoring gestellt:

- Das Produkt muss ein zentrales Management haben.
- Das Produkt muss alle eingesetzten Betriebssysteme unterstützen. Viele Betriebssysteme stellen hierzu bereits Schnittstellen zur Verfügung, die auf Standardprotokolle basieren (z. B. SNMP). Weitere Details sind unter Abschnitt 2.3.11 erläutert.
- Das Produkt muss die Konfiguration von Schwellwerten unterstützen (z. B. die Anzahl laufender Prozesse, Temperaturen, minimaler freier Speicherplatz des Datenspeichers, etc.).
- Das Produkt muss eine Alarmierung (E-Mail, SMS, Pager, etc.) unterstützen.

4.1.8 Integritätsprüfung

Die Integritätsprüfung muss für die Überwachung von Betriebssystem-relevanten Dateien genutzt werden, damit unerlaubte oder ungewollte Konfigurationsänderungen erkannt werden. An das Produkt werden die folgenden Anforderungen gestellt:

- Das Produkt muss die Überwachung der Integrität für die eingesetzten Betriebssysteme unterstützen.

- Die Überwachung der Integrität von Dateien muss anhand von Inhalt, Dateiattributen und Berechtigungen erfolgen. Der Inhalt von Dateien muss z. B. durch Prüfsummen mit Referenzwerten verglichen werden. Änderungen an Dateiattributen und Berechtigungen können auf einen Angriff hindeuten. Dies gilt sowohl für normale Dateien als auch für Treiber, Kernel-Module, Bibliotheken, etc. Werden Windows-Systeme eingesetzt, muss zusätzlich noch die Überwachung der Registry möglich sein.
- Die Integritätsprüfung muss über ein zentrales Management verfügen, an das Integritätsverletzungen gemeldet werden.
- Das Produkt muss Alarmierungen unterstützen.
- Bei der Aktualisierung von Betriebssystemen und den darauf betriebenen Diensten muss es möglich sein, die Referenzwerte neu zu generieren.
- Um spätere Analysen von Änderungen durchzuführen, müssen Ereignisse, die die Systemintegrität beeinflusst haben, protokolliert werden. Eine Analyse kann sinnvoll sein, um festzustellen, ob z. B. eine Änderung bewusst oder auch versehentlich durch einen Administrator durchgeführt wurde.

4.1.9 Datensicherung

Für die Datensicherung ist ein Konzept zu erstellen, welches die zu sichernden Systeme, den Umfang und die Art der Datensicherung festlegt (siehe auch Abschnitt 2.3.16). Die folgenden Anforderungen werden an Produkte zur Datensicherung gestellt:

- Das Produkt zur Datensicherung muss über ein zentrales Management verfügen.
- Das eingesetzte Produkt muss das Wiederherstellen der Daten ermöglichen.
- Die Datensicherung kann über das Produktionsnetz erfolgen. Bei zu hoher Auslastung des Produktionsnetzes wird ein separates Netz für die Datensicherung empfohlen.
- Das eingesetzte Produkt muss alle verwendeten Betriebssysteme unterstützen.

4.1.10 Patch- und Änderungsmanagement

Über das Patch- und Änderungsmanagement werden Sicherheitsupdates, Softwareaktualisierungen und neu zu installierende Software-Komponenten installiert. Die folgenden Anforderungen werden daran gestellt:

- Die Softwareverteilung muss die eingesetzten Betriebssysteme unterstützten.
- Das Einspielen von Software und Updates muss sowohl automatisiert als auch manuell erfolgen können.

4.1.11 Speichernetz

Für die Auswahl eines Speichernetzes müssen die folgenden Punkte berücksichtigt werden:

- Erfolgt der Zugriff auf das Speichernetz ausschließlich durch Nutzer (z. B. für den Zugriff und die Speicherung von Daten), sollte ein NAS eingesetzt werden. Ein Anwendungsbereich ist z. B. die Nutzung als FileServer.

- Erfolgt der Zugriff auf das Speichernetz ausschließlich durch Server (z. B. zur Nutzung einer einheitlichen Datenquelle, auf die mehrere Server zugreifen), dann sollte ein SAN verwendet werden. Ein Anwendungsbereich ist z. B. der Einsatz mit einem Cluster für Virtualisierung.

Bei der Auswahl des Massenspeicherprotokolls müssen die folgenden Punkte berücksichtigt werden:

- Das eingesetzte Massenspeicherprotokoll muss von den verwendeten Betriebssystemen unterstützt werden.
- Soll das Speichernetz die bisherige Infrastruktur mit nutzen, muss auf Kompatibilität des Massenspeicherprotokolls mit den bereitgestellten Komponenten geachtet werden. Meistens ist eine IP-basierte Infrastruktur (Ethernet) bereits vorhanden. Soll diese genutzt werden, dann kommen Protokolle, die auf IP basieren (wie z. B. Fibre-Channel), nicht infrage.
- Werden bei dem Einsatz eines SAN hohe Anforderungen an die Performance gestellt, dann empfiehlt sich der Einsatz von Fibre Channel. Als kostengünstigere Alternativen mit etwas geringerer Performance kann auch iSCSI oder FCoE eingesetzt werden.
- Bei dem eingesetzten Massenspeicherprotokoll ist auf Kompatibilität mit den verwendeten Netz-Komponenten zu achten:
  - Bei dem Einsatz von FCoE ist darauf zu achten, dass die verwendeten Switche Convergence Enhanced Ethernet (CEE) unterstützen (siehe Abschnitt 2.5.4.5).
  - Verwendet das Massenspeicherprotokoll Jumbo Frames (z. B. bei iSCSI oder FCoE), muss dies von den verwendeten Switchen, Routern, etc. unterstützt werden.
- Bei dem Einsatz von FCoE wird der Einsatz von dedizierten Converged Network Adaptern (CNA) empfohlen, um eine höhere Performance zu erzielen.
- Bei dem Einsatz von iSCSI wird der Einsatz von dedizierten Host-Bus-Adaptern (HBA) mit TCP Offload Engines (TOE) empfohlen, um eine höhere Performance zu erzielen.
- Werden dedizierte Netzwerkkarten (HBA oder CNA) eingesetzt, müssen diese von dem verwendeten Betriebssystem unterstützt werden.

4.1.12 Virenschutzprogramm

Das Virenschutzprogramm untersucht Dateien auf der Festplatte nach Schadprogrammen. Es muss die folgenden Anforderungen erfüllen:

- Das Virenschutzprogramm muss alle Betriebssysteme unterstützen, auf denen es eingesetzt werden soll.
- Das Virenschutzprogramm muss über ein zentrales Management verfügen.
- Das Virenschutzprogramm muss bei Verdacht auf Virenbefall eine Alarmierung durchführen können.
- Das Virenschutzprogramm muss Dateien sowohl beim lesenden als auch beim schreibenden Zugriff prüfen können (On Access Scanning).
- Es muss eine zeitgesteuerte oder manuell angeforderte Prüfung der gesamten Festplatte auf Schadprogramme unterstützen (On Demand Scanning).
- Es muss gängige Archivformate – auch verschachtelte – entpacken können, um den Inhalt auf Schadprogramme zu untersuchen.

- Es verwendet zur Erkennung von Schadprogrammen mindestens Signaturen und heuristische Verfahren.
- Es muss erkannte Schadprogramme in eine Quarantäne verschieben und infizierte Dateien, falls möglich, bereinigen können.
- Der Hersteller muss täglich aktualisierte Virensignaturen zur Verfügung stellen und auf neue Schädlinge zeitnah reagieren. Diese müssen automatisiert dem Virenschutzprogramm bereitgestellt werden.

4.1.13 Virtualisierung

Sollen unterschiedliche Betriebssysteme und Dienste auf dem Virtualisierungsserver bereitgestellt werden, empfiehlt sich der Einsatz einer hypervisorbasierten Technologie. Werden ausschließlich Dienste gleicher Art angeboten werden, sollte eine Betriebssystemvirtualisierung eingesetzt werden. Dabei muss berücksichtigt werden, dass bei der Betriebssystemvirtualisierung eine geringere Isolation und Kapselung des virtuellen IT-Systems gegeben ist (Details dazu sind in Abschnitt 2.3.5 beschrieben). Unabhängig von der eingesetzten Virtualisierungstechnologie müssen die folgenden Punkte berücksichtigt werden:

- Das eingesetzte Virtualisierungsprodukt muss die zu installierenden Gast-Betriebssysteme unterstützen.
- Das eingesetzte Produkt zur Virtualisierung muss über ein zentrales Management verfügen.
- Es muss möglich sein, ein Backup des virtualisierten Gastbetriebssystems durchzuführen.
- Die zu beschaffenden Hardware-Komponenten müssen ausreichend Kapazitäten hinsichtlich CPU-, RAM-, Netz- und Speichernetzressourcen haben. Die Herstellerangaben des eingesetzten Virtualisierungsproduktes sind hierbei zu berücksichtigen. Bei der Auswahl der Hardware ist auf Kompatibilität mit dem Virtualisierungsprodukt zu achten. Hierzu ist die Hardwarekompatibilitätsliste (engl. Hardware Compatibility List) des Herstellers zu überprüfen.
- Die eingesetzte Virtualisierungstechnologie muss eine ausreichende Kapselung und Isolation des Betriebssystems sicherstellen (siehe auch Abschnitt 3.5).

Redundante Komponenten

Innerhalb der Grundarchitektur wird der redundante Aufbau einer Virtualisierungsumgebung empfohlen, weil bei Ausfall des Virtualisierungsservers alle auf dem Virtualisierungsserver betriebenen IT-Systeme gleichzeitig nicht mehr verfügbar sind. Dies setzt den Einsatz eines Speichernetzes voraus. Bei der Auswahl der verwendeten Massenspeichertechnologie ist auf Kompatibilität mit dem eingesetzten Virtualisierungsprodukt zu achten (siehe auch Abschnitt 4.1.11). Durch den redundanten Aufbau der Virtualisierungsserver ist die Bildung eines Hochverfügbarkeitsclusters möglich. Fällt ein physischer Server aus, wird dies erkannt und die davon betroffenen virtuellen IT-Systeme auf einem der anderen physischen Server des Clusters neu gestartet.

4.2 Sichere Grundkonfiguration und Minimierung der Komponenten

Nachdem die Phase der Anforderungserhebung und Komponenten-Auswahl sowie Beschaffung beendet ist, erfolgt die Installation und sichere Grundkonfiguration des Servers.

4.2.1 Hardware, Firmware und externe Schnittstellen

Hardware

Bei dem Installationsort des Servers wird davon ausgegangen, dass sich dieser in einem zutrittsgeschützten Raum befindet. Nicht genutzte Hardware-Schnittstellen (z. B. USB, Firewire oder eSATA) sind daher nicht zwingend zu deaktivieren, da davon ausgegangen werden kann, dass nur autorisierte Personen diesen Raum betreten dürfen.

Firmware

Die Firmware des Servers und aller seiner Komponenten (BIOS, RAID-Controller, Festplatten, Host Bus Adapter, etc.) ist auf den aktuellen Stand zu bringen.

Externe Schnittstellen

Die zum Betrieb erforderlichen Peripheriegeräte, wie Tastatur, Maus, Monitor, etc. werden direkt per Kabel oder über einen KVM-Switch an den Server angeschlossenen.

Die Netzverbindungen können ebenfalls schon angeschlossen werden. Hierzu gehört die Verbindung zum Produktionsnetz, zu der Management-Zone, ggf. vorhandene Verbindungen zu einem Speichernetz und bei der Konfiguration eines Virtualisierungsservers auch die Verbindungen zu dem Netz für die Live Migration.

Hardware-Management

Schnittstellen z. B. für das Hardware-Management sind ebenfalls über die Management-Zone zu nutzen. Evtl. vorgegebene Standardpasswörter des Hardware-Herstellers für den Zugriff auf diese Schnittstellen sind durch sichere Passwörter zu ersetzen.

4.2.2 Konfiguration von RAID

Durch den Einsatz von RAID kann sowohl eine höhere Datensicherheit als auch eine höhere Performance beim Lesen und Schreiben von Daten erzielt werden. Die Konfiguration des RAID muss vor der Installation des Betriebssystems durchgeführt werden. Wird zu einem späteren Zeitpunkt eine RAID-Konfiguration der Festplatten durchgeführt, werden alle auf den Datenträgern vorhandenen Daten gelöscht.

4.2.3 Betriebssystem

Die Installation von Betriebssystem und Diensten muss nach dem Minimalprinzip erfolgen, um eine möglichst geringe Angriffsfläche zu bieten. In den folgenden Abschnitten werden die einzelnen Schritte der Installation und Konfiguration des Betriebssystems als Minimalsystem beschrieben.

4.2.3.1 Installation

Die Minimalinstallation des Betriebssystems darf nur die grundlegende Software und die Basisdienste umfassen, die benötigt werden, um ein lauffähiges System zu erhalten. Im Detail müssen die folgenden Punkte berücksichtigt werden:

- Unterstützt das Betriebssystem eine Minimalinstallation, dann muss diese ausgewählt werden. Alternativ kann eine benutzerdefinierte Installation durchgeführt werden, die es ermöglicht Komponenten während der Installation abzuwählen.
- Bei der Installation des Betriebssystems sind nur die für den Betrieb benötigten Komponenten auszuwählen.
- Nach einer Minimalinstallation sollten möglichst keine Netzdienste zur Verfügung gestellt werden. Als einzige Ausnahme kann hier ein Protokoll zur Administration genutzt werden (z. B. SSH oder RDP), da die Installation von Applikationen und Diensten in großen Institutionen häufig von unterschiedlichen Standorten erfolgt. Die weitere Installation von Diensten erfolgt in einem späteren Schritt.
- Um die Angriffsfläche zu minimieren, soll das Betriebssystem möglichst ohne graphische Oberfläche installiert werden. Durch das Installieren einer grafischen Oberfläche werden zusätzliche Bibliotheken und ggf. Dienste installiert, die bei Softwareschwachstellen für Angriffe ausgenutzt werden können. Auf eine grafische Oberfläche kann verzichtet werden, wenn die spätere Administration des Betriebssystems oder der darauf betriebenen Dienste diese nicht voraussetzen.

Automatische oder manuelle Installation

Die meisten Betriebssysteme bieten heutzutage die Möglichkeit einer automatischen Installation ohne Benutzerinteraktion an. Dies kann sowohl von separaten Installationsmedien (CD/DVD) oder auch über das Netz erfolgen. Hierbei wird anhand von vorher erstellten Profilen die Grundkonfiguration des Betriebssystems vorgegeben. Diese umfassen z. B.

- Netzkonfiguration
- Verzeichnisdienstanbindung
- Vorauswahl zu installierender Software-Komponenten.

Sollen viele Systeme mit demselben Betriebssystem installiert werden, dann wird die Erstellung eines Basisprofils für ein minimales Betriebssystem empfohlen, damit nicht bei jeder Installation eine manuelle Konfiguration notwendig ist.

Sollen nur einzelne wenige Systeme installiert werden, kann eine manuelle Installation durchgeführt werden. Die notwendigen Einstellungen müssen durch einen Benutzer konfiguriert werden.

4.2.3.2 Partitionieren und Formatieren der Festplatte

Bevor das Betriebssystem auf der Festplatte installiert wird, muss diese mittels Partitionierung und Formatierung mit einem Dateisystem vorbereitet werden. Diese Vorbereitungen werden üblicherweise am Anfang der Installation abgefragt.

Bei der Partitionierung der Festplatte wird der zur Verfügung stehende Speicherplatz in logische Einheiten (Partitionen) aufgeteilt. Abhängig von dem Betriebssystem können diesen Partitionen unterschiedliche Rechte und Eigenschaften zugewiesen werden (z. B. Partitionen, auf die nur lesend zugegriffen werden darf). Einige Betriebssysteme unterstützen die Installation unterschiedlicher Systemverzeichnisse auf separaten Partitionen. Dies ermöglicht es unterschiedliche Sicherheitseinstellungen für einzelne Partitionen vorzunehmen, die die Sicherheit des Systems erhöhen können. Für Unix-/Linux-basierende Betriebssysteme wird eine Separierung der Partitionen nach dem folgenden Schema empfohlen:

- Separate Partitionen für die Verzeichnisse Root („/“), /home, /tmp, /usr, /var, /opt und Swap.

Für Windows-basierende Betriebssysteme wird das folgende Vorgehen empfohlen:

- separate Partition für das Betriebssystem;
- separate Partition für Daten (z. B. die Daten eines zentralen DatenServers bzw. FileServers).

Nach der Partitionierung sind die neu erstellten Partitionen mit einem Journaling-Dateisystem zu formatieren. Falls nicht bekannt ist, ob das von dem Betriebssystem unterstützte Dateisystem diese Funktionalität bietet, dann muss die Herstellerdokumentation zur Hilfe herangezogen werden. Beispiele für solche Dateisysteme sind:

- ext3/ext4 für Linux
- XFS für Linux und IRIX
- JFS/JFS2 für Linux, AIX und OS/2
- NTFS für Microsoft Windows
- UFS für Solaris, AIX
- ZFS für Solaris
- ReiserFS für Linux

4.2.3.3 Netzkonfiguration

Bei der Netzkonfiguration besteht die Möglichkeit zwischen einer statischen und einer dynamischen Konfiguration des Netzzugangs.

Statische Konfiguration

Bei der statischen Konfiguration erfolgt die Vergabe von IP-Adresse, Netzmaske, Standard-Gateway und DNS-Server manuell. Dies erfolgt entweder während der Installation des Betriebssystems über entsprechende Eingabemasken oder später über ein Konfigurationsmenü oder Konfigurationsdateien.

Dynamische Konfiguration

Bei der dynamischen Konfiguration erfolgt die Vergabe von IP-Adresse, Netzmaske, Standard-Gateway, etc. automatisch über das Dynamic Host Configuration Protokoll (DHCP). Die Konfigurationsdaten des Netzes werden während der Installation oder beim Hochfahren des Systems von einem DHCP-Server abgefragt und auf dem Server hinterlegt. Dies ermöglicht eine zentrale Verwaltung der vergebenen IP-Adressen.

Üblicherweise erfolgt eine Neuvergabe der IP-Adresse, wenn das System längere Zeit nicht mehr im Netz war. Dies kann zur Folge haben, dass das System z. B. nach Wartungsarbeiten eine neue IP-Adresse zugewiesen bekommt. Bei Server-Systemen ist dieses Verhalten oft unerwünscht, da der Server seine Dienste immer unter derselben IP-Adresse zur Verfügung stellt, um eine höhere Verfügbarkeit zu erzielen. Um die Vergabe derselben IP-Adresse zu ermöglichen, besteht die Möglichkeit, auf dem DHCP-Server die MAC-Adresse (Media Access Control) der Netzwerkkarte zu hinterlegen, aufgrund der wieder dieselbe IP-Adresse zugewiesen wird.

Die statische Konfiguration wird im Rahmen dieser Studie für Server empfohlen. Welche Variante jedoch bei der Installation letztendlich eingesetzt wird, ist abhängig von den Anforderungen der jeweiligen Institution.

4.2.3.4 Deaktivieren von Netzprotokollen

Häufig werden bei der Installation eines Betriebssystems Protokolle installiert, die nicht für den Betrieb notwendig sind.

- Alle nicht benötigten Protokolle sind auf dem Server zu deaktivieren.

4.2.3.5 Sichere Konfiguration des Betriebssystems

Nach der Installation ist das Betriebssystem daraufhin zu überprüfen, ob für den späteren Betrieb nicht benötigte Komponenten installiert wurden (z. B. automatische Installation eines FTP-Dienstes, obwohl dieser nicht angeboten werden soll). Diese sind dann mit Betriebssystemmitteln zu deinstallieren. Hilfreich für die Identifizierung solcher Komponenten sind z. B.:

- Die Prozessliste. Diese kann z. B. unter Linux / Unix mit dem Kommando `ps` angezeigt werden. Unter Windows kann der Task-Manager genutzt werden.
- Die Anzeige der im Netz zur Verfügung gestellten Dienste. Unter Linux / Unix und Windows kann das Kommando `netstat` verwendet werden.
- Eine Übersicht über die installierten Programme. Dies erfolgt z. B. bei Linux / Unix mit dem verwendeten Paketmanager (RPM, DPKG, PKG, etc.) bzw. bei Windows unter „Programme und Funktionen“.

Da es oft Abhängigkeiten zwischen den installierten Programmen gibt, kann nicht jedes ohne Risiko entfernt werden. Daher müssen hierzu die einzelnen Komponenten auf Notwendigkeit und Abhängigkeiten analysiert werden, bevor diese entfernt werden. Bei einigen Linux Distributionen ist z. B. die Installation eines Mail Transport Agent (MTA) notwendig, da einige Dienste (z. B. cron) hierüber Statusmeldungen versenden. Eine Deinstallation des MTAs würde auch die davon abhängigen Komponenten entfernen. Kann das Deinstallieren nicht durchgeführt werden, müssen die nicht benötigten Komponenten deaktiviert werden oder so eingerichtet werden, dass diese Dienste nicht von extern genutzt werden können. Nachfolgend sollen hierzu weitere Hinweise aufgeführt werden:

- Einige Netzdienste werden nach der Installation nur lokal auf dem System benötigt und müssen nicht über das Netz bereitgestellt werden. Diese Dienste sind dahingehend zu konfigurieren, dass sie nur an das lokale Netzwerk-Interface (Loopback) gebunden werden. Diese Dienste können z. B. sein:
  - ein E-Mail-Server, der nur eine lokale Mailzustellung durchführt
  - ein NTP Server, der nur zur lokalen Zeitsynchronisation des Servers eingesetzt wird
  - ein DatenbankServer, der nur für lokale Applikationen zur Verfügung stehen muss.
- Dienste, die weder lokal benötigt werden, noch von dem Server angeboten werden sollen, müssen deaktiviert werden.
- Zur sicheren Konfiguration gehört die Härtung des Betriebssystems. Die Hersteller bieten in der Regel Härtungsrichtlinien (sog. Hardening Guides) für die Betriebssysteme an, in denen Hinweise zur Deaktivierung von Diensten oder sichere Standardeinstellungen beschrieben sind. Bei der Umsetzung dieser Richtlinien muss berücksichtigt werden, dass einige Einstellungen Einfluss auf andere Dienste oder Funktionen haben können, sodass ein korrektes Funktionieren des Gesamtsystems nach einer Härtung unbedingt geprüft werden muss.

Um eine sichere Konfiguration des Betriebssystems durchzuführen, sind unabhängig von den Härtungsrichtlinien der Betriebssystemhersteller die folgenden Maßnahmen durchzuführen:

- Schutzmechanismen des Betriebssystems, wie z. B. Speicherschutzmechanismen oder Speicherrandomisierung, werden aktiviert – nach Möglichkeit für alle Anwendungen.
- Evtl. vorhandene Standardpasswörter sind durch sichere Passwörter zu ersetzen.
- Das automatische Abspielen von Inhalten oder Starten von Programmen beim Einlegen eines Wechseldatenträgers (z. B. USB-Stick, USB-Festplatte, CD/DVD-ROM) ist zu deaktivieren.
- Für die Protokollierung ist eine korrekte Systemzeit notwendig. Die Systemzeit des Servers ist regelmäßig mit einer zentralen Zeitsynchronisationsquelle abzugleichen (z. B. mittels NTP).

4.2.4 Dienste

Nachdem die Installation und die sichere Grundkonfiguration des Betriebssystems abgeschlossen sind, kann der Server um die Funktionalität erweitert werden, die er eigentlich anbieten soll. Hierzu sind die Dienste zu installieren, die über das Netz zur Verfügung gestellt werden sollen. Für die Installation und Konfiguration der neuen Dienste sollen die folgenden Punkte berücksichtigt werden:

- Dienste sollen nur über jene Rechte verfügen, die für den Betrieb erforderlich sind (restriktive Rechtevergabe). Wenn möglich, sollten sie mit eingeschränkten (minimalen) Rechten eines Benutzers laufen.
- Der Betrieb eines Dienstes mit Administratorrechten ist möglichst zu vermeiden. Unter Unix/Linux Systemen benötigen z. B. einige Dienste nur beim Starten privilegierte Benutzerrechte, um wichtige Systemressourcen anzufordern, wie das Anlegen eines privilegierten Ports. Werden diese Rechte nicht mehr benötigt, dann kann der Dienst zu einem nicht privilegierten Benutzer wechseln.
- Die Ausgabe von Versionsinformationen der eingesetzten Software über die verwendeten Protokolle (SMTP, SSH, HTTP, etc.) soll nach Möglichkeit ausgeschaltet werden. Dies kann von Angreifern als Information für mögliche Schwachstellen verwendet werden.

- Konfigurationsdateien sind mit minimalen Schreib- und Leserechten zu versehen. Konfigurationseinstellungen, die vertrauliche Daten beinhalten, sollen nach Möglichkeit nicht im Klartext gespeichert werden (z. B. die Hinterlegung eines Passwortes). Ist die Verschlüsselung seitens der Applikation nicht möglich, dann soll die entsprechende Datei mit minimalen Leserechten für den zugehörigen Dienst ausgestattet sein.
- Werden für Applikationen Passwörter benötigt, so müssen diese gemäß existierenden Passwortrichtlinien vergeben werden.
- Lokale Netzdienste dürfen nur an das lokale Netzwerk-Interface (Loopback) gebunden werden.

4.2.5 Benutzerrechte, -verwaltung und -authentisierung

Der Server ist an eine zentrale Benutzerverwaltung anzubinden. Hierzu sind die jeweiligen Schnittstellen des Betriebssystems zu nutzen (z. B. LDAP, Active Directory). Alle Vorgaben bzgl. Passwortrichtlinien und Berechtigungen werden in der zentralen Benutzerverwaltung gepflegt. Für Benutzerkonten, die lokal angelegt werden (z. B. lokale Administrator-Konten), gelten dieselben Richtlinien. Im Detail sind dies folgende:

- Der Zugang zum Betriebssystem muss über eine personenbezogene Benutzerkennung (Benutzerkonto) erfolgen.
- Benutzerkonten ohne Passwort dürfen nicht zum Anmelden an das Betriebssystem genutzt werden können.
- Nur autorisierte Benutzer (z. B. Administratoren) dürfen Zugriff auf das Betriebssystem der Server haben.
- Das Passwort muss regelmäßig gewechselt werden.
- Das Passwort muss ausreichend komplex gewählt werden und muss aus einer Kombination von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.
- Möglichkeiten zur Erkennung von Trivialpasswörtern zur Abwehr von Wörterbuch-Angriffen müssen genutzt werden.
- Nach einer festgelegten Anzahl von fehlgeschlagenen Anmeldungen wird entweder das Benutzerkonto gesperrt oder die Anmeldung zunehmend verzögert, um automatisierten Angriffen entgegenzuwirken. Nur ein Administrator kann das Benutzerkonto dann wieder freischalten.
- Das Passwort darf nicht im Klartext abgelegt werden.
- Benutzern sind nur die Berechtigungen zuzuweisen, die für die Ausübung ihrer Aufgaben benötigt werden.

Benutzerkonten, die lokal angelegt werden, müssen regelmäßig daraufhin überprüft werden, ob sie noch verwendet werden (z. B. für Supportfälle, Administrator-Konten). Nach der Anbindung des Verzeichnisdienstes sind nicht benötigte lokale Benutzerkonten zu deaktivieren bzw. zu löschen. Die Benutzerauthentisierung am Server erfolgt mindestens durch Benutzername und Passwort, wobei die Benutzerinformationen von dem Verzeichnisdienst autorisiert werden. Bei höheren Sicherheitsanforderungen kann auch eine 2-Faktor-Authentisierung eingesetzt werden (siehe Variante 5.1.2.A).

Das Betriebssystem ist dahin gehend zu konfigurieren, dass eine lokale Anmeldung von Administratoren (z. B. bei dem Ausfall der zentralen Benutzerverwaltung) noch möglich ist.

Sind mehreren Benutzern dieselben Rechte zuzuteilen, dann soll eine rollenbasierte Rechtevergabe bevorzugt werden. Die Rechte werden einer Rolle bzw. Gruppe zugeordnet, der die entsprechenden Benutzer hinzugefügt werden (siehe auch Abschnitt 2.2).

4.2.6 Lokale Protokollierung

Die lokale Protokollierung des Betriebssystems ist dahin gehend zu konfigurieren, dass eine Weiterleitung von Ereignissen an die zentrale Protokollierung im Management-Netz erfolgt. Die Protokollierung ist so einzurichten, dass mindestens die folgenden Vorkommnisse protokolliert werden:

- Falsche Passworteingabe für ein Benutzerkonto bis hin zur Sperrung.
- Protokollierung des Benutzerkontos bei Erreichen der maximalen fehlgeschlagenen Authentisierungsversuche bei der Anmeldung.
- Versuche von unberechtigten Zugriffen (z. B. mittels unbekannten Kontonamen).
- Stromausfall (z. B. bei der Übernahme der Spannungsversorgung durch eine USV).
- Herunterfahren / Starten des Systems.

Die Protokolleinträge müssen mindestens einen Zeitstempel, den Namen des meldenden Servers, den Auslöser (z. B. ein Dienst, ein Prozess, eine Benutzerkennung oder eine andere Betriebssystem-Komponente) und eine Beschreibung des Ereignisses enthalten.

Für die zentrale Protokollierung sollte eine automatisierte Auswertung der Protokolle eingerichtet werden, die in Fehlerfällen (z. B. zu viele fehlerhafte Login-Versuche) eine Alarmierung durchführt.

4.2.7 Monitoring

Auf dem Betriebssystem sind Dienste zur Kommunikation mit dem zentralen Monitoring zu installieren und zu konfigurieren. Anschließend ist der Server in das zentrale Management des Monitorings einzubinden. Es sollen mindestens die folgenden Funktionen überwacht werden.

- Bei der Hardware:
  - Die Temperatursensoren (CPU, Gehäuse, etc.) sind bzgl. Überhitzung zu überwachen;
  - Die Funktionsweise der Hardware (Lüfter, Festplatten, Netzteile, etc.) ist zu überwachen;
- Bei dem Betriebssystem:
  - Der Speicherbedarf des Betriebssystems (Arbeitsspeicher, Festplattenspeicher, Größe der Auslagerungsdatei bzw. der Auslagerungspartition);
  - Die Netz- und CPU-Auslastung des Systems;
  - Die korrekte Funktion der zur Verfügung gestellten Dienste;
  - Die Anzahl laufender Prozesse und Dienste, die von dem Server angeboten werden;
  - Die korrekte Funktion der Zeitsynchronisation;
  - Die regelmäßige Durchführung der Datensicherung.

Des Weiteren ist eine Alarmierung einzurichten, die im Problemfall die entsprechenden Verantwortlichen (Administratoren, Applikationsverantwortliche, etc.) umgehend benachrichtigt. Solange das vorliegende Problem nicht bestätigt wurde, können periodisch (z. B. stündlich) weitere Alarmierungen erfolgen, damit dies nicht „unbeabsichtigt“ vergessen wird.

Bei der Konfiguration der Monitoring-Software sind entsprechende Schwellwerte zu konfigurieren, die beim Über- bzw. Unterschreiten einen Alarm auslösen. Die Schwellwerte sind abhängig von der Überwachungs-Komponente (z. B. Temperaturwerte, Anzahl laufender Prozesse, etc.) und sollten aus der Herstellerdokumentation von Hard- und Software-Komponenten bezogen werden.

Einige Protokolle, die für das Monitoring genutzt werden, bieten zusätzlich die Möglichkeit an, dass Konfigurationsdaten über dieselbe Schnittstelle geändert werden können (z. B. SNMP). Dies kann z. B. für Änderungen an Betriebssystemparametern genutzt werden. Ist kein schreibender Zugriff auf die Systemkonfiguration erwünscht, dann ist die Schnittstelle so zu konfigurieren, dass ausschließlich ein reiner Lesezugriff für das Monitoring zur Verfügung steht. Dies soll z. B. verhindern, dass Konfigurationsänderungen von unberechtigten Personen durchgeführt werden.

4.2.8 Integritätsprüfung

Dienste, die für die Integritätsprüfung des Betriebssystems und zur Kommunikation mit dem zentralen Management der Integritätsprüfung kommunizieren, sind auf dem Betriebssystem zu installieren und zu konfigurieren. Anschließend erfolgt die Anbindung des Server-Systems an das zentrale Management der Integritätsprüfung. Die Integritätsprüfung muss alle Betriebssystem-relevanten Daten überwachen, d. h. mindestens die folgenden:

- Die Integrität von Konfigurationseinträgen. Dies können gesamte Verzeichnisse (z. B. unter Linux / Unix unterhalb von /etc) oder auch Registrierungsschlüssel unter Windows sein. Eine Überwachung der folgenden Verzeichnisse wird mindestens empfohlen:
  - Für Linux / Unix Systeme: /etc; /usr/local/etc; /bin; /usr/bin; /usr/local/bin; /sbin; /usr/sbin; /usr/local/sbin; /lib;
  - Für Windows Systeme: %SystemRoot%\system32 inkl. der Unterverzeichnisse

  Die folgenden Registrierungsschlüssel sind unter Windows mindestens zu überwachen:
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Driver
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\
  - HKEY_LOCAL_MACHINE\Security

  Stellt der Hersteller spezielle Profile für Betriebssysteme zur Verfügung, dann sollen diese bevorzugt verwendet werden, da diese Profile auch sich häufig ändernde Dateien bzw. Registrierungsschlüssel berücksichtigen und diese von der Integritätsprüfung ausschließen. Auf diese Weise wird False Positive-Meldungen vorgebeugt.
- Die Berechtigungen von Konfigurationseinträgen müssen überwacht werden. Hierzu gehören sowohl die Eigentümer- bzw. Gruppenrechte als auch die Dateiattribute (z. B. schreibgeschützt oder ausführbar).

- Eine zeitnahe Überwachung und Alarmierung muss aktiviert werden. Eine Alarmierung hat zu erfolgen, wenn eine Verletzung der Integrität (z. B. durch Änderung einer Datei oder der Berechtigungen) erfolgt.

4.2.9 Datensicherung

Es sind die Komponenten zu installieren, die für die Datensicherung auf dem Server benötigt werden. Die Anbindung des Systems erfolgt über das zentrale Management der Datensicherung. Die Datensicherung ist entsprechend dem Datensicherungskonzept zu konfigurieren. Empfohlen wird eine Volldatensicherung mit inkrementeller Datensicherung des gesamten Systems. Die Volldatensicherung kann hierbei z. B. 14-tägig durchgeführt werden. Aufbauend darauf wird eine tägliche inkrementelle Datensicherung durchgeführt. Letztendlich ist das Intervall aber von den Gegebenheiten der Institution abhängig und wird im Datensicherungskonzept festgelegt.

4.2.10 Integration des Betriebssystems in ein Patch- und Änderungsmanagement

Um eine Aktualisierung von Software-Komponenten und Betriebssystem zu ermöglichen und um kurzfristig von Herstellern veröffentlichte Sicherheitsupdates einspielen zu können, ist es erforderlich, den Server in ein Patch- und Änderungsmanagement einzubinden. Hierzu gehört auch die Anbindung an eine Softwareverteilung. Je nach verwendetem Betriebssystem wurde dies evtl. schon während der Installation des Betriebssystems durchgeführt.

Einspielen von Updates und Patches

Ein Betriebssystem, das von dedizierten Installationsmedien oder vorgefertigten Installations-Images installiert wurde, umfasst in der Regel keine aktuellen Sicherheitspatches oder aktuelle Service-Packs. Diese enthalten häufig Korrekturen des Betriebssystems und der Dienste bzgl. Stabilität oder auch neue Funktionalitäten und müssen nach einer Minimalinstallation noch separat installiert werden. Die Installation von Service-Packs und Sicherheitspatches sollte vor der weiteren Minimalisierung und Härtung des Betriebssystems erfolgen, da diese u. U. auch neue Dienste oder Funktionalitäten installieren, die im späteren Betrieb nicht benötigt werden.

4.2.11 Anbindung des Speichernetzes

Die Anbindung eines Speichernetzes (z. B. mittels Fibre Channel oder iSCSI) ist abhängig von den später betriebenen Diensten und Anwendungen und kann daher optional installiert werden. Hierbei sind die folgenden Punkte zu berücksichtigen:

- Wird ein separates Speichernetz verwendet, ist dies über dedizierte physische Schnittstellen anzubinden.
- Das Betriebssystem ist für eine entsprechende Anbindung des Speichernetzes zu konfigurieren. Abhängig von dem eingesetzten Speichernetz gehören hierzu:
  - herstellen der Verbindung zu dem Speichernetz mittels Hostname oder IP-Adresse
  - einbinden des Speichernetzes über den Freigabenamen, Netzwerkpfad. etc.

- Erfolgt die Anbindung an ein Speichernetz, müssen die jeweiligen Speicherprotokolle konfiguriert werden. Im Detail sind dies die folgenden:
  - Konfigurationseinstellungen für iSCSI:
    - IP-Adresse, Port und IQN des iSCSI-Massenspeichers
    - LUN des zu verwendenden Datenspeichers.
  - Konfigurationseinstellungen für Fibre Channel:
    - WWN bzw. WWNN und WWPN des Fibre Channel-Massenspeichers
    - LUN des zu verwendenden Datenspeichers.

4.2.12 Virenschutzprogramm

Komponenten, die für den Virenschutz auf dem Server benötigt werden, sind optional zu installieren. Anschließend ist der Server an die zentrale Management-Konsole des Virenschutzprogramms anzubinden. Die Konfiguration des Virenschutzprogramms erfolgt in der Regel über die zentrale Management-Konsole. Das Virenschutzprogramm ist so zu konfigurieren, dass es

- gefundene Schadprogramme und den Status über die Aktualisierung der Virensignaturen an das zentrale Managementsystem meldet
- infizierte Dateien unter Quarantäne stellt oder bereinigt
- sämtliche Dateien beim Lesen und Schreiben auf Schadprogramme prüft („On Access Scanning“)
- Dateien auf lokal eingebundene Datenträger (lokale Festplatte, CD/DVD-ROM, über USB angebundene Speichermedien) untersucht.

In regelmäßigen Abständen, mindestens jedoch einmal pro Woche, müssen alle lokalen Datenträger auf Schadprogramme untersucht werden („On Demand Scanning“).Das zentrale Management ist so zu konfigurieren, dass eine Benachrichtigung der Administratoren, Applikationsverantwortlichen, etc. erfolgt, sobald Viren erkannt werden.

Nach der Installation und Konfiguration des Virenschutzprogramms erfolgt das Herunterladen der aktuellen Virensignaturen. Diese sollen zentral bereitgestellt werden, sodass nicht jede einzelne Installation die Virensignaturen bei dem Hersteller abholt.

4.2.13 Virtualisierung

Abhängig von dem eingesetzten Virtualisierungsprodukt bringt dieses entweder ein eigenes Betriebssystem mit oder wird als Applikation auf ein bestehendes Betriebssystem installiert. Wird eine Virtualisierungssoftware auf dem Server installiert, müssen auch alle Anforderungen aus der Grundarchitektur (Minimalinstallation, Anbindung an eine zentrale Benutzerverwaltung, etc.) für dieses Produkt umgesetzt werden. Nach der Installation ist das Virtualisierungsprodukt in das zentrale Management zur Virtualisierung einzubinden. Des Weiteren sind die folgenden Punkte zu berücksichtigen:

- Das Einbinden des gemeinsam genutzten Speichernetzes. Abhängig vom verwendeten Massenspeicherprotokoll müssen folgende Einstellungen vorgenommen werden:
  - die Konfiguration des Servers, der das Speichernetz bereitstellt

  - die Konfiguration von WWN (bei Fibre-Channel) oder IQN (bei iSCSI)
  - die Konfiguration für den Pfad der Dateifreigabe (bei CIFS und NFS)
  - die Konfiguration von separaten LUNs bei dem Einsatz eines SAN
  - die Konfiguration von LUN Masking (iSCSI und Fibre-Channel) oder SAN Zoning (Fibre-Channel) bei dem Einsatz eines SAN
  - und evtl. die Konfiguration von Authentisierungsprotokollen.
- Das Einbinden des Massenspeichers muss redundant erfolgen (Einsatz von Multipathing).
- Der Virtualisierungsserver ist an das zentrale Monitoring anzubinden.
- Das Host-Betriebssystem des Virtualisierungsproduktes ist nach Abschnitt 4.2.3.5 und Abschnitt 4.2.4 zu konfigurieren. Bieten die Hersteller des Virtualisierungsproduktes Härtungsrichtlinien für das Produkt an, dann sind diese ebenfalls umzusetzen.
- Bei der Vergabe von Berechtigungen müssen die Administratoren des Virtualisierungsproduktes und die Administratoren der Betriebssysteme unterschieden werden. Die Administratoren des virtuellen IT-Systems dürfen nicht die Möglichkeit haben, Konfigurationen an dem Virtualisierungsprodukt vorzunehmen. Dies gilt ebenfalls in umgekehrter Richtung und muss durch entsprechende Rollen oder Gruppenrechte in der Benutzerverwaltung sichergestellt werden.
- Nur Komponenten im internen Netz aus demselben Netzsegment sollten innerhalb der Grundarchitektur auf einem Virtualisierungsserver zusammengelegt werden. Mit Netzsegment ist in der Grundarchitektur der Bereich gemeint, der von zwei Sicherheits-Gateways getrennt wird. Als Variante wird die Virtualisierung von Komponenten aus unterschiedlichen Netzsegmenten beschrieben (siehe Variante 5.2.2.A).
- Systeme aus unterschiedlichen Schutzzonen (Internet-Verbindung, Sicherheits-Gateway und Internes-Netz) dürfen nicht zusammen auf einem Virtualisierungs-Server virtualisiert werden.
- Es dürfen nur Server mit normalem Schutzbedarf auf demselben Virtualisierungsserver betrieben werden. Für Server mit hohem Schutzbedarf siehe Variante 5.2.2.B.

Die folgenden Netze müssen für den Virtualisierungsserver konfiguriert werden:

- Ein Netz zur Administration des Virtualisierungsservers: Hierüber wird die Konfiguration und Wartung des Virtualisierungsservers durchgeführt. Dies kann über das bereits vorhandene Netz zur Überwachung und Administration erfolgen.
- Ein Netz für das Speichernetz: Hierüber erfolgt der Zugriff auf die gespeicherten virtualisierten Betriebssysteme. Abhängig von der Anzahl der betriebenen virtualisierten Betriebssysteme werden über dieses Netz sehr große Datenmengen transferiert (z. B. bei dem Start eines Betriebssystems). Um das Produktionsnetz nicht zu belasten, sollte das Speichernetz über ein separates Netz angebunden werden.
- Ein Netz zur Live Migration: Hierüber werden die Daten transferiert, die für die Live Migration zwischen den Virtualisierungsservern ausgetauscht werden (z. B. zu Wartungszwecken oder sollte der Server ausfallen). Über dieses Netz können ebenfalls sehr große Datenmengen transferiert werden, daher wird die Separierung in ein eigenes Netz empfohlen.
- Das Produktionsnetz: In diesem Netz stellen die virtuellen IT-Systeme die installierten Dienste zur Verfügung.

- Es sind die Härtungsrichtlinien (Hardening Guides) der Hersteller der Virtualisierungsumgebungen anzuwenden.

4.3 Grundvorgaben für einen sicheren Betrieb

Nach der Installation und Konfiguration des Betriebssystems und den darauf zur Verfügung gestellten Diensten kann der Server in den Betrieb übergehen. Hierfür gilt, dass nur die Server in die Produktivumgebung eingebunden werden dürfen, die nach Abschnitt 4.2 konfiguriert wurden. Im Betrieb muss die Sicherheit des Systems weiterhin gewährleistet sein. Die hierfür benötigten Punkte sind in den nachfolgenden Abschnitten beschrieben.

4.3.1 Organisatorische Aspekte

Organisatorische Aspekte umfassen allgemeine Aufgaben, die nichts mit technischen Aspekten, wie z. B. die Installation oder Konfiguration des Servers zu tun haben. Die nachfolgenden Abschnitte sollen einige dieser Punkte aufführen.

Schulung von Administratoren

Die Administratoren sollten regelmäßige geschult werden. Folgende Inhalte sind zu behandeln:

- Schulungen zu den eingesetzten Technologien (Betriebssystemen, eingesetzte Software, Hardware, Massenspeicher, Virtualisierungsprodukt, etc.), um über die Entwicklungen der Betriebssysteme und deren Sicherheitsvorkehrungen auf dem aktuellsten Stand zu sein. Für viele Systeme gibt es auch dedizierte Sicherheitsschulungen, welche die bereits erwähnte Härtung u. ä. Themen vermitteln.
- Schulungen, die das Sicherheitsbewusstsein (engl. Security Awareness) stärken. Hier sollen die Sicherheitsrichtlinien des Unternehmens (der sichere Umgang mit Passwörtern, etc.) vermittelt werden.
- Organisatorische Abläufe bei Sicherheitsvorfällen oder Verdachtsmomenten.

Durch die Schulungen wird bei den Administratoren ein Bewusstsein für IT-Sicherheit geschaffen und dadurch das Risiko von fahrlässigem Informationsabfluss, Verlust der Vertraulichkeit usw. reduziert.

Notfallvorsorgekonzept

Beim Eintreten eines Sicherheitsvorfalls müssen technische und organisatorische Maßnahmen zur Erstreaktion und weiteren Vorgehensweise beschrieben sein. Dies erfordert zunächst eine Anlaufstelle, die für die IT-Sicherheit der Institution verantwortlich ist (z. B. ein IT-Sicherheitsbeauftragter) und bei einem Sicherheitsvorfall zu informieren ist. Die Vorgehensweise bei einem Sicherheitsvorfall, Ansprechpartner, die informiert werden müssen usw., müssen in einem Notfallplan beschrieben sein. Dieser ist zu erstellen, regelmäßig zu proben und auf Aktualität zu überprüfen.

4.3.2 Hardware und Firmware

Hersteller von Hardware bringen regelmäßig aktualisierte Firmware heraus, die Sicherheitslücken und evtl. vorhandene Fehler korrigiert. Es ist regelmäßig zu überprüfen, ob eine neue Version der jeweils eingesetzten Firmware vorhanden ist. Wird die Firmware über einen längeren Zeitraum nicht überprüft und aktuell gehalten, dann erhöht sich das Risiko von Sicherheitslücken und Fehlfunktionen.

Im laufenden Betrieb kann es auch vorkommen, das Teile der Hardware aufgrund eines Defektes ausfallen. Dieser Ausfall sollte vom Monitoring erkannt und gemeldet werden. Die defekten Komponenten sind zeitnah auszutauschen, um den Betrieb aufrecht zu erhalten. Fallen Festplatten innerhalb der Garantiezeit aus, dann können diese zum Austausch zu dem Hersteller zurückgeschickt werden. Hierbei ist darauf zu achten, dass alle auf dem Datenträger vorhandenen Daten vor dem Versenden gelöscht werden.

4.3.3 Betriebssystem und Dienste

Das Betriebssystem und die darauf installierten Dienste sind regelmäßig zu aktualisieren und Sicherheitspatches sind einzuspielen. Die Hersteller bieten hierfür z. B. Mailinglisten an, die über Sicherheitslücken und Aktualisierungen ihrer Produkte informieren. Zusätzlich gibt es im Internet noch dedizierte Anbieter, die herstellerunabhängig über neue Schwachstellen informieren (z. B. CERT, Heise, Secunia, etc.).

Aktualisierte Softwareversionen (Patches, Updates, etc.) müssen vor der Installation auf Produktionsservern auf identischen oder ähnlich konfigurierten TestServern getestet werden. Dies ist erforderlich, um die Kompatibilität der neuen Softwareversion mit dem Betriebssystem und den bestehenden Diensten sicherzustellen. Treten dort Probleme auf, können diese weiter analysiert werden, ohne den Betrieb zu beeinträchtigen. Das Einspielen von neuen Softwareversionen auf Produktivsystemen muss sorgfältig geplant werden, da angebotene Dienste unter Umständen für den Zeitpunkt der Aktualisierung nicht zur Verfügung stehen. Anwender, Kunden, usw. müssen ggf. vorher rechtzeitig über Einschränkungen informiert werden.

Die auf dem Server zur Verfügung gestellten Dienste sind regelmäßig daraufhin zu überprüfen, ob diese noch genutzt bzw. noch benötigt werden. Besteht kein Bedarf mehr an den installierten Diensten, dann müssen diese deaktiviert oder deinstalliert werden, um möglichen Schwachstellen vorzubeugen.

Die Softwareverwaltung bzw. Paketverwaltung des Betriebssystems ist ebenfalls einer regelmäßigen Kontrolle bzgl. noch benötigter oder veralteter Pakete hin zu überprüfen. Einige Betriebssysteme bieten hierzu gesonderte Programme an, die „verwaiste“ Pakete oder Software aufspüren und bei der Bereinigung des Systems unterstützen (z. B. bei Debian GNU/Linux die Pakete debfoster oder deborphan).

4.3.4 Benutzerrechte, -verwaltung und -authentisierung

Bei der zentralen Benutzerverwaltung müssen im Betrieb die folgenden Punkte berücksichtigt werden:

- Die Benutzerverwaltung muss stets auf dem aktuellen Stand sein. Gerade bei Versetzungen von Mitarbeitern innerhalb des Unternehmens (z. B. in andere Abteilungen) behält der Mitarbeiter häufig die alten Berechtigungen, obwohl diese ggf. nicht mehr benötigt werden. Hierbei gilt es

die Berechtigungen, Gruppenzugehörigkeiten, etc. nach Rücksprache mit den Vorgesetzten und verantwortlichen Abteilungen anzupassen. Es ist ein entsprechender Prozess zu etablieren, der dies berücksichtigt.

- Neue Benutzer müssen bei Neueinstellung in der Benutzerverwaltung angelegt werden. Vorgaben wie z. B. Berechtigungen und Gruppenzugehörigkeit sind mit den Vorgesetzten und verantwortlichen Abteilungen (z. B. Personalabteilung) abzustimmen.
- Verlassen Mitarbeiter das Unternehmen, sind die Benutzerkonten zu löschen. Hierbei ist darauf zu achten, dass möglicherweise noch vorhandene Daten des Mitarbeiters zuvor archiviert werden. Bei einer längeren Abwesenheit eines Mitarbeiters (z. B. durch Elternzeit) wird eine Deaktivierung empfohlen. Nach der Rückkehr kann das Benutzerkonto wieder aktiviert werden.
- Es ist eine regelmäßige Kontrolle der von der Benutzerverwaltung protokollierten, fehlgeschlagenen Authentisierungsversuche durch einen Administrator erforderlich.
- Um den Betrieb der Systeme sicherzustellen, sind die administrativen Zugangskonten (Benutzernamen und Passwort) gesichert zu hinterlegen (z. B. in einem verschlossenen Briefumschlag in einem Tresor). Dies soll sicherstellen, dass eine Vertretung auf die Systeme zugreifen kann, wenn der Administrator nicht da ist (z. B. aufgrund einer Erkrankung).

4.3.5 Protokollierung

Alle Ereignisse der Server werden auf dem zentralen Logging-Server im Management-Netz protokolliert. Die regelmäßige Auswertung der Protokollmeldungen muss automatisiert erfolgen, da aufgrund des Log-Aufkommens im Produktionsbetrieb eine manuelle Auswertung nicht durchgeführt werden kann. Dies kann z. B. durch eigene Skripte oder durch separate Software erfolgen. Bei der Auswertung der Daten sollen die folgenden Punkte berücksichtigt werden:

- Die Protokolldateien sind täglich auf mögliche Angriffsmuster hin zu überprüfen. Eine Anhäufung fehlerhafter Anmeldeversuche kann z. B. auf einen Angriff hindeuten.
- Die Protokolldateien sind nach dem Neustart von Prozessen oder des gesamten Server-Systems zu prüfen, um Fehler zu ermitteln. Häufig fallen z. B. (versehentliche) Konfigurationsänderungen erst auf, wenn Dienste oder das Betriebssystem neu gestartet werden. Bei fehlerhaften Einträgen in einer Konfigurationsdatei eines Dienstes kann dies die Folge haben, dass dieser nicht mehr startet oder mit falschen Parametern gestartet wird.
- Unabhängig vom Inhalt und von der protokollierenden Komponente sind die Meldungen auf dem Logging-Server und den zentralen Managementsystemen unter Berücksichtigung der gesetzlichen Bestimmungen, insbesondere zum Datenschutz, aufzubewahren.

4.3.6 Monitoring

Das Monitoring laufender Systeme ist einer der wichtigsten Punkte im Betrieb, da defekte Hardware und Fehlfunktionen von Software schnell erkannt und behoben werden müssen, um die Auswirkungen der Probleme, die durch die Nichtverfügbarkeit von Diensten verursacht werden, gering zu halten. Um dies sicherzustellen, sind die folgenden Punkte zu berücksichtigen:

- Die Auslastung der Systeme und deren Verfügbarkeit sind ständig zu überwachen. Das Monitoring muss sowohl das Betriebssystem, die darauf laufenden Dienste und die Server-Hardware berücksichtigen.

- Neu installierte Dienste oder Hardware müssen dem Monitoring hinzugefügt werden. Deaktivierte oder deinstallierte Dienste müssen aus dem Monitoring wieder herausgenommen werden.
- Bei Beeinträchtigung der Verfügbarkeit des Systems muss eine automatisierte Benachrichtigung der Administratoren bzw. der verantwortlichen Personen erfolgen, um entsprechende Gegenmaßnahmen einzuleiten (Ersatzbeschaffung, Austausch von defekten Teilen, etc.).
- Es ist ein fortlaufendes Monitoring der Speicherkapazität des Massenspeichers durchzuführen, damit frühzeitig Maßnahmen ergriffen werden können, wenn nicht genügend Speicherplatz zur Verfügung steht.

4.3.7 Integritätsprüfung

Bei Aktualisierungen oder bei der Installation neuer Software-Komponenten ist darauf zu achten, dass auch die Referenzdaten für die Integritätsprüfung aktualisiert werden, damit hinzugefügte Dienste oder geänderte Konfigurationsdateien nicht als Fehler gemeldet werden.

Werden geplante Konfigurationsänderungen oder Installationen neuer Software (auch über die Softwareaktualisierung) auf dem Server durchgeführt, sollten die Integritätsüberprüfungen für diesen Server für den Zeitpunkt der Änderungen deaktiviert werden, damit keine falsche Alarmierung ausgelöst wird. Einige Produkte bieten die Möglichkeit, das Programm zur Integritätsprüfung in einen Wartungsmodus zu versetzen. Nach Abschluss der Arbeiten müssen die durchgeführten Änderungen wieder durch ein erneutes Überprüfen des Systems durch die Integritätsprüfung zu den Referenzdaten hinzugefügt und die kontinuierliche Überwachung des Servers wieder aktiviert werden.

Wird eine Kompromittierung der Integrität erkannt, hat eine zeitnahe Alarmierung der verantwortlichen Personen (Administrator, Applikationsverantwortliche, etc.) zu erfolgen.

4.3.8 Datensicherung

Um dem Ausfall eines Servers und einem möglichen Datenverlust vorzubeugen, sind bei der Datensicherung die nachfolgenden Punkte zu berücksichtigen.

- Es muss stets eine ausreichende Zahl leerer Archivmedien vorhanden sein. Um die Integrität der Daten auf den Archivmedien sicherzustellen, sind die klimatischen und physischen Lagerbedingungen einzuhalten.
- Die Wiederherstellung eines Datenbestands aus einer Datensicherung ist in regelmäßigen Abständen auf Testsystemen durchzuführen.

Das Datensicherungskonzept ist stets aktuell zu halten. Hierbei muss Folgendes berücksichtigt werden:

- Für neu installierte Systeme ist zu prüfen, ob eine Datensicherung notwendig ist. Ist dies der Fall, sind die hinzugefügten Systeme in die Datensicherung miteinzubeziehen. Die Art der Datensicherung und der Umfang der zu sichernden Daten sind festzulegen.
- Sollten sich im laufenden Betrieb die Anforderungen an Häufigkeit, Art und Umfang der Datensicherung ändern, dann ist dies entsprechend zu dokumentieren und in der Datensicherung zu berücksichtigen.

- Systeme, die außer Betrieb genommen werden, sind aus der fortwährenden Datensicherung zu entfernen. Die bisher gesicherten Daten sind jedoch (abhängig von den betrieblichen Anforderungen) weiterhin aufzubewahren.
- Die Aufbewahrungsdauer der Datensicherung wird teilweise durch gesetzliche Anforderungen vorgegeben (z. B. Datenschutz, Handelsgesetzbuch, etc.) sofern nicht betriebliche Aspekte für eine längere Speicherung der Daten sprechen, sind die Daten nach dem Ablauf der jeweiligen Fristen zu löschen.

4.3.9 Virtualisierung

Für den Betrieb eines Virtualisierungsservers sind die folgenden Punkte zu berücksichtigen:

- Die von dem Virtualisierungsserver zur Verfügung gestellten Ressourcen (Massenspeicher, Arbeitsspeicher, CPU, Festplattenspeicher, etc.) sind fortwährend zu überwachen, um Hardware-Engpässe frühzeitig zu erkennen. Werden Engpässe erkannt, ist die verwendete Hardware frühzeitig zu erweitern.
- Es ist zu prüfen, ob die virtuellen Maschinen noch verwendet bzw. benötigt werden, um den „Wildwuchs“ von virtuellen Maschinen zu verhindern.
- Falls virtuelle Maschinen nur für einen festgelegten Zeitraum benötigt werden, sind diese nach Ablauf dieser Zeit wieder zu löschen.
- Die Installation neuer virtualisierter Betriebssysteme hat nach den Vorgaben aus Abschnitt 4.2 zu erfolgen. Die Absicherung der Gastbetriebssysteme (sichere Konfiguration des Betriebssystems, Dienste, Umsetzen von Härtungsrichtlinien, etc.) ist genauso wie bei physischen Systemen vorzunehmen. Hieraus lassen sich Vorlagen erstellen, die für die Installation von weiteren Instanzen desselben Betriebssystems genutzt werden können. Immer wiederkehrende Arbeitsschritte lassen sich so minimieren.
- Bei der Installation der Gastwerkzeuge im virtuellen IT-System dürfen nur benötigte Schnittstellen aktiviert werden. Schnittstellen zur Kommunikation der virtuellen IT-Systeme untereinander sind zu deaktivieren. Ebenso sind Schnittstellen, die zum Ausführen von Skripten genutzt werden können, zu deaktivieren. Die Kommunikation zwischen dem Host-System und den virtuellen IT-Systemen ist auf das Nötigste einzuschränken, um möglichen Schwachstellen und Angriffen vorzubeugen.
- Den virtuellen Betriebssystemen sind nur die Geräte (Netzwerkkarte, Festplatte, Arbeitsspeicher, etc.) zuzuteilen, die sie für den Betrieb benötigen. Nicht benötigte Geräte der virtuellen Maschine sind zu deaktivieren (z. B. USB-Schnittstellen).
- Falls die Funktionalität Snapshots zu erstellen nicht benötigt wird, ist sie zu deaktivieren.

4.3.10 Virenschutzprogramm

Für das Virenschutzprogramm sind im Betrieb die folgenden Punkte zu berücksichtigen:

- Auf dem Server ist täglich zu prüfen, ob die Signaturen des Virenschutzprogramms aktualisiert werden. Dies kann z. B. über das zentrale Management des Virenschutzprogramms erfolgen. Da die Virensignaturen zentral bereitgestellt werden, ist ggf. bei fehlgeschlagener Aktualisierung zu überprüfen, ob das Verteilen der Signaturen korrekt funktioniert.

- Es besteht die Möglichkeit, dass der Server virenbefallene Dateien enthält, die von älteren Virensignaturen noch nicht erkannt wurden. Um diese Viren ebenfalls aufzuspüren, ist ein regelmäßiger „On Demand Scan“ (abhängig von den Daten der Institution) auf dem Server auszuführen.

4.4 Außerbetriebnahme

Die Außerbetriebnahme von Server-Systemen kann aus unterschiedlichen Gründen erfolgen. Dies kann z. B. der Ablauf von Mietverträgen für die Hardware sein, ein irreparabler Schaden an der Hardware oder auch, wenn der zur Verfügung gestellte Dienst des Servers nicht mehr benötigt wird. Bei der Entsorgung bzw. Außerbetriebnahme eines Servers sind die folgenden Punkte zu berücksichtigen:

- Bei der Außerbetriebnahme von Servern sind die Daten auf den enthaltenen Festplatten zu löschen.
- Frei gewordene Lizenzen von Betriebssystem und der installierten Software können in den Pool freier Lizenzen der Institution übertragen werden.
- Werden die Supportverträge für Hardware und Software nicht mehr benötigt, können diese gekündigt werden.
- Der außer Betrieb genommene Server ist aus dem zentralen Management der Sicherheits-Komponenten zu löschen. Berücksichtigt werden müssen hierbei die folgenden Produkte:
  - Management für den Integritätsschutz
  - Management für den Virenschutz
  - Protokollierungsserver
  - Monitoring
  - Datensicherung
  - Softwareverteilung bzw. Patch- und Änderungsmanagement.

5 Gefährdungen und Empfehlungen mit Varianten für den normalen und hohen Schutzbedarf

In Abschnitt 3 wurde eine sichere Grundarchitektur für den normalen Schutzbedarf vorgestellt und in Abschnitt 4 die sichere Auswahl und Konfiguration von Komponenten sowie deren Betrieb beschrieben. Der nachfolgende Abschnitt zeigt die Gefährdungen, denen ein Server ausgesetzt ist, und erläutert, wie die Maßnahmen der letzten beiden Abschnitte gegen diese Gefährdungen schützen. Des Weiteren werden Varianten für den normalen und hohen Schutzbedarf vorgestellt, die Teile der Grundarchitektur ergänzen oder ersetzen.

Die Gefährdungen werden den drei Grundwerten Vertraulichkeit (Abschnitt 5.2), Integrität (Abschnitt 5.3) und Verfügbarkeit (Abschnitt 5.4) zugeordnet. Abschnitt 5.1 enthält die Gefährdungen, die sich durch Eindringen oder Übernehmen des Servers ergeben. Bei diesen Gefährdungen sind typischerweise alle drei Grundwerte bedroht. In der Beschreibung jeder Gefährdung wird erläutert, was die relevanten Schwachstellen sind. Weiterhin werden die Maßnahmen aus den Abschnitten 3 und 4 aufgezeigt, die der Gefährdung entgegenwirken. Abschließend erfolgt die Beschreibung der Restrisiken für den Server, die nach der Umsetzung der Schutzmaßnahmen verbleiben.

Den Gefährdungen werden zusätzlich noch Varianten der Grundarchitektur zugeordnet. Einige dieser Varianten reduzieren das Restrisiko der entsprechenden Gefährdung. Andere Varianten können einfacher umgesetzt werden oder führen zu geringeren Kosten, können jedoch die Sicherheit eines Servers beeinträchtigen. In allen Varianten wird das Restrisiko nach der Umsetzung betrachtet. Dazu werden Schwachstellen aufgeführt, die nach Durchführung der Schutzmaßnahme verbleiben oder neue Schwachstellen aufgeführt, die durch die Schutzmaßnahme zusätzlich zu beachten sind.

Zur einfacheren Orientierung werden im Folgenden unterschiedliche Formatierungen für Gefährdungen und Varianten verwendet:

Gefährdung

Variante für den normalen Schutzbedarf

Variante für den hohen Schutzbedarf

5.1 Gefährdungen durch Eindringen und Übernehmen

Die Gefährdungen durch Eindringen und Übernehmen zielen darauf ab, sich unberechtigten Zugriff zu Server-Systemen zu verschaffen. Ziel eines Angreifer ist es, die Kontrolle über den Server zu erlangen. Dies gefährdet die drei Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität der Betriebssysteme und die darauf enthaltenen Daten.

5.1.1 Ausnutzen von Schwachstellen in Diensten

Bedrohung: Unautorisiertes Ausführen von Programmen

Erlangen von Konsolenzugriff durch Speicherfehler

Zugriff auf Schnittstellen nicht genutzter Dienste

	Kompromittierung eines Servers durch Ausnutzen von Sicherheitslücken
Schwachstelle:	Programmierfehler in Diensten
	Es werden Dienste auf dem Server betrieben, die nicht genutzt werden
	Auf Systemen wird Software eingesetzt, die Sicherheitslücken enthält
	Sicherheits-Updates werden nicht rechtzeitig installiert

Dienste werden von Servern sowohl über das lokale Netz als auch über das Internet angeboten. Im letzten Fall ist der Server eher ein Ziel von Angreifern, da der Benutzerkreis nicht eingeschränkt ist. Aufgrund der immer größer werdenden Komplexität der Software kann heute nicht mehr garantiert werden, dass ein Produkt frei von Fehlern ist. Enthält eine Software Fehler, können Angreifer versuchen, diese als Schwachstelle auszunutzen, um die Kontrolle über das System zu übernehmen. In weiteren Schritten können z. B. Schadprogramme ausgeführt werden oder ein Konsolenzugriff mit Administratorrechten möglich sein. Wird ein Dienst von Anfang an mit Administratorrechten betrieben, dann erhält der Angreifer durch die Kompromittierung direkten administrativen Zugriff, sofern eine Sicherheitslücke ausgenutzt werden kann.

In einer Standardinstallation eines Betriebssystems werden häufig Dienste mitinstalliert und gestartet, die für den eigentlichen Betrieb des Servers nicht benötigt werden. Diese Dienste stellen Schnittstellen zur Verfügung oder können Softwarefehler enthalten, die von Angreifern ausgenutzt werden können.

Gegenmaßnahmen in der Grundarchitektur:

- Die Installation des Betriebssystems und den darauf betriebenen Diensten erfolgt als Minimalsystem.
- Nicht benötigte Dienste sollen deinstalliert oder deaktiviert werden.
- Dienste dürfen nur über jene Rechte verfügen, die für den Betrieb erforderlich sind (restriktive Rechtevergabe). Wenn möglich, sollten sie mit eingeschränkten (minimalen) Rechten eines Benutzers laufen.
- Der Betrieb eines Dienstes mit Administratorrechten ist möglichst zu vermeiden.
- Lokale Netzdienste sollen nur an das lokale Netzwerk-Interface (Loopback) gebunden werden.
- Die Aktivierung von Speicherschutzmechanismen.
- Die Aktivierung von Speicherrandomisierung.

Gegenmaßnahmen im Betrieb:

- Regelmäßige Aktualisierung der Software, insbesondere Sicherheitsupdates.

Restrisiko:	Bisher unentdeckte Schwachstellen im Betriebssystem oder in Anwendungen können von Zero-Day-Exploits ausgenutzt werden.
	Beim Ausnutzen von Schwachstellen können die Rechte erlangt werden, mit denen der Dienst betrieben wird. Wird der Dienst sogar mit Administratorrechten betrieben, kann ein Angreifer auf diese Weise an Administratorrechte gelangen.

5.1.2 Erraten und/oder Manipulation von Passwörtern

Bedrohung: Unerlaubter Zugriff auf Netzdienste (z. B. SSH) oder auf dem Server betriebene Anwendungen

Schwachstelle: Zu schwach gewählte Passwörter

Server-Systeme können Dienste zur Verfügung stellen, die eine Anmeldung mittels Benutzername und Passwort erfordern. Ein Angreifer kann durch Ausprobieren von Benutzerkonten und Passwörtern Zugriff zu dem System erlangen.

Gegenmaßnahme in der Grundarchitektur:

- Definieren von Passwortrichtlinien, die folgende Punkte festlegen:
  - Länge, Komplexität und Gültigkeit von Passwörtern,
  - Regelmäßiges Wechseln von Passwörtern,
  - Die Begrenzung der fehlerhaften Anmeldeversuche bzw. eine zeitliche Verzögerung (Teergrube) erschwert Brute-Force Angriffe.
- Umsetzen der Passwortrichtlinien in der Benutzerverwaltung, dem Betriebssystem und für die betriebenen Dienste.

Restrisiko: Benutzername und Passwort können auf anderen Wegen beschafft werden (z. B. mittels Social Engineering) und unbefugte Personen können sich damit anmelden.

Variante 5.1.2.A für hohen Schutzbedarf: Zwei-Faktor-Authentisierung

Anwendungsbereich: Hoher Schutzbedarf bezüglich mindestens eines Grundwertes

Phase im Ablaufplan: Konzeption, Realisierung, Betrieb

Zusätzlich zu dem Passwort wird bei der Zwei-Faktor-Authentisierung noch ein weiteres Authentisierungsmerkmal überprüft, bevor auf ein System zugegriffen werden kann. Der zweite Faktor kann ein Besitz (z. B. ein USB-Token oder Zertifikat) oder ein biometrisches Merkmal (z. B. Fingerabdruck) sein. Selbst durch die Kenntnis des Passwortes ist ein Angreifer somit nicht in der Lage sich am Server anzumelden.

Der Einsatz einer Zwei-Faktor-Authentisierung kann auch den Missbrauch von lokal gespeicherten Authentisierungsdaten verhindern, da der zweite Faktor als Besitz oder biometrisches Merkmal nicht auf den Server gespeichert werden kann.

Restrisiko: Alle benötigten Authentisierungsmerkmale geraten in den Besitz eines Angreifers.

Verliert der Benutzer ein Authentisierungsmerkmal, kann er sich nicht mehr am System anmelden.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand bei der Konzeption, der Realisierung und im Betrieb.

5.1.3 Unautorisierter Zugriff auf Dienste

Bedrohung: Dienste stehen Benutzern oder Servern zur Verfügung, die nicht für die Nutzung vorgesehen sind

Schwachstelle: Fehlende Zugriffsregelung

Fehlkonfiguration

Einige Dienste dürfen nur von dedizierten Servern oder Netzen erreichbar sein. Z. B. darf ein DatenbankServer seinen Dienst meistens nicht über das Internet zur Verfügung stellen. Durch Fehlkonfiguration oder fehlende Zugriffsregelung können diese Dienste auch von anderen Systemen oder aus dem Internet erreichbar sein. Abhängig von den zur Verfügung gestellten Diensten können Angreifer unbefugt auf Daten zugreifen oder Dienste missbrauchen.

Gegenmaßnahme in der Grundarchitektur:

- Blockieren der Verbindung von nicht zugelassenen Netzen oder Systemen durch die vorgelagerten Paketfilter in der Grundarchitektur (s. ISi-LANA).
- Dienste, die nicht über das Internet zur Verfügung gestellt werden sollen, werden nur auf Server im internen Netz bereitgestellt.
- Alles, was nicht explizit erlaubt ist, muss die Grundkonfiguration abweisen (Whitelist-Ansatz) (s. ISi-LANA).

Restrisiko: Systeme aus demselben Netzsegment, die nicht für die Nutzung der Dienste vorgesehen sind und nicht durch einen Paketfilter von den Diensten getrennt werden können, können noch darauf zugreifen.

5.1.4 Zugriff auf verwaiste Benutzerkonten

Bedrohung: Angreifer können sich an nicht mehr genutzten Benutzerkonten anmelden und mit den erlangten Rechten auf vertrauliche Daten zugreifen.

Schwachstelle: Benutzerkonten werden nach der Versetzung von Mitarbeitern oder nach der Beendigung des Arbeitsverhältnisses nicht deaktiviert oder gelöscht.

Angreifer können auf nicht genutzte Benutzerkonten zugreifen, wenn sie Kenntnis von den Passwörtern haben (z. B. durch Erraten von Passwörtern). Abhängig von den Berechtigungen des Benutzerkontos, können Angreifer z. B. vertrauliche Daten lesen oder die Kommunikation über das Netz abhören.

Gegenmaßnahme in der Grundarchitektur:

- Deaktivieren bzw. Löschen von nicht benötigten Benutzerkonten
- Anbinden einer zentralen Benutzerverwaltung

Restrisiko: Wenn nicht genutzte Benutzerkonten deaktiviert oder gelöscht werden, dann kann diese Schwachstelle nicht mehr ausgenutzt werden.

Variante 5.1.4.A für normalen Schutzbedarf: Lokale Benutzerverwaltung

Anwendungsbereich: Normaler Schutzbedarf bzgl. mindestens eines Grundwertes

Phase im Ablaufplan: Konzeption, Betrieb

> Stehen nur eine geringe Anzahl von Servern und Clients zur Verfügung, kann der Aufbau einer zentralen Benutzerverwaltung zu aufwendig sein. In diesem Fall kann die Benutzerverwaltung lokal erfolgen. Das bedeutet, dass die Benutzerkonten und Berechtigungen direkt auf dem Server manuell erstellt und gepflegt werden.
>
> Ist der Zugriff auf die zentrale Benutzerverwaltung nicht möglich (z. B. aufgrund von Verbindungsregeln in einem separaten Netzsegment), kann ebenfalls eine lokale Benutzerverwaltung erfolgen.

Restrisiko: Verlässt ein Mitarbeiter das Unternehmen, wird vergessen, das Benutzerkonto zu deaktivieren bzw. zu löschen.

Ein Zugriff auf die Daten bleibt lokal auf den Server begrenzt. Dadurch entsteht die Gefahr von Inkonsistenzen zu andern Servern.

Umsetzungsaufwand: Die Umsetzung verursacht einen geringen Aufwand in der Konzeption und einen mittleren Aufwand im Betrieb.

5.1.5 Unbefugter Zugriff auf Schnittstellen zur Fernadministration

Bedrohung: Angreifer erlangen durch Schnittstellen für die Fernadministration Zugriff auf Server-Systeme

Schwachstelle: Keine ausreichende oder zu schwache Authentisierung der Fernadministrationszugänge

Fernadministration bezeichnet hier die Einwahl in das Unternehmensnetz von außerhalb (z. B. über das Internet). Fernadministrationszugänge werden häufig für die Einwahl von Administratoren außerhalb der Kernarbeitszeit zur Administration, Überwachung, Fehleranalyse und Fehlerbehebung genutzt. Sind diese Zugänge nicht ausreichend geschützt, können Angreifer Zugriff auf die Infrastruktur des Unternehmens bekommen.

Bei der Nutzung von Fernadministrationszugängen ist darauf zu achten, dass bei VS-relevanten Daten zusätzlich die VSA zu berücksichtigen ist.

Bei Daten, die dem Datenschutzgesetz unterliegen, ist der Datenschutzbeauftragte hinzu zuziehen.

Gegenmaßnahme in der Grundarchitektur:

- Einwahl zur Fernadministration über kryptografisch gesicherte Zugänge (z. B. VPN) (siehe [ISi-LANA]).
- Erstellen und Umsetzen einer Kennwortrichtlinie.

Restrisiko: Durch Erraten oder systematisches Durchprobieren von Passwörtern (z. B. mittels Brute Force) können Angreifer Zugriff erlangen.

Varianten der Grundarchitektur:

- **Variante 5.1.2.A für hohen Schutzbedarf: Zwei-Faktor-Authentisierung**

5.1.6 Einsatz veralteter Software

Bedrohung: Kompromittierung eines Servers durch Ausnutzen von Sicherheitslücken

Schwachstelle: Auf Systemen wird Software eingesetzt, die Sicherheitslücken enthält

Sicherheits-Updates werden nicht rechtzeitig installiert

Es gibt unterschiedliche Gründe, warum veraltete Softwareversionen auf Servern betrieben werden. Installierte Software wird häufig nicht aktualisiert, da nicht bekannt ist, dass sie Schwachstellen beinhaltet. Oft ist auch nicht bekannt, dass auch neuere Versionen der Software existieren, die Fehler einer älteren Version korrigieren. Ein weiterer Grund kann sein, dass einfach vergessen wird, eine Softwareaktualisierung des Systems durchzuführen. Diese Gründe führen dazu, dass Software auf einem Server betrieben wird, die fehlerhaft ist oder Sicherheitslücken beinhaltet. Diese können durch einen Angreifer ausgenutzt werden, um in den Server einzudringen oder die Verfügbarkeit von Diensten zu beeinträchtigen.

Gegenmaßnahme in der Grundarchitektur:

- Regelmäßige Aktualisierung der Software-Komponenten.
- Einbinden des Servers in ein Patch- und Änderungsmanagement.

Restrisiko: Für vorhandene Sicherheitslücken gibt es noch keine Sicherheits-Updates.

Variante 5.1.6.A für normalen Schutzbedarf: Softwareaktualisierungen nicht über einen zentralen Server, sondern direkt vom Hersteller

Anwendungsbereich: normaler Schutzbedarf mindestens eines Grundwertes

Phase im Ablaufplan: Betrieb

Anstatt einen zentralen Server zur Verteilung von Softwareaktualisierungen zu verwenden, können diese auch, für jeden Server einzeln, vom Hersteller heruntergeladen und anschließend installiert werden. Die Installation der Updates kann hierbei automatisch oder manuell durch den Administrator oder Benutzer erfolgen. Erfolgt dies über den Benutzer, dann muss dieser über entsprechende Berechtigungen zur Installation verfügen. Alternativ kann auch eine automatische Installation erfolgen, damit Updates zeitnah eingespielt werden. Diese Variante ist jedoch nur für kleine Unternehmen mit nur wenigen Servern praktikabel.

Restrisiko: Updates werden verzögert eingespielt (bei manuellem Update).

Updates werden vor der Installation nicht getestet.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand im Betrieb.

5.2 Gefährdungen durch Entwenden und Ausspähen (Vertraulichkeit)

5.2.1 Mitlesen von Administrationstätigkeiten

Bedrohung: Angreifer können Administrationstätigkeiten (z. B. die Eingabe von Passwörtern) mitlesen

Schwachstelle: Ausnutzen von unverschlüsselten Verbindungen

Die Administration erfolgt aus einem Netz heraus, auf das der Angreifer Zugriff hat

Wenn Angreifer die Möglichkeit haben, Administrationstätigkeiten mitzulesen, können sie sensitive Daten über Benutzer oder Systeme erlangen (z. B. Passwörter), die für weitere Angriffe genutzt werden können. Eine solche Schwachstelle kann große Auswirkungen auf den Betrieb haben, wenn dadurch andere Systeme kompromittiert werden.

Gegenmaßnahme in der Grundarchitektur:

- Einsatz eines separaten Management-Netzes (Out-of-Band Management). Die Protokolle sollten, wenn möglich, verschlüsselt werden.

Restrisiko: Werden unverschlüsselte Protokolle im Out-of-Band Management verwendet und ein Angreifer hat Zugriff auf dieses Netzsegment, dann ist das Ausnutzen dieser Schwachstelle immer noch möglich.

Variante 5.2.1.A für hohen Schutzbedarf: Ausschließlicher Einsatz verschlüsselter Protokolle im Out-of-Band Management-Netz

Anwendungsbereich: hoher Schutzbedarf bzgl. Vertraulichkeit

Phase im Ablaufplan: Konzeption, Realisierung

Werden ausschließlich verschlüsselte Protokolle im Out-of-Band Management-Netz eingesetzt, können keine Daten über das Netz mitgelesen werden. Dies umfasst auch die Protokolle, die für das Monitoring der Server verwendet werden.

Restrisiko: Die Gefährdung wird mit dieser Variante bei hohem Schutzbedarf deutlich verringert. Durch Zwischenschalten in die verschlüsselte Verbindung (man-in-the-middle-Angriffe) ist das Ausspähen des Out-of-Band-Managements jedoch immer noch möglich.

Umsetzungsaufwand: Da nicht alle Geräte Protokolle unterstützen, bei denen eine Verschlüsselung möglich ist, kann die Umsetzung dieser Variante zu hohen Kosten in der Beschaffung führen.

Variante 5.2.1.B für normalen Schutzbedarf: Netz ohne Management-Zone (für kleine Netze ohne besonderen Schutzbedarf)

Anwendungsbereich: normaler Schutzbedarf bzgl. eines Grundwertes

Phase im Ablaufplan: Konzeption, Realisierung

Beschreibung:

Bei kleinen Institutionen kann auf den Betrieb eines separaten Management-Netzes verzichtet werden. Hierbei sollen jedoch ausschließlich verschlüsselte Protokolle für den Administrationszugriff verwendet werden, damit die Kommunikation nicht durch einen Angreifer mitgelesen werden kann.

Restrisiko: Durch den Inband-Management-Verkehr können im LAN-Bereich höhere Netzlasten auftreten. Zudem schwächt die physische Verbindung zwischen Management- und Produktivnetz den Schutz vor Angriffen durch Innentäter. Da die Management-Kommunikation im Produktivnetz abhör- und manipulationsgefährdet ist, erfordert In-Band-Management unbedingt integritätsgesicherte und verschlüsselte Management-Protokolle. Bei einem Ausfall des Produktivnetzes können die Server nicht mehr vom Management-Netz erreicht werden. Die Systemadministration muss dann lokal am jeweiligen Server erfolgen, was eine schnelle Reaktion in Krisensituationen erschwert.

Umsetzungsaufwand: Die Umsetzung verursacht zwar einen geringeren Aufwand in der Konzeption und im Betrieb als in der Grundarchitektur, aber einen höheren Aufwand bei der Konfiguration.

5.2.2 Zugriff auf getrennte Netzsegmente durch fehlerhafte Virtualisierung

Bedrohung: Benutzer oder Angreifer können auf ein fremdes Netzsegment zugreifen

Schwachstelle: Fehlerhafte Konfiguration von virtuellen Netzen oder virtuellen Maschinen

Durch die fehlerhafte Konfiguration von virtuellen Netzen oder virtuellen Maschinen können Netzsegmente gekoppelt werden, die normalerweise physisch getrennt sein sollen. Dies ermöglicht Angreifern, Zugriff auf Netze und den darin betriebenen Systemen zu erlangen.

Gegenmaßnahme in der Grundarchitektur:

- Die Anbindung der Paketfilter an den Virtualisierungsserver erfolgt jeweils durch eine eigene physische Netzwerkkarte.
- Kapselung und Isolation

Restrisiko: Eine fehlerhafte Konfiguration bei der Zuordnung der Netzsegmente führt dazu, dass die physische Trennung der Netze nicht mehr gegeben ist.

Variante 5.2.2.A für normalen Schutzbedarf: Virtualisierung von Servern aus unterschiedlichen Netzsegmenten im internen Netz

Anwendungsbereich: Normaler Schutzbedarf bzgl. mindestens eines Grundwertes

Phase im Ablaufplan: Konzeption, Realisierung

Durch die Virtualisierung von Servern aus unterschiedlichen Netzsegmenten auf demselben Virtualisierungsserver entfällt der Aufbau weiterer Virtualisierungs-

umgebungen für jedes einzelne Netzsegment. Dadurch kann die Hardware der Virtualisierungsumgebung besser ausgenutzt werden und evtl. zusätzliche Lizenzkosten für das Virtualisierungsprodukt fallen weg.

Bei der Virtualisierung müssen die folgenden Aspekte beachtet werden:

– Die Segmentierung der Netze soll bei der Virtualisierung aufrechterhalten werden.
– Die Virtualisierung ersetzt keinen physischen Paketfilter.
– Virtuelle Maschinen, die demselben Netzsegment zugeordnet sind, sollen über dedizierte physische Netzwerkkarten an die Paketfilter angebunden werden.

Restrisiko: Aufgrund von Softwareschwachstellen in der Netzseparierung des Virtualisierungsproduktes ist ggf. keine Segmentierung der Netze mehr vorhanden. Ebenso führt eine fehlerhafte Konfiguration bei der Zuordnung der Netzsegmente dazu, dass die physische Trennung der Netze nicht mehr gegeben ist.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand bei der Konzeption und der Realisierung.

Variante 5.2.2.B für hohen Schutzbedarf: Virtualisierung von Servern mit hohem Schutzbedarf

Anwendungsbereich: Hoher Schutzbedarf bzgl. mindestens eines Grundwertes

Phase im Ablaufplan: Konzeption, Realisierung

Die Virtualisierung von IT-Systemen mit hohem Schutzbedarf ist im Einzelfall abhängig von den Anwendungen und der eingesetzten Virtualisierungstechnologie. Hier sollte auf ausreichende Kapselung und Isolation der virtuellen IT-Systeme geachtet werden. Die Virtualisierung von Servern aus unterschiedlichen Netzsegmenten ist nicht erlaubt. Ebenso ist der Betrieb von Servern mit unterschiedlichem Schutzbedarf auf demselben Virtualisierungsserver nicht erlaubt.

Restrisiko: Bei Softwareschwachstellen in der Netzseparierung des Virtualisierungsproduktes ist ggf. keine Segmentierung der Netze mehr vorhanden.

Bei fehlerhafter Konfiguration des Virtualisierungsproduktes können sich Server, die eigentlich in unterschiedlichen Netzsegmenten betrieben werden sollen, in demselben Netzsegment befinden. Der Schutz der physischen Paketfilter wird hierdurch aufgehoben.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand bei der Konzeption und der Realisierung.

5.2.3 Unbefugter Zugriff auf lokalen Massenspeicher

Bedrohung: Ein Angreifer gelangt durch physischen Zugriff auf den Server an die Daten der lokalen Massenspeicher (z. B. bei Wartungsarbeiten)

Schwachstelle: Die Daten auf dem lokalen Massenspeicher liegen im Klartext vor

Der Zugriff auf die gespeicherten Daten des Massenspeichers eines Servers erfordert üblicherweise eine Authentisierung. Die Gefährdungen bzgl. des unerlaubten Zugriffs auf-

grund zu schwach gewählter Passwörter wurden bereits in der Gefährdung 5.1.2 behandelt. Bei physischem Zugriff (z. B. in Wartungsfällen) kann jedoch direkt auf die Festplatte zugegriffen werden. Dadurch können Daten kopiert oder manipuliert werden.

Gegenmaßnahme in der Grundarchitektur:

- Die betriebenen Server stehen in einer gesicherten Umgebung, die über eine Zutrittskontrolle verfügt.

Restrisiko: Werden Server zu Wartungszwecken an den Hersteller zurückgesendet, können schützenswerte Daten auf den Massenspeichern enthalten sein.

Variante 5.2.3.A für hohen Schutzbedarf: Festplattenverschlüsselung

Anwendungsbereich: hoher Schutzbedarf bzgl. Vertraulichkeit

Phase im Ablaufplan: Konzeption, Realisierung

Durch eine Festplattenverschlüsselung werden alle Daten einer Festplatte verschlüsselt. Der Zugriff auf die Daten kann erst nach Eingabe eines Passwortes erfolgen. Wird die Betriebssystempartition ebenfalls verschlüsselt, ist die Eingabe eines Passwortes auch für den Start des Betriebssystems erforderlich.

Wird das System zu Wartungszwecken zum Hersteller gesandt, dann ist es einem Angreifer ohne Wissen des Passwortes nicht möglich, auf die Daten der eingebauten Festplatten zuzugreifen.

Restrisiko: Während des Betriebs ist ein unverschlüsselter Zugang zu den Daten möglich.

Durch die Verschlüsselung der Daten wird deren Verfügbarkeit beeinträchtigt, da z. B. bei Verlust des Schlüssels nicht mehr auf die Daten zugegriffen werden kann.

Erfordert der Start des Betriebssystems die Eingabe eines Passwortes, ist die Verfügbarkeit des Betriebssystems und die seiner Dienste beeinträchtigt (z. B. bei einem ungeplanten Herunterfahren des Servers aufgrund eines Stromausfalls kann der Server erst wieder in Betrieb genommen werden, wenn das Passwort an der Konsole des Servers eingegeben wurde).

Bei der Wahl eines schwachen Passwortes ist dies möglicherweise leicht durch einen Angreifer zu erraten.

Umsetzungsaufwand: Die Umsetzung verursacht einen hohen Aufwand bei der Konzeption und der Realisierung.

Variante 5.2.3.B für hohen Schutzbedarf: Festplattenverschlüsselung mit TPM ohne Passwortschutz

Anwendungsbereich: hoher Schutzbedarf bzgl. Vertraulichkeit

Phase im Ablaufplan: Konzeption, Realisierung

Die Verschlüsselung der gesamten Festplatte (inkl. Systempartition) kann in Verbindung mit einem TPM realisiert werden. Hierbei ist darauf zu achten, dass die Hardware auch TPM-fähig ist. Der Schlüssel, der zur Verschlüsselung der Daten auf der Festplatte benötigt wird, ist in dem TPM gespeichert. Auf die Daten der Festplatten kann dann nur in Verbindung mit dem TPM zugegriffen werden, welches zum Zeitpunkt des Einrichtens der Festplattenverschlüsselung genutzt wurde. Werden die Festplatten in einen anderen Server eingebaut, kann dort nicht auf die Daten zugegriffen werden, da der Schlüssel dort nicht zur Verfügung steht. Der Zugriff auf den Schlüssel innerhalb des TPM erfolgt in dieser Variante ohne die Eingabe eines Passwortes.

Diese Variante schützt die Daten z. B. bei dem Diebstahl der Festplatten. Des Weiteren kann bei Defekt einer Festplatte innerhalb der Garantiezeit diese gefahrlos vom Hersteller ausgetauscht werden, da aufgrund der Verschlüsselung nicht auf die gespeicherten Daten zugegriffen werden kann.

Restrisiko: Während des Betriebs ist ein unverschlüsselter Zugang zu den Daten möglich.

Durch die Verschlüsselung der Daten wird deren Verfügbarkeit beeinträchtigt, da z. B. bei Verlust des Schlüssels oder Defekt des TPM nicht mehr auf die Daten zugegriffen werden kann.

Hat ein Angreifer Zugriff auf den gesamten Server (TPM und Festplatten), kann direkt auf die Daten zugegriffen werden.

Umsetzungsaufwand: Die Schlüsselverwaltung verursacht einen hohen Aufwand.

Variante 5.2.3.C für hohen Schutzbedarf: Festplattenverschlüsselung mit TPM und Passwortschutz

Anwendungsbereich: hoher Schutzbedarf bzgl. Vertraulichkeit

Phase im Ablaufplan: Konzeption, Realisierung

Zusätzlich zu der Variante 5.2.3.B wird der Zugriff auf das TPM durch ein Passwort geschützt. Das Betriebssystem kann erst starten, wenn das Passwort für den Zugriff auf das TPM eingegeben wurde, das den Schlüssel zum Entschlüsseln der Festplatte enthält. Wird z. B. der Server gestohlen, dann kann ein Angreifer nur mit Wissen des Passwortes auf die Daten der Festplatte zugreifen.

Sollen die im TPM gespeicherten Schlüssel auch nach der Außerbetriebnahme des Servers weiterhin genutzt werden (z. B. um noch auf die damit verschlüsselten Daten zuzugreifen), dann ist darauf zu achten, dass bei der Außerbetriebnahme die auf dem TPM gespeicherten kryptografischen Schlüssel zu löschen sind.

Restrisiko: Während des Betriebs ist ein unverschlüsselter Zugang zu den Daten möglich.

Durch die Verschlüsselung der Daten wird deren Verfügbarkeit beeinträchtigt, da z. B. bei Verlust des Schlüssels oder bei Defekt des TPM nicht mehr auf die Daten zugegriffen werden kann.

Wurde ein zu schwaches Passwort gewählt, kann ein Angreifer dieses ggf. erraten.

Umsetzungsaufwand: Die Schlüsselverwaltung verursacht einen hohen Aufwand.

Variante 5.2.3.D für normalen Schutzbedarf: Ausbau der Festplatte bei Wartungsarbeiten.

Anwendungsbereich: normaler Schutzbedarf bzgl. eines Grundwertes

Phase im Ablaufplan: Betrieb

Wartungsarbeiten an Server-Systemen können sowohl in dem Rechenzentrum der Institution erfolgen oder ggf. auch durch das Einsenden der Hardware an den Hersteller. Bei beiden Möglichkeiten haben institutionsfremde Personen Zugriff auf die Hardware und können, wenn Daten auf der lokalen Festplatte abgelegt worden sind, unerlaubt auf diese Daten zugreifen, wenn diese unverschlüsselt sind. Um einen unerlaubten Zugriff auf die lokalen Festplatten vorzubeugen, sollen die Festplatten vor Wartungsarbeiten ausgebaut werden.

Restrisiko: Die Festplatte kann nicht in allen Fällen ausgebaut werden, da sie eventuell bei den Wartungsarbeiten benötigt wird.

Umsetzungsaufwand: Die Umsetzung verursacht einen hohen Aufwand im Betrieb.

Variante 5.2.3.E für hohen Schutzbedarf: Physische Zerstörung der Festplatte bei Entsorgung

Anwendungsbereich: hoher Schutzbedarf bzgl. Vertraulichkeit

Phase im Ablaufplan: Betrieb

Häufig wird eine Datenlöschung nach Außerbetriebnahme eines Servers vergessen oder aufgrund einer defekten Festplatte ist dies nicht mehr möglich. Nach der Außerbetriebnahme werden die Systeme in der Regel anderen Firmen zur Verfügung gestellt, die sich um die Entsorgung der Hardware kümmern. Diese könnten dann auf die noch darauf enthaltenen Daten zugreifen. Werden die eingebauten Festplatten bei der Außerbetriebnahme physisch zerstört, ist es nicht mehr möglich, die darauf enthaltenen Daten auszulesen.

Restrisiko: Wenn die physische Zerstörung der Festplatte nicht ausgereicht hat, können eventuell noch Daten rekonstruiert werden.

Umsetzungsaufwand: Der Ausbau der Festplatte ist mit einem gewissen Aufwand verbunden.

5.2.4 Unbefugter Zugriff auf das Speichernetz

Bedrohung: Unautorisierter Zugriff auf den Massenspeicher

Schwachstelle: Keine Authentisierung beim Zugriff auf das Speichernetz

Häufig werden die Daten einer Institution in einem zentralen Speichernetz abgelegt, auf das über das interne Netz zugegriffen werden kann. Technisch kann dies sowohl über ein NAS als auch über ein SAN realisiert werden. Wird dieser Zugang ohne oder mit zu schwachen Authentisierungsmechanismen zur Verfügung gestellt, kann ein Angreifer, der Zugang zu dem Netz hat, Zugriff auf diese Daten erlangen.

Gegenmaßnahme in der Grundarchitektur:

- Bei dem Einsatz eines SAN wird innerhalb der Grundarchitektur ein dediziertes Speichernetz gefordert. Dadurch wird die Anzahl der berechtigten Benutzer eingeschränkt, die Zugriff auf das Speichernetz haben.

Restrisiko: Haben Angreifer Zugriff auf das Netz der Institution, dann können diese ebenfalls auf vorhandene NAS-Systeme zugreifen.

Verschafft sich ein Angreifer Zugang über den entsprechenden Dienst zu dem separaten Speichernetz, kann er weiterhin auf den zur Verfügung gestellten Massenspeicher zugreifen.

Varianten der Grundarchitektur:

- **Variante 5.1.2.A für hohen Schutzbedarf: Zwei-Faktor-Authentisierung**

Variante 5.2.4.A für hohen Schutzbedarf: Erforderliche Authentisierung bei Zugriff auf das Speichernetz

Anwendungsbereich: Hoher Schutzbedarf bzgl. Integrität

Phase im Ablaufplan: Konzeption, Realisierung, Betrieb

Wird für den Zugriff auf das Speichernetz eine Authentisierung eingesetzt, wird es einem Angreifer erschwert, auf die Daten zuzugreifen.

Restrisiko: Das Restrisiko ist zum größten Teil abhängig vom Sicherheitsbewusstsein der Benutzer und der Einhaltung der organisatorischen Richtlinien.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand in der Konzeption und im Betrieb.

Variante 5.2.4.B für hohen Schutzbedarf: Verschlüsselung von Massenspeicherprotokollen

Anwendungsbereich: Hoher Schutzbedarf bzgl. Vertraulichkeit

Phase im Ablaufplan: Konzeption, Realisierung, Betrieb

Durch die Verschlüsselung der Protokolle, die für das Speichernetz genutzt werden, ist ein Angreifer nicht mehr in der Lage die übertragenen Daten mitzulesen.

Restrisiko: Schwache Passwörter werden durch Ausprobieren/Raten geknackt.

Ein Keylogger kann das Passwort zur Freigabe des Schlüssels aufzeichnen und weitergeben.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand in der Konzeption und einen hohen Aufwand im Betrieb.

5.2.5 Unbefugter Zugriff auf die Backup-Medien

Bedrohung: Verlust sensibler Daten

Schwachstelle: Angreifer haben Zugriff auf die Backup-Medien

Um einem Datenverlust vorzubeugen, werden alle Daten der Massenspeicher auf ein Datensicherungsmedium kopiert. Da der gesamte Datenbestand auf diese Medien gespiegelt wird, können vertrauenswürdige Daten mit hohem Schutzbedarf enthalten sein. Hat ein Angreifer Zugriff auf die Datensicherungsmedien, dann können diese entwendet und ausgelesen werden.

Gegenmaßnahme:

- Die Datensicherungsmedien sind in einer gesicherten Umgebung untergebracht, die über eine Zutrittskontrolle verfügt. Die entsprechenden Maßnahmen werden durch die IT-Grundschutz-Kataloge abgedeckt (siehe [BSI_GSK]).

Restrisiko: Je höher der Aufwand, der bei der Absicherung der Umgebung betrieben wird, desto besser kann die Bedrohung minimiert werden.

Variante 5.2.5.A für hohen Schutzbedarf: Verschlüsselung der Datensicherung

Anwendungsbereich: hoher Schutzbedarf bzgl. Vertraulichkeit

Phase im Ablaufplan: Konzeption, Realisierung

Durch die Verschlüsselung der Datensicherung ist diese bei einem Diebstahl geschützt. Das Entschlüsseln der Daten kann nur durch den Besitz des entsprechenden Schlüssels erfolgen. Ein Angreifer kann ohne diesen Schlüssel nicht auf die Daten gestohlener Backup-Medien zugreifen.

Restrisiko: Ein Angreifer erhält Zugang zu dem Schlüssel, der zum Erstellen der Datensicherung verwendet wurde, und kann ebenfalls auf die Backup-Medien zugreifen.

Durch die Verschlüsselung der Backup-Medien wird deren Verfügbarkeit beeinträchtigt, da z. B. bei Verlust des Schlüssels nicht mehr auf die dort gespeicherten Daten zugegriffen werden kann.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand in der Konzeption und einen hohen Aufwand im Betrieb.

5.2.6 Unbefugter Zugriff auf Daten aufgrund zu umfangreicher Berechtigungen

Bedrohung: Benutzer können auf Daten zugreifen, für die sie eigentlich keine Berechtigung haben

Schwachstelle: Das zugreifende Benutzerkonto ist mit zu umfangreichen Berechtigungen ausgestattet

Werden jedem Benutzer einzeln Rechte zugewiesen, dann können z. B. aufgrund von Administrationsfehlern Inkonsistenzen zwischen Benutzern auftreten, welche dieselbe Aufgabe erfüllen sollen. Dadurch kann es z. B. passieren, dass einzelne Benutzer umfangreichere Berechtigungen erhalten, als sie eigentlich für ihre Arbeit benötigen. Durch diese umfangreichen Berechtigungen kann es einem Benutzer möglich sein, unbefugt auf Daten zuzugreifen, die außerhalb seines Tätigkeitsbereichs liegen.

Gegenmaßnahme in der Grundarchitektur:

- Einführung einer rollenbasierten Rechtevergabe. Rollen werden bestimmte Berechtigungen zugewiesen. Den Rollen werden wiederum Benutzer zugeordnet. Dadurch muss nicht die Berechtigung einzelner Benutzer gepflegt werden, sondern nur die der Rollen.
- Benutzer sollen nur mit den Berechtigungen ausgestattet sein, die sie für die Durchführung ihrer Aufgaben benötigen.

Restrisiko: Fehlkonfiguration durch die Administratoren.

Werden z. B. für Projekte temporär umfangreichere Rechte erteilt, kann vergessen werden, diese Berechtigungen nach Projektende wieder zu entziehen.

5.2.7 Unerlaubtes Starten von ausführbaren Dateien

Bedrohung: Nicht zugelassene Programme werden auf einem Server in dafür nicht zugelassene Verzeichnisse kopiert und ausgeführt (z. B. im /tmp Verzeichnis auf Linux/Unix-Systemen). Diese Programme können z. B. die Stabilität des Betriebssystems oder die Integrität von Daten negativ beeinflussen.

Schwachstelle: Der Benutzer hat zu umfangreiche Berechtigungen

Verzeichnisse oder Partitionen sind mit zu umfangreichen Rechten ausgestattet

Benutzer können ausführbare Dateien auf einen Server kopieren. Kommen diese ausführbaren Dateien aus einer nicht vertrauenswürdigen Quelle, ist es möglich, dass sie Schadsoftware beinhalten. Die Ausführung dieser Dateien kann zur Kompromittierung des Betriebssystems oder von Programmen führen und weitere Angriffe ermöglichen.

Bei Linux-/Unix-Systemen können Programmen (z. B. durch Setzen des SUID-Bits) umfangreiche Rechte zugewiesen werden, die es einem normalen Benutzer ermöglichen das Programm mit Administrationsrechten zu starten. Stammt ein Programm mit gesetztem SUID-Bit aus einer nicht vertrauenswürdigen Quelle, dann kann die Ausführung weitreichende Schäden an Daten und Betriebssystem anrichten.

Gegenmaßnahme in der Grundarchitektur:

- Die Ausführungskontrolle verhindert den Start von Programmen auf Wechseldatenträgern und in Verzeichnissen, in denen der Benutzer Dateien schreiben darf.
- Anbinden einer zentralen Benutzerverwaltung.

Restrisiko: Die richtlinienbasierte Ausführungskontrolle kann bei falscher Konfiguration auch den Start legitimer Anwendungen verhindern.

Das Schadprogramm kann als Anwendungsroutine zugelassener Programme ausgeführt werden, z. B. durch einen Pufferüberlauf in einem regulären Programm.

Unerwünschte Funktionen von zugelassenen Anwendungen werden nicht verhindert.

Variante 5.2.7.A für hohen Schutzbedarf: Ausführen von Dateien unter Linux/Unix verhindern

Anwendungsbereich: Hoher Schutzbedarf bzgl. mindestens eines Grundwertes

Phase im Ablaufplan: Konzeption, Realisierung

Partitionen von Linux-/Unix-Systemen können so konfiguriert werden, dass dort gespeicherte Dateien nicht ausgeführt werden können, obwohl sie als ausführbar markiert sind. Dies ist durch die Verwendung von Dateisystemoptionen möglich, die bei dem Einhängen des Dateisystems gesetzt werden können (z. B. die Option noexec). Diese Option ist abhängig von dem verwendeten Dateisystem und steht evtl. nicht für alle Dateisysteme zur Verfügung.

Restrisiko: Die richtlinienbasierte Ausführungskontrolle kann bei falscher Konfiguration auch den Start legitimer Anwendungen verhindern.

Das Schadprogramm kann als Anwendungsroutine zugelassener Programme ausgeführt werden, z. B. durch einen Pufferüberlauf in einem regulären Programm.

Unerwünschte Funktionen von zugelassenen Anwendungen werden nicht verhindert.

Umsetzungsaufwand: Die Umsetzung verursacht einen zusätzlichen Aufwand in der Realisierung. Im Betrieb erfordert jede Änderung oder Ergänzung zulässiger Anwendungen eine Aktualisierung der Konfiguration und die Durchführung zusätzlicher Tests.

Variante 5.2.7.B für hohen Schutzbedarf: Ausführen von Dateien unter Windows verhindern

Anwendungsbereich: hoher Schutzbedarf bzgl. mindestens eines Grundwertes

Phase im Ablaufplan: Konzeption, Realisierung

Die Ausführungskontrolle, wie sie z. B. unter Windows über die Gruppenrichtlinien realisiert sind, bewirkt, dass ausführbare Dateien nur aus zugelassenen Verzeichnissen gestartet werden dürfen. Sie verwaltet eine Liste von Programmen (eine sogenannte Whitelist), deren Ausführung erlaubt ist. Alle Programme, die nicht in dieser Liste enthalten sind, dürfen nicht ausgeführt werden. Damit soll u. a. verhindert werden, dass Schadprogramme auf dem System ausgeführt werden, die (noch) nicht von einem Virenschutzprogramm erkannt werden.

Restrisiko: Die richtlinienbasierte Ausführungskontrolle kann bei falscher Konfiguration auch den Start legitimer Anwendungen verhindern.

Das Schadprogramm kann als Anwendungsroutine zugelassener Programme ausgeführt werden, z. B. durch einen Pufferüberlauf in einem regulären Programm.

Unerwünschte Funktionen von zugelassenen Anwendungen werden nicht verhindert.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand in der Konzeption und im Betrieb.

5.3 Gefährdungen durch Verändern, Täuschen, Fälschen und Betrügen (Integrität und Authentizität)

5.3.1 Manipulation von Dateien durch Schadprogramme

Bedrohung: Schadprogramme können Dateien (Konfigurationsdateien, Dienste, etc.) auf Servern modifizieren

Schwachstelle: Verbreitung von Schadprogrammen auf dem Server

Durch Schadprogramme kann ein Angreifer die Kontrolle über einen Server erhalten und kann weitere Angriffe durchführen. Ist das Schadprogramm zusätzlich in der Lage, sich im Netz zu verbreiten, sind andere Systeme ebenfalls bedroht.

Gegenmaßnahme in der Grundarchitektur:

- Installation eines Virenschutzprogramms zur Erkennung von Schadprogrammen
- Installation einer Integritätsprüfung zur Feststellung von Änderungen an Dateien

Restrisiko: Das Virenschutzprogramm erkennt die schadhaften Dateien nicht, da diese noch nicht in den aktuellen Virensignaturen enthalten sind.

Das Virenschutzprogramm erkennt die schadhaften Dateien nicht, da die Virensignaturen veraltet sind.

Die Integritätsprüfung erkennt eine Modifikation von Dateien durch Schadprogramme nicht, da diese nicht durch die Integritätsprüfung mit abgedeckt sind.

Variante 5.3.1.A für normalen Schutzbedarf: Verzicht auf Virenschutz

Anwendungsbereich: normaler Schutzbedarf

Phase im Ablaufplan: Konzeption

Bei geeigneter Begründung kann auf den Virenschutz auf Server-Systemen verzichtet werden. Dies kann erfolgen, wenn auf einem vorgelagerten System (z. B. Application Level Gateway) bereits eine Virenprüfung vorgenommen wird oder wenn die Dienste des Servers keinen Virenschutz erfordern. Sollten die Schadprogramme Modifikationen an Dateien des Betriebssystems vornehmen, dann kann dies jedoch noch von der Integritätsprüfung erkannt werden.

Restrisiko: Schadprogramme werden auf den Systemen nicht erkannt.

Umsetzungsaufwand: Die Umsetzung verursacht keinen Aufwand.

Variante 5.3.1.B für normalen Schutzbedarf: Verzicht auf Integritätsprüfung

Anwendungsbereich: normaler Schutzbedarf

Phase im Ablaufplan: Konzeption

Bei geeigneter Begründung kann auf die Integritätsprüfung auf Server-Systemen verzichtet werden.

Restrisiko: Eine Modifikation von Dateien kann nicht automatisiert erkannt werden.

Umsetzungsaufwand: Die Umsetzung verursacht keinen Aufwand.

Variante 5.3.1.C für hohen Schutzbedarf: Erweiterung der Integritätsprüfung auf alle Dateien

Anwendungsbereich: hoher Schutzbedarf bzgl. Integrität

Phase im Ablaufplan: Konzeption, Realisierung

Beschreibung:

Durch die Erweiterung der Integritätsprüfung auf alle Dateien, die auf dem Server liegen, kann ein umfassender Schutz gewährleistet werden, da jede Integritätsverletzung durch diese Maßnahme erkannt wird.

Restrisiko: Veränderungen von Dateien im Arbeitsspeicher (z. B. bereits geladene Bibliotheken) werden nicht erkannt.

Umsetzungsaufwand: Mittlerer Aufwand in der Konzeption und in der Grundkonfiguration.

Variante 5.3.1.D für hohen Schutzbedarf: Einsatz einer Dateisignatur

Anwendungsbereich: hoher Schutzbedarf bzgl. Integrität

Phase im Ablaufplan: Konzeption, Realisierung

Einige Betriebssysteme bieten die Möglichkeit, Signaturen von Dateien zu erstellen (sogenannte Dateisignaturen). Abhängig vom Betriebssystem können diese Signaturen auf unterschiedliche Weise geprüft werden. Die Prüfung kann z. B. vor dem Ausführen eines Programms durchgeführt werden oder bei einer manuell initiierten Überprüfung von Dateien. Je nach Betriebssystem können nicht alle Dateitypen mit einer Signatur versehen werden.

Die Signatur von Dateien kann sowohl manuell von der Institution als auch vom Hersteller erzeugt werden. Einige Betriebssystemhersteller ergänzen bestimmte Dateien bereits mit einer Signatur, um deren Integrität und Authentizität sicherzustellen.

Restrisiko: Eine Modifikation von nicht unterstützten Dateitypen wird hierdurch nicht erkannt.

Bei einer Signaturprüfung kann zwischen dem Zeitpunkt, an dem die Datei verändert wurde und dem Erkennen dieser Änderung bereits Schaden entstanden sein. Dies liegt zum einen daran, dass Widerrufsinformationen von Zertifikaten erst zeitverzögert verfügbar sind und abgerufen werden. Zum anderen werden signierte Dateien auch nach Widerruf des Zertifikats als gültig angesehen, wenn der Widerrufszeitpunkt nach dem Signierzeitpunkt liegt.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand in der Konzeption und in der Grundkonfiguration.

5.3.2 Manipulation des Boot-Codes oder des Bootloaders durch ein Schadprogramm

Bedrohung: Verlust der Vertraulichkeit und der Integrität des Betriebssystems

Schwachstelle: Eine Manipulation des Boot-Codes oder des Bootloaders wird nicht entdeckt

Die Manipulation des Boot-Codes oder des Bootloaders ermöglicht die Kompromittierung des Betriebssystems auf unterster Ebene. Es können dadurch Schnittstellen manipuliert oder vorgetäuscht werden, auf die das Betriebssystem zugreift. Virenschutzprogramme sind in der Lage Bootsektor-Viren zu erkennen. Ebenfalls ist die Manipulation durch ein Virtualisierungs-Rootkit (z. B. Blue Pill) möglich, bei dem das installierte Betriebssystem durch ein Rootkit als virtuelles System betrieben werden kann.

Gegenmaßnahme in der Grundarchitektur:

Installation eines Virenschutzprogramms (abhängig vom Einsatzzweck des Servers).

Restrisiko: Das Virenschutzprogramm kann nur bei gestartetem Betriebssystem die Installation oder Modifikation durch ein Schadprogramm erkennen.

Variante 5.3.2.A für hohen Schutzbedarf: Absicherung des Bootvorgangs mittels TPM

Anwendungsbereich: hoher Schutzbedarf bzgl. Integrität

Phase im Ablaufplan: Konzeption, Realisierung

Durch ein eingebautes TPM in Kombination mit einem angepassten Bootloader kann der Bootvorgang des Servers verifiziert werden. Bevor eine Komponente (Partitionstabelle, Bootloader, Boot-Code, etc.) geladen wird, erfolgt eine Verifikation ihrer Integrität. Schlägt diese Verifikation fehl, wird der Bootvorgang abgebrochen.

Restrisiko: Ein TPM ist nicht für alle Serverarchitekturen verfügbar.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand in der Beschaffung.

5.3.3 Manipulation der Systemuhrzeit

Bedrohung: Die Systemuhrzeit geht falsch

Schwachstelle: Nicht erlaubte Manipulation der Systemuhrzeit

Ungenaue Systemuhr

Die Uhrzeit wird auf Server-Systemen häufig als Zusatzinformation (z. B. für die Protokollierung) verwendet. Bei komplexen Umgebungen ist die genaue Systemuhrzeit wichtig für die Fehleranalyse. Einige Dienste (z. B. eine Zertifizierungsstelle zur Ausstellung von Zertifikaten oder ein Authentifizierungsdienst) benötigen für ihre Aufgabe eine korrekte

Uhrzeit. Steht keine korrekte Uhrzeit für diese Dienste zur Verfügung, dann kann dies eine Beeinträchtigung der Funktionsweise des Dienstes zur Folge haben.

Gegenmaßnahme in der Grundarchitektur:

- Einsatz von Zeitsynchronisation mittels des Network Time Protocols (NTP).

Restrisiko: Durch eine manipulierte Kommunikation mit dem NTP-Server wird eine falsche Systemuhrzeit verbreitet.

Variante 5.3.3.A für hohen Schutzbedarf: Gesicherte Kommunikation mit einem NTP-Server

Anwendungsbereich: hoher Schutzbedarf bzgl. Integrität

Phase im Ablaufplan: Konzeption, Realisierung

Um die Kommunikation mit einem NTP-Server abzusichern, besteht die Möglichkeit, die Antwortdaten mittels einer symmetrischen Signatur (Message Authentication Code, MAC) abzusichern. Der NTP-Server berechnet hierbei eine kryptografische Prüfsumme über die zu sendenden Daten, die mit einem symmetrischen Schlüssel verschlüsselt werden. Um die Prüfsumme zu verifizieren, muss der Empfänger über denselben kryptografischen Schlüssel verfügen. Damit können die Prüfsumme entschlüsselt und die Antwortdaten mit einer nachgerechneten Prüfsumme verifiziert werden.

Restrisiko: Bei der Kompromittierung des NTP-Servers oder des Zeitsignals für den NTP-Server kann eine falsche Uhrzeit verbreitet werden.

Umsetzungsaufwand: Die Umsetzung verursacht einen geringen Aufwand in der Konzeption und einen mittleren Aufwand in der Grundkonfiguration.

5.3.4 Manipulation von Dateien

Bedrohung: Eine ungewollte oder durch einen Angreifer beabsichtigte Manipulation von Dateien

Schwachstelle: Eine Manipulation von Dateien wird nicht erkannt

Eine versehentliche oder durch einen Angreifer beabsichtigte Manipulation von Dateien kann die Integrität und Verfügbarkeit des Servers beeinträchtigen. Dies kann z. B. die Manipulation einer Konfigurationsdatei eines Dienstes sein, durch die neue Funktionen oder Schnittstellen über das Netz zur Verfügung gestellt werden.

Gegenmaßnahme in der Grundarchitektur:

- Verwendung einer Integritätsprüfung.
- Zugriffsschutz auf Dateien (z. B. Authentisierung)

Restrisiko: Änderungen von Dateien, die nicht von der Integritätsprüfung überwacht werden, werden nicht erkannt.

Varianten der Grundarchitektur:

- Variante 5.3.1.B für normalen Schutzbedarf: Verzicht auf Integritätsprüfung
- Variante 5.3.1.C für hohen Schutzbedarf: Erweiterung der Integritätsprüfung auf alle Dateien

- Variante 5.1.2.A für hohen Schutzbedarf: Zwei-Faktor-Authentisierung

5.3.5 Nutzung von kompromittierten Installationsmedien

Bedrohung: Das Installationsmedium beinhaltet bereits kompromittierte Software wie z. B. Viren, Trojaner, o. ä., die später im Netz weiteren Schaden anrichten.

Schwachstelle: Bezug der Medien von einer unautorisierten Quelle

Werden Installationsmedien von einer nicht autorisierten Quelle bezogen, besteht die Möglichkeit, dass sie bereits Schadprogramme oder modifizierte Programme enthalten, die bei der Installation auf das Zielsystem kopiert werden.

Gegenmaßnahme in der Auswahl von Komponenten:

- Bezug der Installationsmedien von einer autorisierten Quelle.
- Überprüfung der Installationsmedien mittels Prüfsummen oder Signatur, die vom Hersteller zur Verfügung gestellt werden.

Restrisiko: Die Installationsmedien und die zur Verfügung gestellten Prüfsummen oder Signaturen sind bereits auf Herstellerseite durch Angreifer kompromittiert worden.

5.4 Gefährdungen durch Verhindern und Zerstören (Verfügbarkeit)

5.4.1 Nicht-Verfügbarkeit durch einen Defekt der Hardware oder Ausfall eines Dienstes

Bedrohung: Das System ist nicht mehr verfügbar

Schwachstelle: Der Ausfall eines Servers oder Dienstes wird zu spät oder gar nicht erkannt

Ein Hardwaredefekt kann die Verfügbarkeit des Gesamtsystems beeinflussen (z. B. bei Ausfall eines Netzteils) oder zum Absturz von Programmen führen (z. B. bei defekten Speicherbausteinen). Die Nicht-Verfügbarkeit des gesamten Servers wird häufig von Benutzern oder Administratoren sehr schnell erkannt, da alle betriebenen Dienste nicht mehr zur Verfügung stehen. Fällt jedoch nur ein einzelner Dienst aus, der zugleich nicht häufig genutzt wird, dann wird dieser Ausfall eher spät erkannt. Wenn Benutzer bemerken, dass ein Dienst nicht verfügbar ist, kann dies der Organisation schaden. Dies ist besonders dann der Fall, wenn diese Dienste z. B. für wichtige Geschäftsprozesse (Bestellungen, Rechnungsstellung, Buchungen, etc.) benötigt werden.

Gegenmaßnahme in der Grundarchitektur:

- Durchführung von Monitoring der Systeme
- Erstellung eines Notfallvorsorgekonzeptes.

Restrisiko: Bei unzureichendem Monitoring wird der Ausfall eines einzelnen Dienstes nicht erkannt.

Abhängig von den zeitlichen Intervallen, in denen das System bzgl. Verfügbarkeit überprüft wird, kann ein Ausfall zu spät erkannt werden.

Variante 5.4.1.A für hohen Schutzbedarf: Einsatz redundanter Komponenten

Anwendungsbereich: hoher Schutzbedarf bzgl. Verfügbarkeit

Phase im Ablaufplan: Konzeption, Realisierung

In den meisten Servern können heutzutage viele eingesetzte Hardware-Komponenten (z. B. Netzteil, Festplatten, Controller) redundant ausgelegt werden, sodass bei dem Ausfall einer Komponente deren Funktion automatisch von der redundanten Komponente übernommen wird. Wichtig ist hierbei, dass die Verfügbarkeit aller Komponenten über das Monitoring überwacht wird, damit eine ausgefallene Komponente entdeckt und kurzfristig ersetzt wird.

Restrisiko: Nicht redundante Komponenten fallen aus.

Umsetzungsaufwand: Die Umsetzung verursacht einen geringen Aufwand in der Konzeption und der Realisierung.

Variante 5.4.1.B für hohen Schutzbedarf: Einsatz redundanter Server-Systeme

Anwendungsbereich: hoher Schutzbedarf bzgl. Verfügbarkeit

Phase im Ablaufplan: Konzeption, Realisierung

Um eine höhere Verfügbarkeit von Diensten zu erreichen, können komplette Server-Systeme redundant betrieben werden. Bei dem Ausfall eines Servers wird dessen Aufgabe durch das bzw. die verbleibenden redundanten Systeme übernommen. Hierbei werden häufig Loadbalancer eingesetzt, welche einerseits die Last auf die verfügbaren Systeme verteilen und andererseits die Verfügbarkeit der einzelnen Systeme überwachen. Erkennt der Loadbalancer den Ausfall eines Systems, dann wird dieses nicht mehr mit Anfragen versorgt. Bei der Verwendung eines Loadbalancers sollte dieser ebenfalls redundant ausgelegt werden, damit kein Single Point of Failure entsteht.

Restrisiko: Redundanz beseitigt die Bedrohung des Ausfalls nicht, sie verringert lediglich die Eintrittswahrscheinlichkeit.

Umsetzungsaufwand: Die Umsetzung verursacht einen mittleren Aufwand in der Konzeption und Realisierung.

5.4.2 Datenverlust aufgrund einer defekten Festplatte

Bedrohung: Bedrohung der Integrität und der Verfügbarkeit von Daten

Schwachstelle: Ausfall der Festplatte

Inkonsistentes Dateisystem durch einen abrupten Ausfall des Servers

Die Daten einer Festplatte können durch einen Stromausfall oder den Absturz des Server-Systemes in einen inkonsistenten Zustand geraten, da Metadaten (z. B. Dateiattribute) nicht korrekt auf der Festplatte gespeichert sind. Teile der auf dem Datenträger gespeicherten Daten können hierdurch unbrauchbar werden. Im schlimmsten Fall können die gesamten Daten, die sich auf der Festplatte befinden, unbrauchbar werden. Eine Rekonstruktion der Daten ist unter Umständen nicht mehr möglich.

Gegenmaßnahme in der Grundarchitektur:

- Durchführen einer regelmäßigen Datensicherung.
- Durchführung von Monitoring der Systeme.
- Einsatz eines Journaling-Dateisystems.
- Erstellung eines Notfallvorsorgekonzeptes.
- Einsatz eines RAID-Systems.

Restrisiko: Datenverlust von Daten, die seit der letzten Datensicherung geschrieben wurden.

Variante 5.4.2.A für normalen Schutzbedarf: Weglassen eines RAID

Anwendungsbereich: normaler Schutzbedarf bzgl. Verfügbarkeit

Phase im Ablaufplan: Konzeption, Realisierung

Ein RAID-System wird eingesetzt, um mehrere physische Festplatten eines Servers zu organisieren. Dadurch kann eine höhere Verfügbarkeit bzw. ein größerer Datendurchsatz gewährleistet werden.

Ist eine hohe Verfügbarkeit der Daten und/oder eine hoher Datendurchsatz nicht notwendig, kann auf das RAID verzichtet werden.

Restrisiko: Ausfall der eingesetzten Festplatte und dadurch bedingt der Verlust von Daten.

Umsetzungsaufwand: Die Umsetzung verursacht einen geringen Aufwand in der Konfiguration und einen mittleren Aufwand in der Realisierung.

5.4.3 Ausfall der Energieversorgung

Bedrohung: Server und Daten sind zeitweise nicht verfügbar

permanenter Datenverlust durch Beschädigung des Dateisystem

Schwachstelle: ungeschützt verlegte Verkabelung

defekte Netzkomponenten oder Verkabelung

Bei dem Ausfall der Energieversorgung ist die gesamte Infrastruktur nicht mehr erreichbar. Ein abrupter Ausfall kann auch zu einem Datenverlust oder einer Inkonsistenz von Daten führen, da Daten im Arbeitsspeicher nicht mehr auf die Festplatte geschrieben werden können.

Gegenmaßnahme in der Grundarchitektur:

- Mit einem Journaling File System können Inkonsistenzen im Dateisystem in der Regel beseitigt werden.
- Regelmäßige Backups stellen die Wiederherstellbarkeit der Daten sicher.
- Erstellung eines Notfallvorsorgekonzeptes.

Restrisiko: Daten, die noch nicht permanent gespeichert wurden, gehen bei Stromausfall verloren.

Variante 5.4.3.A für normalen Schutzbedarf: Verzicht auf den Einsatz einer Unterbrechungsfreien Stromversorgung (USV)

Anwendungsbereich: normaler Schutzbedarf bzgl. Verfügbarkeit

Phase im Ablaufplan: Konzeption

Wenn Datenverlust, bedingt durch einen Stromausfall, zu keinen großen Schäden führt und/oder die Daten schnell zu reproduzieren sind, kann auf eine USV verzichtet werden.

Restrisiko: Bei einem Ausfall der Stromversorgung kann es zu Datenverlust kommen. Ebenso ist das System bis zum Wiederanlauf nicht verfügbar.

Umsetzungsaufwand: Kein Umsetzungsaufwand.

5.4.4 Datenverlust durch mangelnde Speicherkapazität

Bedrohung: Bedrohung der Integrität und der Verfügbarkeit von Daten.

Schwachstelle: Kein freier Speicherplatz auf der Festplatte.

Wenn auf einer Festplatte kein Speicherplatz mehr zur Verfügung steht, können noch anstehende Schreiboperationen nicht mehr durchgeführt werden. Dies kann einen Datenverlust zur Folge haben. Daten, die sich noch im Arbeitsspeicher befinden, können nicht mehr auf das Dateisystem geschrieben werden. Mangelnder Speicherplatz führt bei Programmen häufig zu undefinierten Verhalten, bis hin zum Absturz. Dadurch ist ebenfalls die Verfügbarkeit von Diensten beeinträchtigt.

Gegenmaßnahme in der Grundarchitektur:

- Durchführung von Monitoring der Systeme.
- Erstellung eines Notfallvorsorgekonzeptes.
- Verwendung eines Speichernetzes.

Restrisiko: Abhängig von den zeitlichen Intervallen, in denen das System bzgl. freien Speicherplatz überprüft wird, kann ein Ausfall zu spät erkannt werden.

Wurde der Schwellwert für den Füllstand des Speicherplatzes zu klein gewählt, kann zwischen dem Erkennen und dem Erweitern des Speicherplatzes bereits ein Datenverlust erfolgen.

5.4.5 Datenverlust durch Löschen oder Ändern von Daten

Bedrohung: Bedrohung der Integrität und Verfügbarkeit von Daten

Schwachstelle: Benutzer sind mit zu umfangreichen Rechten ausgestattet

Dateien können versehentlich oder vorsätzlich gelöscht oder geändert werden. Dies hat sowohl einen Integritätsverlust oder auch einen Datenverlust zur Folge. Sind Benutzer mit zu umfangreichen Rechten ausgestattet, können z. B. auch betriebssystemrelevante Daten (Treiber, Konfigurationsdateien, etc.) gelöscht und die Verfügbarkeit des Betriebssystems gefährdet werden.

Gegenmaßnahme in der Grundarchitektur:

- Durchführen einer regelmäßigen Datensicherung.
- Benutzer dürfen nur mit den Berechtigungen ausgestattet sein, die sie für die Durchführung ihrer Aufgabe benötigen.

Restrisiko: Verlust von Daten, die seit der letzten Datensicherung gelöscht oder geändert wurden.

5.4.6 Nicht-Verfügbarkeit des Virtualisierungsservers

Bedrohung: Ist der Virtualisierungsserver nicht mehr verfügbar, sind auch alle darauf betriebenen virtuellen Systeme nicht mehr verfügbar

Schwachstelle: Ausfall der Hardware oder der Virtualisierungssoftware auf dem der Virtualisierungsserver betrieben wird

Durch den Einsatz von Virtualisierung werden mehrere Betriebssystemeauf einem Virtualisierungsserver betrieben, die unterschiedliche Dienste über das Netz zur Verfügung stellen. Tritt ein Hardware-Defekt auf, der die Verfügbarkeit des Servers einschränkt, hat dies zur Folge, dass daraufhin alle auf den Virtualisierungsserver betriebenen Dienste ebenfalls nicht mehr zur Verfügung stehen.

Gegenmaßnahme in der Grundarchitektur:

- Redundante Auslegung der Virtualisierungsserver

Restrisiko: Redundanz beseitigt die Bedrohung des Ausfalls nicht, sie verringert lediglich die Eintrittswahrscheinlichkeit.

Variante 5.4.6.A für normalen Schutzbedarf: Nutzung von Live Migration

Anwendungsbereich: normaler Schutzbedarf

Phase im Ablaufplan: Konzeption, Realisierung

Um Wartungsarbeiten an einem physischen Server eines Virtualisierungsclusters durchzuführen, ist es erforderlich, dass die virtuellen IT-Systeme auf andere Server verteilt werden, um ihre Verfügbarkeit sicher zu stellen. Durch den Einsatz von Live Migration ist das Verschieben von virtuellen IT-Systemen zwischen Virtualisierungsservern im laufenden Betrieb möglich. Aus Sicht der Gast-Betriebssysteme oder der Benutzer geschieht dies unterbrechungsfrei.

Restrisiko:	Ausfall aktiver Netz-Komponenten (Router / Switch) wodurch die Erreichbarkeit des Clusters nicht mehr gegeben ist. Die anderen physischen Systeme stellen nicht genügend Ressourcen für CPU und RAM zur Verfügung, sodass es zu Leistungseinschränkungen bei den virtuellen IT-Systemen kommt.
Umsetzungsaufwand:	Die Umsetzung verursacht einen mittleren Aufwand bei der Konzeption und der Realisierung.

6 Fazit

Server bilden das Rückgrat der IT-Infrastruktur. Sie stellen unzählige Dienste zur Verfügung, die heutzutage automatisch von anderen IT-Systemen, wie z. B. einem Arbeitsplatz-PC, genutzt werden, ohne dass der Anwender dies mitbekommt. Alleine bei einem Zugriff auf das Internet sind eine Reihe von Servern, wie z. B. DNS-Server, Proxy-Server, Web-Server, involviert. Stellen Server Dienste im Internet bereit, dann sind diese oft unzähligen Bedrohungen ausgesetzt, da der Zugriff von dort aus nicht kontrolliert werden kann. Jedoch können Bedrohungen auch aus dem internen Netz kommen. Angefangen bei den Mitarbeitern, die versuchen auf nicht für sie bestimmte Informationen zuzugreifen, über ausgefallene Dienste wegen Softwarefehlern bis hin zu nicht frühzeitig erkannten Hardwaredefekten von Servern. Die in dieser Studie vorgestellte Grundarchitektur stellt diesen Bedrohungen Sicherheits-Komponenten entgegen, um einen Ausfall entgegenzuwirken oder eine Gefährdung abzuwehren.

Die Basis der Grundarchitektur beruht auf einem Minimalsystem, welches nur die für den Betrieb notwendige Funktionalität besitzt und eine geringe Angriffsfläche für Bedrohungen bietet. Die Grundarchitektur empfiehlt Sicherheits-Komponenten, die entweder bereits integraler Bestandteil von Betriebssystemen sind (z. B. Zeitsynchronisation oder die zentrale Benutzerverwaltung) oder durch gesonderte Komponenten installiert werden müssen (wie z. B. die Software zur Integritätsprüfung).

Letztendlich ist die Absicherung eines Servers keine statische Angelegenheit, die einmal bei der Installation eingerichtet wird, sondern vielmehr ein Prozess, der stets die aktuellen Anforderungen aus Sicht der IT-Sicherheit betrachten muss. Die in der Studie vorgestellten Maßnahmen müssen im Betrieb permanent überwacht und bei sich ändernden Anforderungen angepasst oder durch weitere Maßnahmen ergänzt werden.

Gerade das Monitoring spielt bei dem Betrieb von Servern eine zentrale Rolle, da der Ausfall eines Servers nicht immer sofort bemerkt wird. Eine fehlerhafte Funktion oder der Ausfall einer Komponente wird häufig erst über andere Komponenten festgestellt, die nicht mehr einwandfrei funktionieren. Beispielsweise kann der Ausfall der Zeitsynchronisation bei der Nutzung von Kerberos irgendwann zur Folge haben, dass Benutzer sich nicht mehr am Betriebssystem oder an Diensten anmelden können.

Aufbauend auf das Modul [ISi-LANA], welches die Absicherung der unteren drei Schichten des TCP/IP Referenzmodells sicherstellt, wird durch die ISi-Server-Studie die Basis eines sicheren Servers geschaffen. Ergänzt wird dies noch durch die spezifischen Module [ISi-Mail-Server] und [ISi-Web-Server], die Maßnahmen für spezifische Applikationen vorstellen.

7 Anhang

7.1 Abdeckungsmatrix

In den Abschnitten 3 und 4 wurden zahlreiche Empfehlungen für die Umsetzung einer sicheren Grundarchitektur für Server aufgeführt. Der Abschnitt 5 erläuterte Gefährdungen, denen ein Server ausgesetzt ist und die Maßnahmen der Grundarchitektur, die gegen diese Gefährdungen schützen. Als Ergänzung wurden zahlreiche Varianten aufgeführt, die eine Vereinfachung der Grundarchitektur darstellen, oder weitere Sicherheits-Komponenten aufgezeigt, die für den hohen Schutzbedarf eingesetzt werden können. Der folgende Abschnitt bietet eine Gegenüberstellung der Maßnahmen und Varianten aus den Abschnitten 3 bis 5 zu den Gefährdungen aus Abschnitt 5.

In Tabelle 2 sind die Empfehlungen für den normalen Schutzbedarf zusammengefasst. Die Tabelle 3 zeigt eine entsprechende Matrix für den hohen Schutzbedarf. Verbindliche Maßnahmen sind mit „X“ und optionale Maßnahmen mit „(X)“ gekennzeichnet.

Gefährdung	Abdeckungsmatrix für den normalen Schutzbedarf	Ausnutzen von Schwachstellen in Diensten	Erraten und/oder Manipulation von Passwörtern	Unautorisierter Zugriff auf Dienste	Zugriff auf verwaiste Benutzerkonten	Unbefugter Zugriff auf Schnittstellen zur Fernadministration	Einsatz veralteter Software	Mitlesen von Administrationstätigkeiten	Zugriff auf getrennte Netzsegmente durch fehlerhafte Virtualisierung	Unbefugter Zugriff auf lokalen Massenspeicher	Unbefugter Zugriff auf das Speichernetz	Unbefugter Zugriff auf die Backup-Medien	Unbefugter Zugriff auf Daten aufgrund umfangreicher Berechtigungen	Unerlaubtes Starten von ausführbaren Dateien	Manipulation der Systemuhrzeit	Manipulation von Boot-Code / Bootloader durch ein Schadprogramm	Manipulation von Dateien durch Schadprogramme	Manipulation von Dateien	Nutzung von kompromitierten Installationsmedien	Nicht-Verfügbarkeit durch einen Defekt der Hardware	Datenverlust aufgrund einer defekten Festplatte	Ausfall der Energieversorgung	Datenverlust durch mangelnde Speicherkapazität	Datenverlust durch Löschen oder Ändern von Daten	Nicht-Verfügbarkeit des Virtualisierungsservers
	Empfehlung																								
	Grundarchitektur und Grundkonfiguration																								
	Minimalinstallation	x		x																					
	Monitoring																				x		x		
	Protokollierung																								
	Speichernetz										x													x	
	Zeitsynchronisation														x										
	Patch- und Änderungsmanagement	x					x														x				
	Datensicherung																				x	x			x
	Benutzerverwaltung	x	x		x								x	x											x
	Virenschutz															x	x								
	Integritätsprüfung															x	x		x		x		x		
	Notfallvorsorgekonzept																				x		x	x	
	Vorgelagerte Paketfilter			x																					
	Kapselung und Isolation								x																
	Zutrittskontrolle									x		x													
	Out-of-Band Management							x																	
	Separate phys. Netzwerkkarten								x																
x	Virtualisierung mit redundanten Komponenten																								
	Einsatz von RAID																					x			
	Einsatz einer USV																						x		
	Speicherschutzmechanismen	x																							
	Speicherrandomisierung	x																							
	Einsatz eines Journaling-Dateisystems																					x	x		
	Bezug der Installationsmedien von autorisierter Quelle																			x					
	Prüfen der Installationsmedien mittels Prüfsummen																			x					
	Kryptografisch gesicherte Zugänge (s. ISi-LANA)				x																				
	Varianten																								
	Lokale Benutzerverwaltung					(x)																			
	Updates direkt vom Hersteller						(x)																		
	Netz ohne Management-Zone							(x)																	
	Virtual. von Servern aus unterschied. Netzsegm.								(x)																
	Ausbau der Festplatte bei Wartungsarbeiten									(x)															
	Verzicht auf Virenschutz																(x)								
	Verzicht auf Integritätsprüfung																(x)								
	Weglassen von RAID																					(x)			
	Verzicht auf den Einsatz einer USV																						(x)		
(x)	Nutzung von Live Migration																								

Tabelle 2: Abdeckungsmatrix für den normalen Schutzbedarf

Gefährdung	Abdeckungsmatrix für den hohen Schutzbedarf	Ausnutzen von Schwachstellen in Diensten	Erraten und/oder Manipulation von Passwörtern	Unautorisierter Zugriff auf Dienste	Zugriff auf verwaiste Benutzerkonten	Unbefugter Zugriff auf Schnittstellen zur Fernadministration	Einsatz veralteter Software	Mitlesen von Administrationstätigkeiten	Zugriff auf getrennte Netzsegmente durch fehlerhafte Virtualisierung	Unbefugter Zugriff auf lokalen Massenspeicher	Unbefugter Zugriff auf das Speichernetz	Unbefugter Zugriff auf die Backup-Medien	Unbefugter Zugriff auf Daten aufgrund umfangreicher Berechtigungen	Unerlaubtes Starten von ausführbaren Dateien	Manipulation von Dateien durch Schadprogramme	Manipulation von Boot-Code oder Bootloader durch ein Schadprogramm	Manipulation der Systemuhrzeit	Manipulation von Dateien	Nutzung von kompromittierten Installationsmedien	Nicht-Verfügbarkeit durch einen Defekt der Hardware	Datenverlust aufgrund einer defekten Festplatte	Ausfall der Energieversorgung	Datenverlust durch mangelnde Speicherkapazität	Datenverlust durch Löschen oder Ändern von Daten	Nicht-Verfügbarkeit des Virtualisierungsservers
	Empfehlung																									
	Zwei-Faktor-Authentisierung		X			X					X							X								
	Einsatz ausschließlich verschlüsselter Protokolle in Out-of-Band Management							X																		
	Virtualisierung von Servern mit hohem Schutzbedarf								X																	
	Festplattenverschlüsselung									X			X													
	Festplattenverschlüsselung mit TPM ohne Passwortschutz									X						X										
	Festplattenverschlüsselung mit TPM und Passwortschutz																									
	Zerstörung der Festplatte bei Entsorgung									X																
	Authentisierung bei Zugriff auf das Speichernetz										X															
	Verschlüsselung von Massenspeicher-protokollen										X															
	Verschlüsselung der Datensicherung											X														
	Ausführen von Dateien unter Linux / Unix verhindern													X												
	Ausführen von Dateien unter Windows													X												
	Integritätsschutz für alle Dateien														X			X								
	Einsatz einer Dateisignatur														X											
	Absicherung des Bootvorgangs mittels TPM																									
	Gesicherte Kommunikation mit einem NTP-Server																X									
	Einsatz redundanter Komponenten																				X					
	Einsatz redundanter Server-Systeme																				X					

Tabelle 3: Abdeckungsmatrix für den hohen Schutzbedarf

7.2 Varianten der Grundarchitektur

In Abschnitt 3 wurde eine sichere Grundarchitektur für Server in einer großen Organisation mit normalem Schutzbedarf vorgestellt.

Darüber hinaus wurden in Abschnitt 5 verschiedene Architektur- und Konfigurationsvarianten beschrieben. Einige dieser Varianten ergänzen die Grundarchitektur und erhöhen den Schutz, sind aber in der Regel mit höheren Aufwänden in der Realisierung oder im Betrieb verbunden. Andere Varianten vereinfachen die Grundarchitektur oder senken den Aufwand für deren Umsetzung, bieten jedoch einen geringeren Schutz. Ob eine Vereinfachung der Grundarchitektur und die damit verbundene Erhöhung des Restrisikos tragbar ist, muss im Einzelfall entschieden werden.

Im folgenden Anhang werden einige Beispiele vorgestellt, wie die Architektur an eine veränderte Unternehmensgröße oder einen veränderten Schutzbedarf angepasst werden kann und welche Konsequenzen dies für die Gefährdungslage hat.

Im Fokus stehen dabei die Änderungen, die sich auf den Server beziehen. Änderungen, die das Sicherheits-Gateway und die Internet-Anbindung betreffen, sind in [ISi-LANA] und [ISi-Web-Server] beschrieben.

Für jedes vorgestellte Szenario werden Annahmen getroffen, die beispielhaft eine kleine, mittelgroße bzw. große Organisation kennzeichnen. Aufbauend auf diesen Annahmen werden Änderungsmöglichkeiten aufgegriffen, die bereits als Varianten in Abschnitt 5 vorgestellt worden sind. Die Änderung der Gefährdungslage des Unternehmens wird jeweils in einer Tabelle dargestellt. Die Änderung der Gefährdungslage des Unternehmens durch die Abweichung von der Grundarchitektur wird jeweils in einer Tabelle dargestellt.

In der Tabelle bedeutet „↑↑“ deutlich erhöhte Gefährdung, „↑“ erhöhte Gefährdung, „↔“ Gefährdung, wie bei Verwendung der Grundarchitektur, „↑↓“ teils erhöhte, teils verringerte Gefährdung, „↓“ verringerte Gefährdung und „↓↓“ deutlich verringerte Gefährdung.

Die konkrete Kombination der eingesetzten Varianten muss unter Berücksichtigung der Gewichtung der Schutzziele ausgewählt werden. Maßnahmen, die einen besseren Schutz der Vertraulichkeit bewirken, können unter Umständen eine zusätzliche Gefährdung der Verfügbarkeit zur Folge haben. Geht z. B. das Passwort für eine Verschlüsselung verloren, sind die damit geschützten Daten nicht verfügbar.

7.2.1 Kleines Unternehmen

Annahmen

Für ein kleines Unternehmen werden folgende Annahmen getroffen:

- es handelt sich um keine Behörde,
- wenige (5-10) Clients und Server im internen Netz,
- kein Management- und Überwachungsnetz vorhanden,
- kein Patch- und Änderungsmanagement vorhanden.

Änderungen der Grundarchitektur für den normalen Schutzbedarf

Für den normalen Schutzbedarf können folgende Varianten verwendet werden:

- Aktualisierungen für die Server (Betriebssystem + Dienste) werden direkt vom Server des Herstellers heruntergeladen. Auf eine zentrale Softwareverteilung kann verzichtet werden (siehe Variante 5.1.6.A).
- Bei dem Einsatz eines Virtualisierungsservers können Server aus unterschiedlichen Netzsegmenten virtualisiert werden (siehe Variante 5.2.2.A).
- Verzicht auf Virenschutz auf Server-Systemen (siehe Variante 5.3.1.A).
- Auf eine Integritätsprüfung kann verzichtet werden (siehe Variante 5.3.1.B).
- Auf eine zentrale Benutzerverwaltung über einen Verzeichnisdienst kann verzichtet werden (siehe Variante 5.1.4.A).
- Auf ein Notfallvorsorgekonzept kann verzichtet werden.
- Weglassen von RAID (siehe Variante 5.4.2.A)
- Verzicht auf den Einsatz einer unterbrechungsfreien Stromversorgung (siehe Variante Variante 5.4.3.A)

Konsequenzen für die Gefährdung eines kleinen Unternehmens mit normalem Schutzbedarf

Bedrohung	*Gefährdung*	*Bemerkung*
Systemhoheit	↑	Durch die separate Verwaltung der Benutzerkonten auf den Servern ist mit einem höheren Aufwand zu rechnen. Der Softwarestand der einzelnen Server kann nicht zentral eingesehen werden. Sicherheitshinweise beziehen sich in der Regel auf bestimmte Versionsstände von Betriebssystem und Software. Um festzustellen, welche Server von den Sicherheitslücken betroffen sind, muss jeder Server manuell geprüft werden. Werden bei der Virtualisierung Server aus unterschiedlichen Netzsegmenten zusammengeführt, dann können Konfigurationsfehler oder auch Softwarefehler die Gefährdung weiter erhöhen.
Vertraulichkeit	↑	Durch die Gefährdung der Systemhoheit sowie das Fehlen eines Virenschutzes kann es zur Beeinträchtigung der Vertraulichkeit kommen.
Integrität	↑↑	Durch das Fehlen der Integritätsprüfung können Modifikationen von Konfigurationseinträgen nicht kurzfristig erkannt werden. Durch das Fehlen eines Virenschutzes auf den Servern besteht das Risiko, dass Schadprogramme auf den Servern nicht erkannt werden.
Verfügbarkeit	↑	Werden Aktualisierungen automatisch vom Hersteller geladen, können diese vorher nicht getestet werden. Dies kann die Verfügbarkeit von Betriebssystem und Diensten beeinträchtigen. Keine Notfallstrategie beim Ausfall eines Servers durch das Fehlen eines Notfallkonzeptes. Wird das RAID-System weggelassen, kann es bei Ausfall der Festplatte zu einem Verlust der Daten kommen. Es kann ebenso zu Datenverlust kommen, wenn auf den Einsatz einer unterbrechungsfreien Stromversorgung verzichtet wird.

Tabelle 4: Konsequenzen für ein kleines Unternehmen mit normalem Schutzbedarf

Änderungen der Grundarchitektur für den hohen Schutzbedarf

Für den hohen Schutzbedarf können die folgenden Varianten verwendet werden:

- Bei hohem Schutzbedarf bzgl. Vertraulichkeit:
  - Variante 5.2.3.A für hohen Schutzbedarf: Festplattenverschlüsselung
- Bei hohem Schutzbedarf bzgl. Verfügbarkeit:
  - Variante 5.4.1.B für hohen Schutzbedarf: Einsatz redundanter Server-Systeme

Konsequenzen für die Gefährdung eines kleinen Unternehmens mit hohem Schutzbedarf

Bedrohung	*Gefährdung*	*Bemerkung*
Systemhoheit	↔	Kein erhöhtes Risiko.
Vertraulichkeit	↓	Durch die Verschlüsselung von Datenträgern sind die Daten vor Verlust bzw. Diebstahl geschützt.
Integrität	↔	Kein erhöhtes Risiko.
Verfügbarkeit	↓	Bei dem Einsatz von Verschlüsselung ist die Verfügbarkeit von Daten bei Verlust des Schlüssels bedroht. Durch den Einsatz redundanter Komponenten wird die Verfügbarkeit der Server erhöht.

Tabelle 5: Konsequenzen für ein kleines Unternehmen mit hohem Schutzbedarf

7.2.2 Mittelgroßes Unternehmen

Annahmen

Für ein mittelgroßes Unternehmen werden folgende Annahmen getroffen:

- mittlere Anzahl (100-400) von Clients und Servern im internen Netz,
- zentrale Server und Management-Systeme vorhanden.

Änderungen der Grundarchitektur für den normalen Schutzbedarf

Für den normalen Schutzbedarf genügen die Maßnahmen der Grundarchitektur. Es können noch die folgenden Varianten als Ergänzung dienen:

- Bei dem Einsatz eines Virtualisierungsservers können Server aus unterschiedlichen Netzsegmenten virtualisiert werden (siehe Variante 5.2.2.A).

Konsequenzen für die Gefährdung eines mittleren Unternehmens mit normalem Schutzbedarf

Bedrohung	*Gefährdung*	*Bemerkung*
Systemhoheit	↑	Werden bei der Virtualisierung Server aus unterschiedlichen Netzsegmenten zusammengeführt, dann können Konfigurationsfehler oder auch Softwarefehler die Gefährdung weiter erhöhen.
Vertraulichkeit	↔	Kein erhöhtes Risiko.
Integrität	↔	Kein erhöhtes Risiko.
Verfügbarkeit	↔	Kein erhöhtes Risiko.

Tabelle 6: Konsequenzen für ein mittelgroßes Unternehmen mit normalem Schutzbedarf

Änderungen der Grundarchitektur für den hohen Schutzbedarf

Für den hohen Schutzbedarf können die folgenden Varianten verwendet werden:

- Bei hohem Schutzbedarf bzgl. Vertraulichkeit:
  - Variante 5.2.3.A für hohen Schutzbedarf: Festplattenverschlüsselung
  - Variante 5.2.5.A für hohen Schutzbedarf: Verschlüsselung der Datensicherung
  - Variante 5.2.7.B für hohen Schutzbedarf: Ausführen von Dateien unter Windows verhindern
- Bei hohem Schutzbedarf bzgl. Integrität:
  - Variante 5.3.1.C für hohen Schutzbedarf: Erweiterung der Integritätsprüfung auf alle Dateien
  - Variante 5.3.1.D für hohen Schutzbedarf: Einsatz einer Dateisignatur
  - Variante 5.3.3.A für hohen Schutzbedarf: Gesicherte Kommunikation mit einem NTP-Server
  - Variante 5.3.2.A für hohen Schutzbedarf: Absicherung des Bootvorgangs mittels TPM
- Bei hohem Schutzbedarf bzgl. Verfügbarkeit:
  - Variante 5.4.1.A für hohen Schutzbedarf: Einsatz redundanter Komponenten

- Variante 5.4.1.B für hohen Schutzbedarf: Einsatz redundanter Server-Systeme

Konsequenzen für die Gefährdung eines mittleren Unternehmens mit hohem Schutzbedarf

Bedrohung	*Gefährdung*	*Bemerkung*
Systemhoheit	↔	Kein erhöhtes Risiko.
Vertraulichkeit	↓	Durch die Verschlüsselung von Datenträgern und Backup-Medien sind die Daten vor Verlust bzw. Diebstahl geschützt.
Integrität	↓	Durch die Erweiterung der Integritätsprüfung wird eine bessere Integritäts-sicherung des Servers erzielt.
Verfügbarkeit	↓	Bei dem Einsatz von Verschlüsselung ist die Verfügbarkeit von Daten bei Verlust des Schlüssels bedroht. Durch den Einsatz redundanter Komponenten wird die Verfügbarkeit der Server erhöht.

Tabelle 7: Konsequenzen für ein mittelgroßes Unternehmen mit hohem Schutzbedarf

7.2.3 Großes Unternehmen

Annahmen

Für ein großes Unternehmen werden folgende Annahmen getroffen:

- große Anzahl (>500) von Clients und Servern im internen Netz,
- stark ausgeprägtes zentrales Management der IT-Infrastruktur mit vielen Servern,
- Patch- und Änderungsmanagements vorhanden.

Änderungen der Grundarchitektur für den normalen Schutzbedarf

Für den normalen Schutzbedarf genügen die Maßnahmen der Grundarchitektur. Es können noch die folgenden Varianten als Ergänzung dienen:

- Variante 5.2.2.A für normalen Schutzbedarf: Virtualisierung von Servern aus unterschiedlichen Netzsegmenten im internen Netz

Konsequenzen für die Gefährdung eines großen Unternehmens mit normalem Schutzbedarf

Bedrohung	*Gefährdung*	*Bemerkung*
Systemhoheit	↑	Werden bei der Virtualisierung Server aus unterschiedlichen Netzsegmenten zusammengeführt, dann können Konfigurationsfehler oder auch Softwarefehler die Gefährdung weiter erhöhen.
Vertraulichkeit	↔	Kein erhöhtes Risiko.
Integrität	↔	Kein erhöhtes Risiko.
Verfügbarkeit	↔	Kein erhöhtes Risiko.

Tabelle 8: Konsequenzen für ein großes Unternehmen mit normalem Schutzbedarf

Änderungen der Grundarchitektur für den hohen Schutzbedarf

Für den hohen Schutzbedarf können die folgenden Varianten verwendet werden:

- Bei hohem Schutzbedarf bzgl. der Systemhoheit:
  - Variante 5.1.2.A für hohen Schutzbedarf: Zwei-Faktor-Authentisierung
- Bei hohem Schutzbedarf bzgl. Vertraulichkeit:
  - Variante 5.2.3.A für hohen Schutzbedarf: Festplattenverschlüsselung
  - Variante 5.2.3.E für hohen Schutzbedarf: Physische Zerstörung der Festplatte bei Entsorgung
  - Variante 5.2.4.A für hohen Schutzbedarf: Erforderliche Authentisierung bei Zugriff auf das Speichernetz
  - Variante 5.2.4.B für hohen Schutzbedarf: Verschlüsselung von Massenspeicherprotokollen
  - Variante 5.2.5.A für hohen Schutzbedarf: Verschlüsselung der Datensicherung
  - Variante 5.2.7.B für hohen Schutzbedarf: Ausführen von Dateien unter Windows verhindern
- Bei hohem Schutzbedarf bzgl. Integrität:

- Variante 5.3.1.C für hohen Schutzbedarf: Erweiterung der Integritätsprüfung auf alle Dateien
- Variante 5.3.1.D für hohen Schutzbedarf: Einsatz einer Dateisignatur
- Variante 5.3.3.A für hohen Schutzbedarf: Gesicherte Kommunikation mit einem NTP-Server
- Variante 5.3.2.A für hohen Schutzbedarf: Absicherung des Bootvorgangs mittels TPM

– Bei hohem Schutzbedarf bzgl. Verfügbarkeit:

- Variante 5.4.1.A für hohen Schutzbedarf: Einsatz redundanter Komponenten
- Variante 5.4.1.B für hohen Schutzbedarf: Einsatz redundanter Server-Systeme

Konsequenzen für die Gefährdung eines großen Unternehmens mit hohem Schutzbedarf

Bedrohung	*Gefährdung*	*Bemerkung*
Systemhoheit	↓↓	Durch den Einsatz einer Zwei-Faktor-Authentisierung werden Angriffe auf die Zugangsmechanismen der Server erschwert.
Vertraulichkeit	↓↓	Durch die Verschlüsselung von Datenträgern und Backup-Medien sind die Daten vor Verlust bzw. Diebstahl geschützt. Datenträger werden bei ihrer Entsorgung zerstört, sodass die Daten auch im Nachhinein nicht von einem Angreifer rekonstruiert werden können.
Integrität	↓	Durch die Erweiterung der Integritätsprüfung wird eine bessere Integritäts-sicherung des Servers erzielt.
Verfügbarkeit	↓	Bei dem Einsatz von Verschlüsselung ist die Verfügbarkeit von Daten bei Verlust des Schlüssels bedroht. Durch den Einsatz redundanter Komponenten wird die Verfügbarkeit der Server erhöht.

Tabelle 9: Konsequenzen für ein großes Unternehmen mit hohem Schutzbedarf

8 Glossar

Active Directory

Verzeichnisdienst zur zentralen Benutzerverwaltung von Microsoft Windows Servern. Der Zugriff auf das Active Directory kann u. a. auch über LDAP erfolgen.

Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computer-Netze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzer-Kennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

Angriff (attack [engl.])

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Anwendungsschicht (application layer [engl.])

Die Anwendungsschicht ist die oberste Schicht im TCP/IP-Referenzmodell. Sie umfasst alle Protokolle, die von Anwendungsprogrammen, z. B. Browser oder E-Mail-Client, verarbeitet und für den Austausch anwendungsspezifischer Daten genutzt werden. Beispiele für Protokolle der Anwendungsschicht sind das Hypertext Transfer Protocol (HTTP) oder das Simple Mail Transfer Protocol (SMTP).

ASLR (Address Space Layout Randomization [engl.])

Schutzmechanismus zur Vermeidung von Buffer Overflow-Angriffen durch die zufällige Anordnung von Adressbereichen für ausgeführte Programme.

ATX (Advanced Technology Extended [engl.])

Norm für Gehäuse, Netzteile, Hauptplatinen und Steckkarten.

Authentisierung (authentication [engl.])

Unter einer Authentisierung versteht man die Vorlage eines Nachweises eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

Authentizität (authenticity [engl.])

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Autorisierung (authorization [engl.])

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

Bedrohung (threat [engl.])

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen bedrohen kann, wodurch dem Besitzer der Informationen ein Schaden entsteht.

Benutzer-Kennung (user account [engl.])

Die Benutzer-Kennung ist der Name, mit dem sich der Benutzer einem IT-System gegenüber authentisiert. Dies kann z. B. der tatsächliche Name sein, ein Pseudonym, eine Abkürzung oder eine automatisch vergebene Kombination aus Buchstaben oder Ziffern.

Betriebssystem (operating system [engl.])

Das Betriebssystem ist ein Steuerungsprogramm, das es dem Benutzer ermöglicht, seine Dateien zu verwalten, angeschlossene Geräte (z. B. Drucker, Festplatte) zu kontrollieren oder Programme zu starten. Weit verbreitet sind z. B. Windows, Linux oder MacOS.

BIOS (Basic Input Output System [engl.])

Firmware für x86-basierte Computer.

Browser [engl.]

Mit Browser (von "to browse", auf deutsch: schmökern, blättern, umherstreifen) wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (Federal Office for Information Security [engl.])

Bundesbehörde im Geschäftsbereich des Bundesministerium des Innern.

Client [engl.]

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme eines Servers zugreift.

Controller

Physische Steuereinheit innerhalb eines Servers, die für den Datenaustausch mit anderen Schnittstellen verwendet wird (z. B. RAID-Controller, Festplatten-Controller, SCSI-Controller, etc.).

Datenschutz

Mit Datenschutz wird der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Datensicherheit

Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist IT-Sicherheit.

Datensicherung (backup [engl.])

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren. Ordnungsgemäße Datensicherung bedeutet, dass die getroffenen Maßnahmen in Abhängigkeit von der Datensensitivität eine sofortige oder kurzfristige Wiederherstellung des Zustands von Systemen, Daten, Programmen oder Prozeduren nach erkannter Beeinträchtigung der Verfügbarkeit, Integrität oder Konsistenz aufgrund eines schadenswirkenden Ereignisses ermöglichen. Die Maßnahmen umfassen dabei mindestens die Herstellung und Erprobung der Rekonstruktionsfähigkeit von Kopien der Software, Daten und Prozeduren in definierten Zyklen und Generationen.

DHCP (Dynamic Host Configuration Protocol [engl.])

Protokoll zur automatischen Vergabe der Netzwerkkonfiguration (u. a. IP-Adresse, Netzmaske, Routing, etc.).

DNS (Domain Name System [engl.])

Das Domain Name System übersetzt alphanumerische Adressnamen (z. B. www.bsi.bund.de) in numerische Adressen (z. B. 194.95.177.86). Auch eine Übersetzung in die umgekehrte Richtung ist mit dem DNS möglich. Alphanumerische Namen für Rechner sind für die Benutzer einfach zu behalten und einzugeben. Da allerdings IPv4 und IPv6 Adressen in numerischer Form verlangen, ist eine Adressumsetzung durch das DNS notwendig.

DoS (Denial of Service [engl.])

Angriffe, mit dem Ziel, die Verfügbarkeit von IT zu schädigen.

EFI (Extensible Firmware Interface [engl.])

Firmware für x86-basierte Computer. Gilt als Nachfolger des BIOS und wurde speziell für die Anforderungen an 64-Bit-Systeme entwickelt.

ESP (Executable Space Protection [engl.])

Speicherschutztechnologie, die die Ausführung von Programmen aus dafür nicht zugelassenen Speicherbereichen verhindert.

Fibre Channel

Massenspeicherprotokoll zur Anbindung von Serversystemen an ein Storage Area Network (SAN).

Firmware

Als Firmware wird die Betriebssoftware von elektronischen Komponenten bezeichnet. Analog zu dem Betriebssystem eines Computers, das die Zusammenarbeit aller Komponenten eines Rechners koordiniert, ist die Firmware auf den einzelnen Hardware-Komponenten installiert und sorgt für den korrekten Betrieb der Hardware-Komponente.

Flash [engl.]

Mit dem Programm Flash können interaktive Vektorgrafik, Animation und Präsentation erstellt werden. Für die Betrachtung der Filme ist ein kostenloses Plug-In erforderlich. Flash zählt zu den Aktiven Inhalten.

FTP (File Transfer Protocol [engl.])

Das File Transfer Protocol umfasst Funktionen, mit denen man Dateien auf einfache Weise zwischen zwei Rechnern austauschen kann.

Gefährdung

Eine Gefährdung ist eine Bedrohung, die konkret auf ein Objekt über eine Schwachstelle einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. So sind beispielsweise Computer-Viren eine Bedrohung oder eine Gefährdung für Anwender, die im Internet surfen. Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwender prinzipiell durch Computer-Viren im Internet bedroht sind. Der Anwender, der eine virenbefallene Datei herunterlädt, wird von dem Computer-Virus gefährdet, wenn sein Computer anfällig für diesen Typ Computer-Virus ist. Für Anwender mit einem wirksamen Schutzprogramm, einer Konfiguration, die das Funktionieren des Computer-Virus verhindert, oder einem Betriebssystem, das den Virencode nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

GUI (Graphical User Interface [engl.])

Die "grafische Bedieneroberfläche", d. h. Möglichkeit mittels Maus an einem virtuellen Arbeitsplatz auf dem Monitor zu arbeiten.

HBA (Host Bus Adapter [engl.])

Ein Host Bus Adapter wird für die Anbindung eines Rechnersystems an ein SAN (z. B. für Fibre Channel oder iSCSI) verwendet. Als Übertragungsprotokoll zum SAN kommt hierzu z. B. TCP/IP oder Fibre Channel zum Einsatz.

Hot Swap

Hot Swap bezeichnet die Möglichkeit, System-Komponenten (z. B. Netzteil, Festplatte oder auch Arbeitsspeicher) im laufenden Betrieb des Server-Systems zu wechseln ohne den Server herunterzufahren.

HTTP (Hypertext Transfer Protocol [engl.])

Das Hypertext Transfer Protocol dient zur Übertragung von Daten - meist Webseiten - zwischen einem HTTP-Server und einem HTTP-Client, also z. B. einem Browser. Die Daten werden über Uniform Resource Locators (URL) eindeutig bezeichnet. URLs werden meist in der Form Protokoll://Rechner/Pfad/Datei angegeben. Protokoll steht dabei für Protokolle der Anwendungsschicht, Rechner für den Namen oder die Adresse des Servers und der Pfad der Datei gibt den genauen Ort der Datei auf dem Server an. Ein Beispiel für eine URL ist http://www.bsi.bund.de/fachthem/sinet/index.htm.

HTTPS (HTTP secure [engl.])

Protokoll zur sicheren Übertragung von HTML-Seiten im Internet. SSL/TLS dient dabei zur Absicherung der Client-Server-Kommunikation.

IMAP (Internet Message Accept Protocol [engl.])

Protokoll zum Transfer von E-Mails zwischen einem E-Mail-Client und einem E-Mail-Server. Im Gegensatz zu POP3 ist IMAP ein Online-Protokoll, welches die E-Mails nur temporär (zum Lesen) herunterlädt.

Integrität (integrity [engl.])

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. Integrität ist ein Grundwert der IT-Sicherheit.

IP (Internet Protocol [engl.])

Verbindungsloses Protokoll der Internet-Schicht im TCP/IP-Referenzmodell. Ein IP-Header enthält in der Version IPv4 u. a. zwei 32-Bit-Nummern (IP-Adressen) für Ziel und Quelle der kommunizierenden Rechner.

IPMI (Intelligent Platform Management Interface [engl.])

Herstellerübergreifende Schnittstelle für Hardware-Management im Serverbereich.

IPv4 (Internet Protocol Version 4 [engl.])

Das Internet Protocol Version 4 ist ein verbindungsloses Protokoll der Vermittlungsschicht und erlaubt den Austausch von Daten zwischen zwei Rechnern ohne vorherigen Verbindungsaufbau. IPv4 setzt nicht voraus, dass das darunterliegende Netz Fehlererkennung ausführt. Ferner verfügt es über keine Verlässlichkeits- oder Flusssteuerungsmechanismen. Die meisten dieser Probleme gibt IPv4 an die nächsthöhere Schicht (die Transportschicht) weiter.

IPv6 (Internet Protocol Version 6 [engl.])

Das Internet Protocol Version 6 ist die Nachfolgeversion von IPv4 und soll dieses ablösen, da es u. a. die Zahl der verfügbaren Rechneradressen stark erweitert und Maßnahmen zum Schutz der übertragenen Daten vor dem Verlust der Vertraulichkeit, der Integrität und der Authentizität umfasst. Die Sicherungsmaßnahmen sind unter dem Namen "IPSec" zusammengefasst. IPSec definiert Sicherungsdienste, die durch zwei zusätzliche Header, den "IP Authentication Header" (AH) und den Header "IP Encapsulating Security Payload" (ESP) realisiert werden. Mithilfe der Header können unterschiedliche kryptografische Algorithmen eingebunden werden. IPSec erlaubt die Integration der Header in Datagramme des IPv4 sowie des IPv6. AH- und ESP-Header können einzeln oder gemeinsam in einem IP-Datagramm auftreten. Die Sicherheitsmechanismen schützen IPv4/IPv6 und die darüberliegenden Protokolle.

IT-Grundschutz

IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von IT-Verbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen für IT-Systeme mit normalem Schutzbedarf umgesetzt sind. Für Systeme mit hohem oder sehr hohem Schutzbedarf sind möglicherweise darüber hinausgehende Sicherheitsmaßnahmen notwendig.

IT-Sicherheit (IT Security [engl.])

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

IT-Sicherheitsbeauftragter

Personen mit eigener Fachkompetenz zur IT-Sicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde, die für alle IT-Sicherheitsfragen, Mitwirkung im IT-Sicherheitsprozess und IT-Sicherheitsmanagement-Team zuständig sind, die IT-Sicherheitsleitlinie, das IT-Sicherheitskonzept und andere Konzepte z. B. für Notfallvorsorge koordinierend erstellen und deren Umsetzung planen und überprüfen.

IQN (iSCSI Qualified Name [engl.])

Der IQN (iSCSI Qualified Name) dient zur internen Verwaltung und Zuordnung der Geräte in einem iSCSI SAN.

Jumbo Frames

Innerhalb von Ethernet ist die maximale Paketgröße 1518 Bytes. Größere Pakete werden als Jumbo Frames bezeichnet. Um eine höhere Datenübertragung zu erreichen, wird durch den Einsatz von Jumbo Frames die maximale Paketgröße auf bis zu 9000 Bytes erhöht. Eingesetzt wird dies z. B. in einem Ethernet-SAN.

Kryptografie

Mathematisches Fachgebiet, das sich mit Methoden zum Schutz von Informationen befasst (u. a. mit Vertraulichkeit, Integrität und Authentizität von Daten).

LDAP (Lightweight Directory Access Protocol [engl.])

Netzwerkprotokoll für den Zugriff auf einen Verzeichnisdienst. Dieses Protokoll wird z. B. für den Zugriff auf eine zentrale Benutzerverwaltung verwendet.

LUN (Logical Unit Number [engl.])

Mit Hilfe der Logical Unit Number (LUN) wird eine Zugriffssteuerung in einem SAN realisiert. Der physische Speicher des Festplattensubsystems wird dabei in mehrere logische Festplatten unterteilt, auf die mittels der LUN von einem Client aus zugegriffen werden kann.

LUN Masking

Mittels LUN Masking ist es möglich, die Sichtweise von LUNs in einem SAN auf bestimmte Hosts einzuschränken. Dadurch kann man in iSCSI oder Fibre Channel Netzen konfigurieren, welcher Rechner welches Massenspeichersystem sehen darf.

MAC (Media Access Control [engl.])

Hardware-Adresse von Netzadaptern zur eindeutigen Adressierung innerhalb von Ethernet Netzwerken.

Multipathing

Anbindung eines Servers an ein SAN über mehr als einen HBA. Die HBAs sollen hierbei über unterschiedliche Netz-Komponenten (Pfade) angebunden werden, um beim Ausfall einer einzelnen Komponente einen Totalausfall vorzubeugen.

NAS (Network Attached Storage [engl.])

Als NAS bezeichnet man einen zentralen Netzwerkspeicher, der z. B. mehrere durch RAID-Konfiguration zusammengeschaltete physische Festplatten über das Netzwerk zur Verfügung stellt.

NFS (Network File System [engl.])

Netzwerkdateisystem für den Zugriff von Computern auf NAS-Systeme. NFS wird vorwiegend von Computern mit dem Betriebssystem Linux/Unix eingesetzt.

NTP (Network Time Protocol [engl.])

Protokoll zur Zeitsynchronisation über das Internet oder lokale Netz.

Passwort

Geheimes Kennwort, das Daten, Rechner, Programme u. a. vor unerlaubtem Zugriff schützt.

Patch [engl.]

Ein Patch (vom englischen "patch", auf deutsch: Flicken) ist ein kleines Programm, das Software-Fehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

POP (Post Office Protocol [engl.])

Verbreitetes Protokoll für das Herunterladen von E-Mails von einem Mailserver auf einen PC.

POP3 (Post Office Protocol [engl.])

Protokoll zum Transfer von E-Mails zwischen einem E-Mail-Client und E-Mail-Server. Im Gegensatz zu IMAP ist POP3 ein Offline-Protokoll, welches die E-Mails herunterlädt und auf dem Client speichert.

Proxy

Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Proxy-Server

Ein Proxy-Server agiert gegenüber einem Client als Stellvertreter des eigentlichen Servers und gegenüber dem Server als Stellvertreter des Clients. Der Client kommuniziert nur mit dem Proxy-Server. Der Proxy-Server leitet also

Prüfsumme (checksum [engl.])

In der Informatik ist eine Prüfsumme eine einfache Maßnahme zur Gewährleistung von Datenintegrität bei der Datenübermittlung oder -speicherung.

RAID (Redundant Array of Independent Disks [engl.])

Mittels RAID können mehrere lokale physische Festplatten eines Servers zu einer logischen Speichereinheit zusammengefasst werden und dem Betriebssystem zur Verfügung gestellt werden. Die Konfiguration erfolgt über sogenannte RAID-Level, die sowohl die Datensicherheit als auch die Performance von Lese- und Schreiboperationen erhöhen kann.

RDP (Remote Desktop Protocol [engl.])

Fernwartungsprotokoll für den Zugriff auf Computer.

Restrisiko (residual risk [engl.])

Risiko, das grundsätzlich bleibt, auch wenn Maßnahmen zum Schutz des IT-Einsatzes ergriffen worden sind.

Risiko (risk [engl.])

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden

oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

Router [engl.]

Ein (IP-)Router ist ein Vermittlungsrechner, der Netze auf IP-Ebene koppelt und Wegewahlentscheidungen anhand von IP-Protokollschicht-Informationen trifft. Router trennen Netze auf der Netzzugangsschicht und begrenzen daher die Broadcast-Domäne eines Ethernets.

SAN (Storage Area Network [engl.])

Hochperformantes Netzwerk, welches Massenspeicher für Serversysteme zur Verfügung stellt. Der Zugriff auf ein SAN erfolgt über Massenspeicherprotokolle wie z. B. iSCSI oder Fibre Channel.

SAN-Zoning

Mit SAN-Zoning wird eine logische Zugriffskontrolle innerhalb eines SANs ermöglicht (vergleichbar mit einem VLAN).

SAS (Serial Attached SCSI [engl.])

Schnittstelle für die Verbindung und Datenübertragung zwischen Peripheriegeräten (z. B. Festplatten). Der Datenaustausch erfolgt bei SAS über eine serielle Schnittstelle.

Schutzbedarf (protection requirements [engl.])

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Schwachstelle (vulnerability [engl.])

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

SCSI (Small Computer System Interface [engl.])

Schnittstelle für die Verbindung und Datenübertragung zwischen Peripheriegeräten (z. B. Festplatten). Der Datenaustausch erfolgt bei SCSI über eine parallele Schnittstelle.

Server [engl.]

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server.

Sicherheits-Gateway

Ein Sicherheits-Gateway (oft auch Firewall genannt) gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden. Ein Sicherheits-Gateway für normalen Schutzbedarf besteht im Allgemeinen aus mehreren, in Reihe geschalteten Filterkomponenten. Dabei ist zwischen Paketfilter und Application-Level Gateway (ALG) zu unterscheiden.

Sicherheitsmaßnahme (saveguard control [engl.])

Mit Sicherheitsmaßnahme werden alle Aktionen bezeichnet, die dazu dienen, Sicherheitsrisiken zu steuern und entgegenzuwirken. Dies schließt organisatorische, personelle, technische und infrastrukturelle Sicherheitsmaßnahmen ein. Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt.

Skript

Quelltextdatei eines Programmes in Skriptsprache. Skriptsprachen werden gewöhnlich für kleine, überschaubare Programmieraufgaben verwendet. Skripte benötigen vor der Ausführung keine Übersetzung in Maschinensprache.

SMB/CIFS (Server Message Block /Common Internet File System [engl.])

Netzwerkdateisystem für den Zugriff von Computern auf NAS-Systeme. SMB/CIFS wird vorwiegend von Computern mit dem Betriebssystem Windows eingesetzt.

SMTP (Simple Mail Transfer Protocol [engl.])

Das Simple Mail Transfer Protocol legt fest, wie E-Mails zwischen Servern zu übertragen sind. Auch für den Transport von E-Mails vom Mail-Client zum Server (und die umgekehrte Richtung) kann SMTP genutzt werden.

SNMP (Simple Network Management Protocol [engl.])

Schnittstelle zur Administration und Fernwartung von Computern und Netz-Komponenten.

SSH (Secure shell [engl.])

Protokoll zum Aufbau einer verschlüsselten Verbindung zur Fernadministration von Computern.

SSL (Secure Sockets Layer [engl.])

Protokoll zur sicheren Kommunikation über das Internet.

TCP (Transmission Control Protocol [engl.])

Verbindungsorientiertes Protokoll der Transportschicht im TCP/IP-Referenzmodell, welches auf IP aufsetzt.

TLS (Transport Layer Security [engl.])

Protokoll zur sicheren Datenübertragung über das Internet. Nachfolger von SSL.

TPM (Trusted Platform Module [engl.])

Hardware des Mainboards zur sicheren Speicherung von kryptografischen Schlüsseln und Prüfsummen.

UDP (User Datagram Protocol [engl.])

Das User Datagram Protocol ist ein verbindungsloses Protokoll der Transportschicht im TCP/IP-Referenzmodell. Es sieht (anders als TCP) keine Transportquittungen oder andere Sicherheitsmechanismen für die Korrektheit der Übertragung vor. Der Header enthält wie bei TCP zwei Portnummern, die eine Zuordnung zu Diensten der Anwendungsschicht erlauben, aber unabhängig von den bei TCP benutzten Portnummern sind. Der Aufwand zur Verarbeitung eines Datenpakets ist bei UDP geringer als bei TCP. Der geringere Aufwand wird jedoch durch mehrere Nachteile, wie die höhere Wahrscheinlichkeit für Paketverluste, erkauft.

USB-Stick

Der USB-Stick ist ein mobiles Speichermedium, das an einen USB-Port angeschlossen wird.

Verfügbarkeit (availability [engl.])

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern stets wie gewünscht zur Verfügung stehen. Verfügbarkeit ist ein Grundwert der IT-Sicherheit.

Verschlüsselung (encryption [engl.])

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die Schlüssel genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartexts aus dem Geheimtext - wird Entschlüsselung genannt.

Vertraulichkeit (confidentiality [engl.])

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Vertraulichkeit ist ein Grundwert der IT-Sicherheit.

Virenschutzprogramm

Ein Virenschutzprogramm ist eine Software, die bekannte Computer-Viren, Computer-Würmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Virus (virus [engl.])

Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich nach ihrer Ausführung selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.

VPN (Virtual Private Network [engl.])

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft dem Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind. Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

WBEM (Web Based Enterprise Management [engl.])

Schnittstelle zur Administration und Fernwartung von Computern.

WMI (Windows Management Instrumentation [engl.])

Auf WBEM basierende Schnittstelle von dem Betriebssystem Windows zur Administration und Konfigurationen von Computern.

WWN (World Wide Names [engl.])

Der WWN ist eine 64-Bit lange Adresse für Fibre Channel-Komponenten, die weltweit einmalig vergeben wird. Sie sind vergleichbar mit den MAC-Adressen von Ethernet-Netzadaptern.

XML (Extensible Markup Language [engl.])

Vom World Wide Web Consortium (W3C) herausgegebene Spezifikation zur Darstellung hierarchisch strukturierter Daten in Form von Textdaten.

Zeitstempel (timestamp [engl.])

Elektronische Bescheinigung einer (vertrauenswürdigen) Stelle, dass ihr bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Es ist dabei im Allgemeinen nicht erforderlich, dass diese Stelle den Inhalt der Daten zur Kenntnis nimmt.

Zertifikat

Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem das IT-Grundschutz-Zertifikat, Schlüsselzertifikate, IT-Sicherheitszertifikate und CC-Zertifikate.

9 Stichwort- und Abkürzungsverzeichnis

Administrator.....11, 12, 37-40, 44, 54, 55, 62, 63, 65, 67-69, 71, 72, 76, 79, 80, 89, 95, 112
Angriff.....6, 13, 38, 41, 46, 48, 55, 59, 63, 71, 73, 77, 81, 82, 89, 91, 101, 111, 112, 114
ASLR (Address Space Layout Randomization).....23, 112
ATX (Advanced Technology Extended).....8-10, 112
Authentisierung 11, 12, 32, 33, 37, 39, 40, 44, 49, 53, 54, 63, 64, 68, 71, 77, 79, 83, 86, 87, 94, 104, 111, 112
Authentizität.....53, 91, 92, 112
Bedrohung.....6, 13, 19, 38, 75, 77-83, 86-89, 91, 93-99, 101, 107-111, 113, 115, 120
BIOS (Basic Input Output System).....8, 14, 58, 113, 114
Blade Server.....8, 9
Browser.....16, 112, 113, 116
BSI (Bundesamt für Sicherheit in der Informationstechnik)..1, 2, 6, 25, 35, 38, 45, 51, 88, 113, 117, 128
CIFS (Common Internet File System).....29, 32, 68, 121
Client.....7, 11, 32, 33, 37, 79, 106, 108, 110, 112, 113, 116, 118-121
Controller.....7, 8, 10, 22, 29, 30, 32, 58, 96, 113
Datenschutz.....41, 54, 71, 73, 79, 114
Datensicherheit.....58, 114, 119
Datensicherung.....23, 24, 37, 39, 42, 43, 48, 55, 64, 66, 72-74, 87, 88, 97, 99, 114
DHCP (Dynamic Host Configuration Protocol).....11, 61, 114
DNS (Domain Name Service).....11, 35, 47, 60, 101, 114
EFI (Extensible Firmware Interface).....8, 114
ESP (Executable Space Protection).....23, 114, 117
Fibre Channel.....29-32, 34, 49, 53, 56, 66, 67, 115, 118, 120, 123
Firmware.....8, 51, 58, 70, 113-115
FTP (File Transfer Protocol).....19, 61, 115
Gefährdung.....6, 75, 81, 83, 84, 91, 95, 101-105, 107-112, 115, 117
GUI (Graphical User Interface).....10, 115
Hardware..7, 8, 10, 11, 13-18, 21-23, 25, 29, 30, 34, 36-39, 42, 48, 50-53, 57, 58, 64, 69-74, 83, 85, 86, 95, 96, 99, 101, 103, 104, 113, 115, 116, 118, 120, 122
HBA (Host Bus Adapter).....7, 8, 30-32, 56, 115, 118
Hot-Swap.....8, 13, 24, 25
http.....2, 51, 116, 128, 129
HTTP (Hypertext Transfer Protocol).....11, 21, 62, 112, 116
IMAP (Internet Message Accept Protocol).....11, 19, 116, 119
Integrität...6, 20, 35-37, 40, 42, 43, 45, 46, 53-55, 65, 66, 72, 74, 75, 87, 89, 91-94, 96, 98, 99, 101, 103, 104, 106-111, 113, 114, 116-118, 123
IP.....11, 16, 20, 22, 30, 33, 56, 60, 61, 66, 67, 101, 112, 114-117, 120-122, 128
IPv4.....11, 114, 116, 117
IPv6.....11, 114, 117, 128
IQN.....31, 67, 68, 117
IT-Grundschutz.....26, 35, 45, 88, 117, 123, 128
IT-Sicherheit.....69, 101, 114, 116, 117, 121-123
Jumbo Frames.....56, 117
LDAP (Lightweight Directory Access Protocol).....11-13, 19, 40, 63, 112, 118
LUN (Logical Unit Number).....32, 49, 67, 68, 118
LUN Masking.....32, 49, 68, 118

MAC (Media Access Control).....31, 61, 65, 94, 118, 123
Multipathing.....30, 31, 68, 118
NAS (Network Attached Storage).....29, 44, 48, 49, 52, 53, 55, 86, 87, 118, 121
NFS (Network File System).....29, 33, 68, 118
NTP (Network Time Protocol).....11, 36, 37, 46, 47, 62, 94, 104, 118
Passwort.....12, 13, 40, 41, 63, 64, 71, 77, 84, 85, 87, 104, 105, 118
Patch.....37, 39, 43, 44, 51, 55, 66, 70, 74, 80, 103, 106, 110, 119
POP3.....11, 19, 116, 119
Proxy.....101, 119
Prüfsumme.....14, 20, 30, 51, 55, 94, 95, 103, 119, 122
RAID (Redundant Array of Independent Disks)..7, 8, 10, 29, 37, 52, 58, 97, 106, 107, 113, 118, 119
RDP (Remote Desktop Protocol).....11, 52, 59, 119
Restrisiko.....75-100, 105, 119
Risiko.....61, 69, 70, 107-110, 119, 120
Router.....21, 33, 56, 100, 120
SAN (Remote Desktop Protocol).....29-33, 44, 48, 49, 52, 53, 56, 68, 86, 115, 117, 118, 120
SAS (Serial Attached SCSI).....8, 29, 120
Schutzbedarf…6, 18, 27, 35, 36, 38, 44, 48, 50, 52, 68, 75, 77, 79-94, 96-99, 102-111, 117, 120, 121
Schwachstelle.....37, 40, 44, 62, 70, 73, 75-83, 86-89, 91, 93-99, 103, 104, 115, 120
SCSI (Internet Small Computer System Interface)....8, 29-33, 53, 56, 66-68, 113, 115, 117, 118, 120
Server.....1-3, 6-15, 18-25, 27, 29-58, 60-86, 89, 91-97, 99-113, 115, 116, 118-121, 128
Sicherheits-Gateway.....35, 36, 45, 46, 48, 68, 105, 121
Sicherheitsmaßnahme.....6, 117, 121
Skript.....21, 48, 71, 73, 121
SMB (Server Message Block).....29, 32, 121
SMTP (Simple Mail Transfer Protocol).....11, 19, 62, 112, 121
SNMP (Simple Network Management Protocol).....21, 54, 65, 121
Software6, 11, 16, 19-21, 23, 30, 35-37, 39, 40, 42, 44, 50, 51, 55, 59, 62, 65, 66, 69-72, 74, 76, 80, 83, 95, 101, 103, 104, 106-108, 110, 113, 114, 119, 120, 122
SSH (Secure shell).....11, 33, 52, 59, 62, 77, 121
SSL (Secure Sockets Layer).....21, 33, 116, 121, 122
TCP (Transmission Control Protocol).....30, 33, 56, 101, 112, 115, 116, 121, 122
TLS (Transport Layer Security).....116, 122
TPM (Trusted Platform Module).....14, 84, 85, 93, 104, 122
UDP (User Datagram Protocol).....33, 122
Verfügbarkeit.....6, 21, 23-27, 29, 35-38, 42, 45, 47, 49, 51, 61, 71, 72, 75, 80, 84, 85, 88, 94-100, 103-105, 107-111, 113, 114, 117, 122
Verschlüsselung.....13, 14, 21, 32, 33, 44, 51, 63, 81, 84, 85, 87, 88, 104, 105, 107, 109, 111, 122
Vertraulichkeit....6, 13, 14, 35, 43-45, 69, 75, 81, 84-88, 93, 105, 107-111, 113, 114, 117, 118, 122, 123
Virenschutzprogramm.....19, 20, 37, 40, 45, 51, 56, 57, 67, 73, 90, 91, 93, 122
Virtualisierung 7, 14-19, 29, 44, 47-49, 52, 56-58, 67-69, 73, 82, 83, 93, 99, 100, 103, 104, 106-108, 110
Virus.....115, 122
VPN (Virtual Private Network).....79, 123
WBEM (Web Based Enterprise Management).....21, 123
WMI (Windows Management Instrumentation).....21, 123
WWN (Windows Management Instrumentation).....31, 32, 67, 68, 123
XML (Extensible Markup Language).....21, 123
Zeitstempel.....64, 123

Zertifikat.....14, 77, 92, 93, 123

10 Literaturverzeichnis

[ISi-LANA]	Bundesamt für Sicherheit in der Informationstechnik, Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA): https://www.bsi.bund.de/DE/Themen/InternetSicherheit/ISiReihe/ModulederISiReihe/moduledерisireihe_node.html
[ISi-Web-Server]	Bundesamt für Sicherheit in der Informationstechnik, Sicheres Bereitstellen von Webangeboten (ISi-Web-Server): https://www.bsi.bund.de/DE/Themen/InternetSicherheit/ISiReihe/ModulederISiReihe/moduledерisireihe_node.html
[ISi-Mail-Server]	Bundesamt für Sicherheit in der Informationstechnik, Sicherer Betrieb von E-Mail-Servern (ISi-Mail-Server): https://www.bsi.bund.de/DE/Themen/InternetSicherheit/ISiReihe/ModulederISiReihe/moduledерisireihe_node.html
[ISi-IPv6]	Bundesamt für Sicherheit in der Informationstechnik, Sicherer Einsatz von IPv6 (ISi-IPv6): https://www.bsi.bund.de/DE/Themen/InternetSicherheit/ISiReihe/ModulederISiReihe/moduledерisireihe_node.html
[ISi-Fern]	Bundesamt für Sicherheit in der Informationstechnik, Sicherer Fernzugriff auf das interne Netz (ISi-Fern): https://www.bsi.bund.de/DE/Themen/InternetSicherheit/ISiReihe/ModulederISiReihe/moduledерisireihe_node.html
[BSI_KRYPTOALGO]	Bundesamt für Sicherheit in der Informationstechnik, Kryptografische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/cln_165/DE/Themen/weitereThemen/ElektronischeSignatur/TechnischeRealisierung/Kryptoalgorithmen/kryptoalgorithmen_node.html
[BSI_STD_100-4]	Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-4 Notfallmanagement: https://www.bsi.bund.de/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html
[BSI_HV_KOMP]	Bundesamt für Sicherheit in der Informationstechnik, Hochverfügbarkeitskompendium – Einführung: https://www.bsi.bund.de/DE/Themen/weitereThemen/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html
[BSI_STANDARDS]	Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Standards: https://www.bsi.bund.de/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html
[BSI_GSK_KLIMA]	Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, Maßnahme M 1.27 Klimatisierung: https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m01/m01027.html
[BSI_GSK]	Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge:

	https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html