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

Sicherheitsrichtlinie "Windows Server"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300025 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Windows Server" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

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

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc80521573)

[Dokumentenhistorie 3](#_Toc80521574)

[Inhaltsverzeichnis 4](#_Toc80521575)

[Allgemeine Festlegungen 5](#_Toc80521576)

[Ziel / Zweck 5](#_Toc80521577)

[Geltungsbereich 5](#_Toc80521578)

[Zuständigkeiten 6](#_Toc80521579)

[Genehmigungs- und Änderungsverfahren 6](#_Toc80521580)

[Aufbau des Dokuments 6](#_Toc80521581)

[Sicherheitsrichtlinie „Windows Server" 8](#_Toc80521582)

[Basismaßnahmen 8](#_Toc80521583)

[Allgemeiner Server 8](#_Toc80521584)

[Windows Server 2012 R2 10](#_Toc80521585)

[Windows Server 2016 11](#_Toc80521586)

[Windows Server 2019 12](#_Toc80521587)

[Standardmaßnahmen 13](#_Toc80521588)

[Allgemeiner Server 13](#_Toc80521589)

[Windows Server 2012 R2 16](#_Toc80521590)

[Windows Server 2016 17](#_Toc80521591)

[Windows Server 2019 19](#_Toc80521592)

[Maßnahmen bei erhöhtem Schutzbedarf 23](#_Toc80521593)

[Allgemeiner Server 23](#_Toc80521594)

[Windows Server 2012 R2 24](#_Toc80521595)

[Windows Server 2016 25](#_Toc80521596)

[Windows Server 2019 26](#_Toc80521597)

# Allgemeine Festlegungen

## Ziel / Zweck

Mit Windows Server 2012 hat Microsoft im September 2012 ein Betriebssystem für Server auf den Markt gebracht, das diverse Verbesserungen der Sicherheit gegenüber bisherigen Windows-Versionen, insbesondere auch gegenüber dem Vorgänger Windows Server 2008 R2, mitbringt. Technisch wird dabei nicht auf Windows Server 2008 R2 aufgebaut, sondern auf der Codebasis des Client-Betriebssystems Windows 8. Mit dem Release Windows Server 2012 R2 im Oktober 2013 wurde das Betriebssystem nochmals aktualisiert und erweitert, um es zum Server-Äquivalent zu Windows 8.1 auf der Clientseite zu machen.

Mit Windows Server 2016 hat Microsoft ein Serverbetriebssystem auf den Markt gebracht, dass in Bezug auf die Sicherheit weitere Verbesserungen gegenüber der Vorgängerversion (Windows Server 2012R2) aufweist. Entwickelt wurde Windows Server 2016 parallel zu Windows 10. Im Gegensatz zu Windows Server 2012 bzw. Windows Server 2012 R2 weist Windows Server 2016 folgende neuen Sicherheitsfunktionen und -standards auf.

* Shielded Virtual Machines
* Credential Guard
* Remote Credential Guard
* Device Guard

Microsoft hat die Sicherheit mit der aktuellen Server Version noch weiter erhöht. Windows Server 2019 enthält im Vergleich zu Windows Server 2016 die folgenden neuen oder verbesserten Funktionen.

* Neue Verbesserungen bei abgeschirmten VMs
* Aktualisierungen der Device Guard-Richtlinie ohne Neustart
* Kernel-Kontrollflusswächter (CFG)
* System-Wächter-Laufzeit-Monitor
* Verschlüsselung von virtuellen Netzwerken
* Windows Defender ATP-Agent enthaltener OOB

Diese Sicherheitsrichtlinie definiert verbindliche Vorgaben für die <Institution> zum Einsatz von Windows Servern in der Version 2012 R2, 2016 und 2019. Es werden sowohl organisatorische als auch technische Maßnahmen definiert, die zum Aufbau und Aufrechterhaltung eines angemessenen Schutzniveaus notwendig sind.

Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben der BSI Bausteine SYS.1.1. „Allgemeiner Server" und SYS.1.2.2 „Windows Server 2012" beachtet. Aus diesem Grunde wurden die Anforderungen in die Abschnitte "Allgemeiner Server" sowie dedizierten Windows Servern "Windows Server 2012 R2", "Windows 2016" und "Windows 2019" zusätzlich unterteilt.

## Geltungsbereich

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

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

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

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

## Zuständigkeiten

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

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

## Genehmigungs- und Änderungsverfahren

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

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

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

# Sicherheitsrichtlinie „Windows Server"

## Basismaßnahmen

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

### Allgemeiner Server

#### Geeignete Aufstellung (SYS.1.1.A1)

Die Systeme sind in einem speziell dafür vorgesehenen Raum aufzustellen. Server müssen daher in Rechenzentren, Rechnerräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden. Besondere Infrastrukturen wie Zutrittskontrolle, Temperaturregulierung, Luftfeuchteregulierung, mehrere Stromkreise, die mit einer USV abgesichert sind, Alarm- und Löschsysteme für Feuer sowie ein Alarmsystem für Wasser, sind in diesen Räumen zu installieren. Die Server, die gesichert werden sollen, müssen geeignet von den sichernden Systemen, etwa Backup-Servern, in unterschiedlichen Brandabschnitten getrennt werden.

Es ist zu regeln, wer Zutritt zu den Räumen beziehungsweise zu den Servern selbst erhält.

#### Benutzerauthentisierung an Servern (SYS.1.1.A2)

Für die Anmeldung von Benutzern und Diensten am Server sind Authentisierungsverfahren einzusetzen, die dem Schutzbedarf der Server angemessen sind. Dieses ist in besonderem Maße für administrative Zugänge zu berücksichtigten. Soweit möglich, sind dabei zentrale, netzbasierte Authentisierungsdienste zu bevorzugen. Verwendete Passwörter müssen sicher sein.

Die Authentisierung beziehungsweise Autorisierung muss gemäß den Anforderungen für das Identitäts- und Berechtigungsmanagement erfolgen.

#### Restriktive Rechtevergabe (SYS.1.1.A3)

Zugriffsrechte auf Dateien, die auf Servern gespeichert sind, sind restriktiv zu vergeben. Jeder Benutzer darf nur auf die Dateien zugreifen können, die er für seine Aufgabenerfüllung benötigt (Need-to-know-Prinzip). Nur Mitarbeitende mit administrativen Zugriffsrechten dürfen auf die Systemverzeichnisse zugreifen.

Alle Anträge, Änderungen, Löschungen und Freigaben zu Zugriffsrechten sind geeignet zu dokumentieren. Es sollte regelmäßig überprüft werden, ob die Berechtigungen, insbesondere für Systemverzeichnisse und -dateien, den Vorgaben der <Institution> entsprechen.

#### Rollentrennung (SYS.1.1.A4)

Es ist sicherzustellen, dass Kennungen mit Administratorrechten nur für Administrationsaufgaben verwendet werden. Für alle Administratoren sind zusätzliche Benutzerkennungen einzurichten, die nur über die eingeschränkten Rechte verfügen, die die Administratoren zur Aufgabenerfüllung außerhalb der Administration benötigen. Für Arbeiten, die nicht der Administration dienen, dürfen die Administratoren nur diese Benutzerkennungen verwenden. Über die notwendigen Benutzerkennungen hinaus sollten keine weiteren Benutzer auf dem Server angelegt werden.

Die Installation, Modifikation, Änderung oder Löschung von Anwendungen und Systemkonfigurationen sollte nur durch die Administration unter Zuhilfenahme von zentralen Managementwerkzeugen erfolgen.

#### Schutz der Administrationsschnittstellen (SYS.1.1.A5)

Die Administration der Server muss über freigegebene kryptografische Protokolle und Algorithmen erfolgen. Die Tools, Methoden und die Sicherheitsvorkehrungen sind geeignet zu dokumentieren.

Die Administration der Server sollte aus einem dedizierten Sicherheitsbereich für Administration heraus erfolgen.

#### Deaktivierung nicht benötigter Dienste und Kennungen (SYS.1.1.A6)

Nach der Installation sind nur solche Module, Programme, Dienste, Benutzerkennungen und Schnittstellen aktiv, die für die Verwendung des Systems an der vorgesehenen Einsatzstelle notwendig sind. Alle nicht benötigten Komponenten bzw. Funktionen sind zu deaktivieren oder zu deinstallieren. Nicht benötigte Benutzerkennungen sind entweder zu löschen oder zumindest so zu deaktivieren, dass unter diesen Kennungen keine Anmeldungen am System weiterhin möglich sind. Vorhandene Default-Kennungen sind soweit möglich zu deaktivieren oder zumindest zu ändern. Voreingestellte Default-Passwörter und Default-Passwörter von Default-Kennungen sind zu ändern. Auf Servern sollte der Speicherplatz für die einzelnen Benutzer, aber auch für Anwendungen, geeignet beschränkt werden.

Die Konfiguration und die Veränderungen dieser Einstellungen an den Servern sind zu dokumentieren und dürfen nur mit administrativen Rechten durchgeführt werden.

#### Updates und Patches für Firmware, Betriebssystem und Anwendungen (SYS.1.1.A7)

Die verantwortlichen Administratoren müssen sich regelmäßig über bekannt gewordene Schwachstellen der Firmware, Betriebssysteme, eingesetzter Anwendungen und Dienste informieren. Die identifizierten Schwachstellen sind so schnell wie möglich zu beheben. Grundsätzlich ist darauf zu achten, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden.

Solange kein entsprechender Patch zur Verfügung steht, ist abhängig vom Schweregrad (Impact) der Schwachstelle und Bedrohungen eine geeignete Maßnahme (Workaround) zum Schutz des Systems zu etablieren.

#### Regelmäßige Datensicherung (SYS.1.1.A8)

Unter Berücksichtigung der etablierten Datensicherungsverfahren sind die Server regelmäßig zu sichern. In virtuellen Umgebungen sollte geprüft werden, ob das System unter Umständen durch Snapshot-Mechanismen der Virtualisierungsumgebung gesichert werden kann.

Die Wiederherstellung einer Datensicherung ist zur Minimierung von Fehlern im Datensicherungsprozess regelmäßig zu üben. Zur Vermeidung von Fehlfunktionen ist beim Einspielen einer Datensicherung darauf zu achten, dass die Wiederherstellung von produktiv Systemen zuvor auf einem identisch eingerichteten Testsystem stattfindet. Im Rahmen des Notfallplans sind der Wiederanlauf, die Wiederherstellung und die benötigten Zeiten zu definieren. Der Notfallplan sollte durch praktische Tests validiert und kontinuierlich verbessert werden.

#### Einsatz von Virenschutz-Programmen (SYS.1.1.A9)

Bei der Auswahl des Virenschutz-Programmes sind die zu unterstützenden Betriebssysteme sowie die Service- und Supportleistungen des Herstellers zu berücksichtigen. Bei der Nutzung von Cloud-Diensten ist zu prüfen und zu dokumentieren, ob Datenschutzaspekte eventuell gegen den Einsatz sprechen. Alle Server sind in eine zentrale Infrastruktur zur Erkennung, Behandlung und Vermeidung von Malware zu integrieren.

Die Virenschutz-Programme und deren Signaturen sind nach den Vorgaben des Herstellers zu aktualisieren. Nach einem Update der Virenschutz-Programme sollten die Konfigurationseinstellungen mit den dokumentierten Vorgaben abgeglichen werden.

Es ist sicherzustellen, dass die berechtigten Administratoren oder installierten Anwendungen keine sicherheitsrelevanten Konfigurationsänderungen am Virenschutz-Programm vornehmen oder dieses deaktivieren.

#### Protokollierung (SYS.1.1.A10)

Alle sicherheitsrelevanten Ereignisse von Servern und Anwendungen sind zu protokollieren. Diese umfassen mindestens:

* Systemstarts und Reboots,
* erfolgreiche und erfolglose Anmeldungen am System (Betriebssystem und Anwendungssoftware),
* fehlgeschlagene Berechtigungsprüfungen,
* blockierte Datenströme (Verstöße gegen ACLs oder Firewall-Regeln),
* Einrichtung oder Änderungen von Benutzern, Gruppen und Berechtigungen,
* sicherheitsrelevante Fehlermeldungen (z. B. Hardwaredefekte, Überschreitung von Kapazitätsgrenzen) sowie
* Warnmeldungen von Sicherheitssystemen (z. B. Virenschutz).

Bei der Einrichtung der Protokollierung sind die Herstellervorgaben für die jeweiligen IT-Systeme oder Anwendungen zu beachten und in einem angemessenen Rahmen anzuwenden.

Es ist in geeigneten Intervallen stichpunktartig zu überprüfen, ob die Protokollierung noch korrekt funktioniert. Die Intervalle sollten an die zu berücksichtigen Server und deren ermittelten Schutzbedarf (Verfügbarkeit, Vertraulichkeit und Integrität) angepasst werden.

Bei der Protokollierung sind die gesetzlichen Datenschutzbestimmungen einzuhalten. Dazu zählen unter anderem die gesetzlichen Anforderungen der EU-DSGVO und des BDSG-neu. Sofern wir Kunden aus dem öffentlichen Sektor betreuen, können zusätzlich landestypische Datenschutzanforderungen mit zu beachten sein. Die Protokollierungsdaten sind nach einem festgelegten Aufbewahrungsprozess zu löschen.

Seitens der <Institution> wird technisch unterbunden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden können.

### Windows Server 2012 R2

#### Planung von Windows Server 2012 R2 (SYS.1.2.2.A1)

Der Einsatz von Windows Server 2012 ist vor der Installation sorgfältig zu planen. Die Anforderungen an die Hardware sind vor der Beschaffung des Server Betriebssystems zu prüfen. Es ist eine begründete und dokumentierte Entscheidung für eine geeignete Edition des Windows Server 2012 R2 zu treffen. Der Einsatzzweck des Servers sowie die Einbindung ins Active-Directory sind dabei unter Berücksichtigung des Schutzbedarfes (Verfügbarkeit, Vertraulichkeit, Integrität) sowie des potentiellen Angriffsvektors zu spezifizieren. Die Nutzung von ins Betriebssystem integrierten Cloud-Diensten sind grundsätzlich zu beurteilen und zu planen. Sofern nicht benötigt, ist die Einrichtung von Microsoft-Konten auf dem Server zu blockieren.

#### Sichere Installation von Windows Server 2012 R2 (SYS.1.2.2.A2)

Das Installationsmedium ist aus einer verlässlichen Quelle zu beziehen. Es dürfen nur die benötigten Serverrollen und Features bzw. Funktionen installiert werden. Wenn vom Funktionsumfang herausreichend, ist die Server-Core-Variante zu installierten. Andernfalls ist zu begründen, warum die Server-Core-Variante nicht ausreichend ist. Der Server ist im Rahmen der Installation als erstes auf einen aktuellen Patch-Stand zu aktualisieren.

#### Sichere Administration von Windows Server 2012 R2 (SYS.1.2.2.A3)

Lokale Administrationskonten sind mit einzigartigen, sicheren Passwörtern abzusichern. Alle verantwortlichen Administratoren sind in den sicherheitsrelevanten Aspekten der Administration von Windows Server 2012 entsprechend dem vereinbarten Schulungsprogramm zu schulen. Administratoren dürfen ihre privilegierten Rechte nur zum Zwecke der Administration einsetzen (siehe Abschnitt Rollentrennung (SYS.1.1.A4)). Browser auf dem Server dürfen nicht zum Surfen im Web verwendet werden.

### Windows Server 2016

#### Planung des Einsatzes von Windows Server 2016 (SYS.bd.1.A1)

Der Einsatz beziehungsweise Einsatzzweck von Windows Server 2016 muss sorgfältig geplant werden. Es muss eine begründete und dokumentierte Entscheidung für eine geeignete Windows Server 2016 Edition getroffen werden. Bei einer geplanten Cloud-Einbindung muss sichergestellt sein, dass die Cloud-Features erst aktiviert werden, wenn die Cloud-Mechanismen im Rahmen einer grundsätzlichen Beurteilung der Cloud-Nutzung geplant wurden. Sofern Microsoft-Konten nicht benötigt werden, muss die Einrichtung von Microsoft-Konten auf dem Server blockiert werden.

#### Sichere Installation von Windows Server 2016 (SYS.bd.1.A2)

Die Windows Server 2016 müssen aus nachweislich integren Quellen bezogen und sicher installiert werden. Je nach benötigtem Funktionsumfang muss entweder die Variante „Server with Desktop Experience“, „Server-Core“ oder „Nano-Server“ installiert werden. Es muss gewährleistet sein, dass ausschließlich die benötigten Serverrollen, Features oder Funktionen installiert werden. Jede Entscheidung im Rahmen der Installation von Windows Server 2016 muss begründet und dokumentiert erfolgen. Bei erhöhtem Schutzbedarf muss eine deny-all, permit-by-exception policy für die autorisierte Softwareausführung verwendet werden.

#### Sichere Administration von Windows Server 2016 (SYS.bd.1.A3)

Lokale Administrationskonten sind mit einzigartigen, sicheren Passwörtern abzusichern. Alle verantwortlichen Administratoren sind in den sicherheitsrelevanten Aspekten der Administration von Windows Server 2016 entsprechend dem vereinbarten Schulungsprogramm zu schulen. Administratoren dürfen ihre privilegierten Rechte nur zum Zwecke der Administration einsetzen (siehe Abschnitt Rollentrennung (SYS.1.1.A4)). Browser auf dem Server dürfen nicht zum Surfen im Web verwendet werden.

#### Telemetrie und Datenschutzeinstellungen unter Windows Server 2016 (SYS.bd.1.A4)

Die Telemetriedienste, also die Diagnose- und Nutzungsdaten, die zur Identifizierung und Lösung von Problemen, zur Verbesserung der Dienste und Produkte und zur Personalisierung des Systems mit eindeutigen Identifizierungsmerkmalen verknüpft und an Microsoft übermittelt werden, können im Betriebssystem nicht vollständig abgeschaltet werden. Es ist daher durch geeignete Maßnahmen, etwa auf Netzebene, sicherzustellen, dass diese Daten nicht an Microsoft übertragen werden.

### Windows Server 2019

#### Planung des Einsatzes von Windows Server 2019 (SYS.bd.2.A1)

Der Einsatz beziehungsweise Einsatzzweck von Windows Server 2019 muss sorgfältig geplant werden. Es muss eine begründete und dokumentierte Entscheidung für eine geeignete Windows Server 2019 Edition getroffen werden. Bei einer geplanten Cloud-Einbindung muss sichergestellt sein, dass die Cloud-Features erst aktiviert werden, wenn die Cloud-Mechanismen im Rahmen einer grundsätzlichen Beurteilung der Cloud-Nutzung geplant wurden. Sofern Microsoft-Konten nicht benötigt werden, muss die Einrichtung von Microsoft-Konten auf dem Server blockiert werden.

#### Sichere Installation von Windows Server 2019 (SYS.bd.2.A2)

Die Windows Server 2019 müssen aus nachweislich integren Quellen bezogen und sicher installiert werden. Je nach benötigtem Funktionsumfang muss entweder die Variante „Server with Desktop Experience“, „Server-Core“ oder „Nano-Server (Basis-Betriebssystemimage für Container)“ installiert werden. Denn seit Windows Server 2019 kann man sich nicht mehr dadurch behelfen, dass man die Desktop Experience installiert und das System nach dem Einspielen der Anwendungen auf Server Core herunter­stuft. Vielmehr muss man sich schon beim Setup endgültig entscheiden.

Es muss gewährleistet sein, dass ausschließlich die benötigten Serverrollen, Features oder Funktionen installiert werden. Jede Entscheidung im Rahmen der Installation von Windows Server 2019 muss begründet und dokumentiert erfolgen. Bei erhöhtem Schutzbedarf muss eine deny-all, permit-by-exception policy für die autorisierte Softwareausführung verwendet werden.

#### Sichere Administration von Windows Server 2019 (SYS.bd.2.A3)

Lokale Administrationskonten sind mit einzigartigen, sicheren Passwörtern abzusichern. Alle verantwortlichen Administratoren sind in den sicherheitsrelevanten Aspekten der Administration von Windows Server 2019 entsprechend dem vereinbarten Schulungsprogramm zu schulen. Administratoren dürfen ihre privilegierten Rechte nur zum Zwecke der Administration einsetzen (siehe Abschnitt Rollentrennung (SYS.1.1.A4)). Browser auf dem Server dürfen nicht zum Surfen im Web verwendet werden.

#### Telemetrie und Datenschutzeinstellungen unter Windows Server 2019 (SYS.bd.2.A4)

Die Telemetriedienste, also die Diagnose- und Nutzungsdaten, die zur Identifizierung und Lösung von Problemen, zur Verbesserung der Dienste und Produkte und zur Personalisierung des Systems mit eindeutigen Identifizierungsmerkmalen verknüpft und an Microsoft übermittelt werden, können im Betriebssystem nicht vollständig abgeschaltet werden. Es ist daher durch geeignete Maßnahmen, etwa auf Netzebene, sicherzustellen, dass diese Daten nicht an Microsoft übertragen werden.

## Standardmaßnahmen

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

### Allgemeiner Server

#### Planung des Server-Einsatzes (SYS.1.1.A12)

Jedes Server-System sollte geeignet geplant werden. Dabei sind mindestens die folgenden Punkte zu berücksichtigen werden:

* Auswahl der Hardwareplattform, des Betriebssystems und der Anwendungssoftware,
* Dimensionierung der Hardware (Leistung, Speicher, Bandbreite etc.),
* Art und Anzahl der Kommunikationsschnittstellen,
* Leistungsaufnahme, Wärmelast, Platzbedarf und Bauform,
* Realisierung administrativer Zugänge,
* Zugriffe von Benutzern,
* Realisierung der Protokollierung,
* Realisierung der Systemaktualisierung sowie
* Einbindung ins System- und Netzmanagement, in die Datensicherung und die Schutzsysteme (Virenschutz, IDS etc.).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, sind nachvollziehbar zu dokumentieren.

#### Beschaffung von Servern (SYS.1.1.A13)

Bevor ein oder mehrere Server beschafft werden, sollte eine Anforderungsliste erstellt werden, anhand derer die am Markt oder vom Dienstleister erhältlichen Produkte bewertet werden.

#### Erstellung eines Benutzer- und Administrationskonzepts (SYS.1.1.A14)

Bei den eingesetzten Servern muss eine Funktionstrennung zwischen der Administration des Betriebssystemsystems und dem normalen Standardnutzer erfolgen. Nur verantwortliche Administratoren erhalten eine zusätzliche Benutzerkennung mit Administrationsrechten für das Server-System.

Die Installation, Modifikation, Änderung oder Löschung von Anwendungen und Systemkonfigurationen dürfen nur durch ein zentrales Konfigurationsmanagement und den verantwortlichen Administratoren erfolgen.

Die Rahmenbedingungen, Anforderungen und Aufgabentrennungen an die Rollen des Benutzers und der Administration sind im Standard „IT-Administration“ festgelegt.

#### Unterbrechungsfreie und stabile Stromversorgung (SYS.1.1.A15)

Jeder Server sollte an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV sollte eine ausreichende Leistung und Kapazität haben. Es ist erneut zu prüfen, ob die Stützzeit der verwendeten USV ausreicht, wenn Änderungen an den Verbrauchern durchgeführt wurden.

Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV ist regelmäßig zu testen. Die USV ist in die zentralen Wartungspläne aufzunehmen. Sofern die USV zentral überwacht und verwaltet werden kann, ist diese in ein vorhandenes System- und Netzmanagement einzubinden.

#### Sichere Installation und Grundkonfiguration von Servern (SYS.1.1.A16)

Die Installation von Servern muss auf Basis eines dokumentierten Installationsprozess und ausschließlich durch die verantwortlichen Administratoren erfolgen. Soweit vorhanden, sind Installation-Templates oder zentrale Verwaltungssysteme wie bspw. Puppet, SaltStack, Chef, Ansible zu verwenden.

Die System- und Anwendungssoftware ist vertrauenswürdigen Installationsquellen zu beziehen.

Alle nicht benötigten Dienste, Prozesse und Benutzer sind zu entfernen, alle Standardpasswörter sind zu ändern.

Alle Installationsschritte sollten so dokumentiert werden, dass die Installation durch einen sachkundigen Dritten nachvollzogen und wiederholt werden kann.

#### Einsatzfreigabe für Server (SYS.1.1.A17)

Bevor Server im produktiven Betrieb eingesetzt und bevor die Server an ein produktives Netz angeschlossen werden, sollte eine Prüfung und Einsatzfreigabe erfolgen. Mittels Soll-/Ist-Vergleich zwischen der Anforderungsliste und der aktuellen Installation sowie der Prüfung, ob nur benötigte Dienste und Prozesses auf dem System laufen sollte die Einsatzfreigabe vorbereitet werden. Die Prüfung/Tests umfassen auch die Verifizierung der einwandfreien Funktion des Systems sowie der Anwendungssoftware.

Alle Ergebnisse der Prüfungen und Tests sollten geeignet dokumentiert und abgelegt werden.

Sind alle Tests und Prüfungen ohne Auffälligkeiten bestanden, ist der Server an das produktive Netzwerk anzuschließen.

#### Verschlüsselung der Kommunikationsverbindungen (SYS.1.1.A18)

Für alle vom Server angebotenen und genutzten Netzdienste ist zu prüfen, ob mit vertretbarem Aufwand eine Verschlüsselung der Kommunikationsverbindungen möglich und praktikabel ist. Ist dies der Fall, so ist die Verschlüsselung entsprechend den internen Vorgaben der <Institution> zu aktivieren.

#### Einrichtung lokaler Paketfilter (SYS.1.1.A19)

Für die lokale Kommunikationsfilterung und gestaffelte Verteidigung (Defense-in-Depth) sind bei erhöhtem Schutzbedarf neben der Segmentierung von Netzen, Zonierung und Paketfilterung durch dedizierte und aktive Firewalls eine lokale Paketfilterung zu aktivieren. Zum weiteren Schutz wird die lokale Firewall auf dem Server-System für den eingehenden und ausgehenden Datenverkehr strikt eingestellt/aktiviert. Die Identität von einem entfernten System und die Integrität der Verbindungen mit dem entfernten System sind kryptografisch abzusichern.

#### Beschränkung des Zugangs über Netze (SYS.1.1.A20)

Generell sollte das gesamte Netz durch eine entsprechende Firewall-Infrastruktur gegen unbefugte Zugänge geschützt sein. Server, die Dienste nach außen hin anbieten, sind in einer Demilitarisierten Zone (DMZ) aufzustellen.

Server dürfen nicht im selben IP-Subnetz wie die Clients platziert sein. Server sind mindestens durch ein Layer-3-Gerät (Router, L3-Switch, Firewall) von den Clients zu trennen.

#### Betriebsdokumentation für Server (SYS.1.1.A21)

Zur Betriebsdokumentation sind die Server in das zentrale Monitoring einzubinden. Alle manuellen Tätigkeiten, wie z. B. der Austausch des Speichers oder Änderungen an der Konfiguration, sind in die Serverdokumentation einzupflegen.

#### Einbindung in die Notfallplanung (SYS.1.1.A22)

Der Server ist im Notfallmanagementprozess zu berücksichtigen. Dazu SOLLTEN die Notfallanforderungen an das System ermittelt und geeignete Notfallmaßnahmen umgesetzt werden, z. B. indem Wiederanlaufpläne erstellt oder Passwörter und kryptografische Schlüssel sicher hinterlegt werden.

#### Systemüberwachung und Monitoring von Servern (SYS.1.1.A23)

Das Server-System ist in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept einzubinden, das den Systemzustand und die Funktionsfähigkeit des Systems und der darauf betriebenen Dienste laufend überwacht und Fehlerzustände sowie die Überschreitung definierter Grenzwerte an die verantwortlichen Mitarbeitenden meldet.

Beim Überschreiten definierter Grenzwerte sind entsprechende Alarme auszulösen.

#### Sicherheitsprüfungen (SYS.1.1.A24)

Die Server sind regelmäßigen Sicherheitstests zu unterziehen, die überprüfen, ob alle Sicherheitsvorgaben der <Institution> eingehalten werden und ggf. vorhandene Schwachstellen identifizieren. Diese Sicherheitsprüfungen sind insbesondere auf Servern mit externen Schnittstellen durchzuführen. Um mittelbare Angriffe über infizierte Systeme zu vermeiden, sollten jedoch auch interne Server in festgelegten Zyklen entsprechend überprüft werden. Es sollte geprüft werden, ob die Sicherheitsprüfungen automatisiert, z. B. mittels geeigneter Skripte, realisiert werden können.

#### Geregelte Außerbetriebnahme eines Servers (SYS.1.1.A25)

Die Außerbetriebnahme von Servern erfolgt dokumentiert. Dabei ist auf die Sicherung aller notwendigen Daten zu achten. Die Speichermodule sind entweder sicher zu löschen oder einer zertifizierten Zerstörung zu zuführen. Alle angebrachten Beschriftungen sind zu entfernen.

### Windows Server 2012 R2

#### Sichere Konfiguration von Windows Server 2012 R2 (SYS.1.2.2.A4)

Mehrere wesentliche Funktionen bzw. Rollen sollten nicht durch einen einzigen Server erfüllt, sondern geeignet aufgeteilt werden. Vor Inbetriebnahme ist das Server-System grundlegend zu härten. Dafür sollten funktionsspezifische und <Institution>-weite Sicherheitsvorlagen erstellt, gepflegt und auf die Server ausgerollt werden. Die Einstellungen sollten sowohl anfangs als auch bei jeder Änderung vor einer erneuten Inbetriebnahme getestet werden. Die Nutzung des Internet Explorer (Browser) ist auf dem Server nur in der Enhanced Security Configuration und im Enhanced Protected Mode freigegeben.

#### Schutz vor Schadsoftware auf Windows Server 2012 R2 (SYS.1.2.2.A5)

Alle Server (außer Stand-Alone-Systeme ohne Netz-Anschluss und Anschluss für Wechselmedien) müssen vor dem ersten Verbinden mit einer Netzverbindung, einem mobilen Netz oder einem Wechselmedium in die etablierte Anti-Malware-Infrastruktur integriert werden. Die Protokollierung muss entsprechend den veröffentlichten Vorgaben vorgenommen werden. Die Administratoren müssen Alarmierungen bei Virenfunden durchführen, konfigurieren und regelmäßig auswerten. Zusätzlich muss eine automatisierte Auswertung der Alarme geprüft werden, da so Sicherheitslücken zeitnah erkannt und behandelt werden können.

#### Sichere Authentisierung und Autorisierung in Windows Server 2012 R2 (SYS.1.2.2.A6)

Alle Benutzer müssen unter Windows Server 2012 R2 Mitglieder der Sicherheitsgruppe „Geschützte Nutzer“ sein. Dienste- und Computer-Konten sollten hingegen nicht Mitglied von „Geschützte Nutzer“ sein. Dienste-Konten in Windows Server 2012 sind als Mitglieder der Gruppe „Managed Service Account“ zu hinterlegen. Der PPL-Schutz des Local Credential Store (LSA) ist zu aktivieren. Der Einsatz dynamischer Zugriffsregeln auf Ressourcen sollte bevorzugt werden. Mitarbeitende mit administrativen Rechten arbeiten auf ihren eigenen Clients mit beschränkten Rechten.

#### Prüfung der Sicherheitskonfiguration von Windows Server 2012 R2 (SYS.1.2.2.A7)

Die Sicherheitskonfiguration von Windows Server 2012 ist mittels geeigneter Tools regelmäßig zu überprüfen, zu dokumentieren und kontinuierlich zu verbessern.

#### Schutz der Systemintegrität eines Windows Servers 2012 R2 (SYS.1.2.2.A8)

Secure Boot sollte aktiv sein. AppLocker ist zu strikt zu konfigurieren und zu aktiviert. Die Auswirkungen der Einstellungen und deren Änderungen sollten vorab getestet werden.

#### Lokale Kommunikationsfilterung eines Windows Servers 2012 R2 (SYS.1.2.2.A9)

Die lokale Firewall des Windows Server 2012 sollte für eingehenden und ausgehenden Netzverkehr aktiviert und möglichst strikt eingestellt sein. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen sollte kryptografisch abgesichert sein.

Die lokale Windows Server 2012 Firewall oder ein installierte Firewall eines Dritt-Herstellers sind zentral zu administrieren.

### Windows Server 2016

#### Sichere Konfiguration eines Windows Server 2016 (SYS.bd.1.A5)

Die Windows Server 2016 Systeme müssen entsprechend den Anforderungen des Stands der Technik gehärtet werden. Um die Systemhärtung umzusetzen, müssen funktionsspezifische Sicherheitsvorlagen erstellt, gepflegt und angewendet werden. Für die Windows Server 2016 und gegebenenfalls auch weiteren Serversysteme einer bestimmten Einsatzklasse müssen Baselines erstellt, regelmäßig geprüft und fortgeschrieben werden. Vor der Installation von Servicepacks oder Enhancement-Packs auf produktiven IT-Systemen müssen im Rahmen des Patch- und Änderungsmanagements der <Institution> Prüfungen der Härtungsmaßnahmen erfolgen. Das System muss für das Patch- und Änderungsmanagement auf ein unterstütztes Service Level gehoben werden. Zusätzlich müssen alle Windows Server 2016 bei erhöhten Schutzbedarfsanforderungen einem geeigneten Monitoring unterliegen. Jede Entscheidung im Rahmen der Konfiguration von Windows Server 2016 ist zu begründen und zu dokumentieren.

#### Rollenbasierte Administration unter Windows Server 2016 (SYS.bd.1.A6)

Auf Basis von Windows PowerShell wird bei Windows Server 2016 mithilfe von Just Enough Administration (JEA) eine rollenbasierte Administration implementiert. Die rollenbasierte Administration wird so eingesetzt, dass die Administratoren nur auf die Bereiche eines IT-Systems beziehungsweise Netzes Zugriff erhalten, die in ihren Aufgabenbereich fallen. Zur etablierten rollenbasierten Administration wurde ein feingranulares rollenbasiertes Administrationskonzept nach dem Prinzip Least Privilege erstellt und etabliert. Für kritische Dienste wird eine Zwei-Faktor-Authentifizierung eingesetzt.

#### Sichere Authentisierung und Autorisierung in Windows Server 2016 (SYS.bd.1.A7)

Alle Benutzer müssen unter Windows Server 2016 Mitglieder der Sicherheitsgruppe „Geschützte Nutzer“ sein. Dienste- und Computer-Konten sollten hingegen nicht Mitglied von „Geschützte Nutzer“ sein. Dienste-Konten in Windows Server 2016 sind als Mitglieder der Gruppe „Managed Service Account“ zu hinterlegen. Der PPL-Schutz des Local Credential Store (LSA) ist zu aktivieren. Der Einsatz dynamischer Zugriffsregeln auf Ressourcen sollte bevorzugt werden. Mitarbeitende mit administrativen Rechten arbeiten auf ihren eigenen Clients mit beschränkten Rechten.

#### Hochverfügbarkeit und Storages Spaces unter Windows Server 2016 (SYS.bd.1.A8)

Für die Gewährleistung der Hochverfügbarkeit von Festplattenspeichern unter Windows Server 2016 sollte die Funktion „Storage Spaces“ genutzt werden. Durch „Storage Spaces“ sind redundante und flexible Festplattenspeicher zu erstellen. Wenn besonders hohe Verfügbarkeitsanforderungen an ein System bestehen, welches unter Windows Server 2016 betrieben wird, sind Maßnahmen aus der jeweiligen Anwendung berücksichtigt.

#### Einsatz der Virtual Machine Lastenausgleichsfunktion unter Windows Server 2016 (SYS.bd.1.A9)

Zur Optimierung der Auslastung von Knoten in einem Failovercluster sollten die Windows Server 2016 Funktion für den Lastenausgleich für Virtual Machine (VM) entsprechend den Schutzbedarfen konfiguriert und gesteuert werden. Von den verantwortlichen Administratoren sind die abgestimmten Vorgaben für den „VM-Lastenausgleich“ zu dokumentieren und regelmäßig zu aktualisieren.

#### Schutz vor Schadsoftware auf einem Windows Server 2016 (SYS.bd.1.A10)

Alle Server (außer Stand-Alone-Systeme ohne Netz-Anschluss und Anschluss für Wechselmedien) müssen vor dem ersten Verbinden mit einer Netzverbindung, einem mobilen Netz oder einem Wechselmedium in die etablierte Anti-Malware-Infrastruktur integriert werden. Die Protokollierung muss entsprechend den veröffentlichten Vorgaben vorgenommen werden. Die Administratoren müssen Alarmierungen bei Virenfunden durchführen, konfigurieren und regelmäßig auswerten. Zusätzlich muss eine automatisierte Auswertung der Alarme geprüft werden, da so Sicherheitslücken zeitnah erkannt und behandelt werden können.

Der Malware-Schutz muss die Szenarien „Hyper-V-Hosts“ und „Hochverfügbarkeitscluster“ berücksichtigen. Bei einem erhöhten Schutzbedarf muss für jeden Windows Server 2016 ein hostbasiertes Intrusion Detection oder Prevention System eingesetzt werden.

#### Enhanced Threat Detection unter Windows Server 2016 (SYS.bd.1.A11)

Um bösartiges Verhalten besser überwachen zu können sollte „Enhanced Threat Detection“ eingesetzt werden. Die gesammelten Informationen der „Enhanced Threat Detection“ sind an ein zentrales Analysetool und an ein SIEM weiterzuleiten. Eine Alarmierung bei böswilligem Verhalten beziehungsweise vorliegenden Bedrohungen ist einzurichten.

#### Sicherer Umgang mit Containern unter Windows Server 2016 (SYS.bd1.A12)

Bei „Windows Server Containern“ und „Hyper-V Containern“ sind ausschließlich OS Images zu nutzen. In Abhängigkeit vom Einsatzzweck und Schutzbedarf ist die zu verwendende Container-Variante zu wählen. Die Entscheidung für eine Variante sollte begründet und dokumentiert werden.

#### Einsatz von Containern unter Windows Server 2016 (SYS.bd.1.A13)

Beim Einsatz von Containern sollten die Anforderungen an die Sicherheit von Anfang an berücksichtigt werden. Beim Betrieb von Containern auf Basis von Windows Server 2016 sollte die Umsetzungsvariante mittels Hyper-V-Containern bevorzugt werden.

Beim Betrieb einer Containerlösung müssen die Verantwortlichen sicherstellen, dass der innerhalb des Containers verwendete Code aus einer bekannten und vertrauenswürdigen Quelle stammt. Es müssen in regelmäßigen Abständen Schwachstellen-Tests unter Zuhilfenahme von Schwachstellen-Analyse-Tools durchgeführt werden.

#### Einsatz von Shielded Virtual Machines von Windows Server 2016 (SYS.bd.1.A14)

Auf Basis des Schutzbedarfes und der Einsatzszenarien muss der Einsatz von „Shielded Virtual Machines“ geprüft werden. Für den Einsatz von „Shielded Virtual Machines“ muss ein vertrauenswürdiger Hyper-V-Host eingerichtet sein. Für die Verschlüsselung „Shielded Virtual Machines“ wird eine Guarded-Fabric-Instrastruktur vorausgesetzt, demzufolge müssen Host Guardian Services (HGS) und Guarded Hosts eingerichtet werden. Es müssen je nach Bedarf beim HGS die Modi „Admin-trusted Modus“ oder „TPM-trusted-Modus“ genutzt werden.

#### Einsatz von Credential Guard und Remote Credential Guard unter Windows Server 2016 (SYS.bd.1.A15)

Für die Sicherheit von Zugangsdaten sollte „Credential Guard“ oder „Remote Credential Guard“ bei Windows Server 2016 eingesetzt werden. Die Hardware-Sicherheit, die virtualisierungsbasierte Sicherheit und der Schutz gegen fortgeschrittene dauerhafte Bedrohungen sind bei „Credential Guard“ oder „Remote Credential Guard“ zu berücksichtigen. Für „Credential Guard“ ist auf domänenverbundenen Systemen das „Trusted Platform Module (TPM)“ zu aktivieren.

#### Einsatz von Device Guard unter Windows Server 2016 (SYS.bd.1.A16)

Der Schutz vor nicht vertrauenswürdiger Software sollte durch „Device Guard“ gewährleistet werden. Die Konfiguration von „Device Guard“ darf nur durch geschulte und verantwortliche Administratoren erfolgen. Bei erhöhtem Schutzbedarf von domänenverbundenen Systemen in virtuellen Umgebungen ist „Device Guard“ zu aktivieren. Der Einsatz von „Device Guard“ muss den Vorgaben des Patch- und Änderungsmanagements der <Institution> unterliegen.

#### Einsatz vom Control Flow Guard unter Windows Server 2016 (SYS.bd.1.A17)

Sofern Windows Server 2016 als Terminal-Server eingesetzt wird, ist zum Schutz vor Browser-Malware „Control Flow Guard“ zu etablieren. Die Kontrolle von „Indirect Calls“ in Programmen sind zum Schutz vor Exploits zu aktivieren.

#### Schutz der Systemintegrität von Windows Server 2016 (SYS.bd.1.A18)

Secure Boot sollte aktiv sein. AppLocker ist zu strikt zu konfigurieren und zu aktiviert. Die Auswirkungen der Einstellungen und deren Änderungen sollten vorab getestet werden.

#### Prüfung der Sicherheitskonfiguration von Windows Server 2016 (SYS.bd.1.A19)

Die Sicherheitskonfiguration von Windows Server 2016 ist mittels geeigneter Tools regelmäßig zu überprüfen, zu dokumentieren und kontinuierlich zu verbessern.

#### Lokale Kommunikationsfilterung von Windows Server 2016 (SYS.bd.1.A20)

Die lokale Firewall des Windows Server 2016 sollte für eingehenden und ausgehenden Netzverkehr aktiviert und möglichst strikt eingestellt sein. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen sollte kryptografisch abgesichert sein.

Die lokale Windows Server 2016 Firewall oder ein installierte Firewall eines Dritt-Herstellers sind zentral zu administrieren.

### Windows Server 2019

#### Sichere Konfiguration eines Windows Server 2019 (SYS.bd.2.A5)

Die Windows Server 2019 Systeme müssen entsprechend den Anforderungen des Stands der Technik gehärtet werden. Um die Systemhärtung umzusetzen, müssen funktionsspezifische Sicherheitsvorlagen erstellt, gepflegt und angewendet werden. Für die Windows Server 2019 und gegebenenfalls auch weiteren Serversysteme einer bestimmten Einsatzklasse müssen Baselines erstellt, regelmäßig geprüft und fortgeschrieben werden. Vor der Installation von Servicepacks oder Enhancement-Packs auf produktiven IT-Systemen müssen im Rahmen des Patch- und Änderungsmanagements der <Institution> Prüfungen der Härtungsmaßnahmen erfolgen. Das System muss für das Patch- und Änderungsmanagement auf ein unterstütztes Service Level gehoben werden. Zusätzlich müssen alle Windows Server 2019 bei erhöhten Schutzbedarfsanforderungen einem geeigneten Monitoring unterliegen. Jede Entscheidung im Rahmen der Konfiguration von Windows Server 2019 ist zu begründen und zu dokumentieren.

#### Rollenbasierte Administration unter Windows Server 2019 (SYS.bd.2.A6)

Auf Basis von Windows PowerShell wird bei Windows Server 2019 mithilfe von Just Enough Administration (JEA) eine rollenbasierte Administration implementiert. Die rollenbasierte Administration wird so eingesetzt, dass die Administratoren nur auf die Bereiche eines IT-Systems beziehungsweise Netzes Zugriff erhalten, die in ihren Aufgabenbereich fallen. Zur etablierten rollenbasierten Administration wurde ein feingranulares rollenbasiertes Administrationskonzept nach dem Prinzip Least Privilege erstellt und etabliert. Für kritische Dienste ist eine Zwei-Faktor-Authentifizierung einzusetzen.

#### Sichere Authentisierung und Autorisierung in Windows Server 2019 (SYS.bd.2.A7)

Alle Benutzer müssen unter Windows Server 2019 Mitglieder der Sicherheitsgruppe „Geschützte Nutzer“ sein. Dienste- und Computer-Konten sollten hingegen nicht Mitglied von „Geschützte Nutzer“ sein. Dienste-Konten in Windows Server 2019 sind als Mitglieder der Gruppe „Managed Service Account“ zu hinterlegen. Der PPL-Schutz des Local Credential Store (LSA) ist zu aktivieren. Der Einsatz dynamischer Zugriffsregeln auf Ressourcen sollte bevorzugt werden. Mitarbeitende mit administrativen Rechten arbeiten auf ihren eigenen Clients mit beschränkten Rechten.

#### Hochverfügbarkeit und Storages Spaces unter Windows Server 2019 (SYS.bd.2.A8)

Für die Gewährleistung der Hochverfügbarkeit von Festplattenspeichern unter Windows Server 2019 sollte die Funktion „Storage Spaces“ genutzt werden. Durch „Storage Spaces“ sind redundante und flexible Festplattenspeicher zu erstellen. Wenn besonders hohe Verfügbarkeitsanforderungen an ein System bestehen, welches unter Windows Server 2019 betrieben wird, sind Maßnahmen aus der jeweiligen Anwendung zu berücksichtigen.

#### Einsatz der Virtual Machine Lastenausgleichsfunktion unter Windows Server 2019 (SYS.bd.2.A9)

Zur Optimierung der Auslastung von Knoten in einem Failovercluster sollten die Windows Server 2019 Funktion für den Lastenausgleich für Virtual Machine (VM) entsprechend den Schutzbedarfen konfiguriert und gesteuert werden. Von den verantwortlichen Administratoren sind die abgestimmten Vorgaben für den „VM-Lastenausgleich“ zu dokumentieren und regelmäßig zu aktualisieren.

#### Schutz vor Schadsoftware auf einem Windows Server 2019 (SYS.bd.2.A10)

Alle Server (außer Stand-Alone-Systeme ohne Netz-Anschluss und Anschluss für Wechselmedien) müssen vor dem ersten Verbinden mit einer Netzverbindung, einem mobilen Netz oder einem Wechselmedium in die etablierte Anti-Malware-Infrastruktur integriert werden. Die Protokollierung muss entsprechend den veröffentlichten Vorgaben vorgenommen werden. Die Administratoren müssen Alarmierungen bei Virenfunden durchführen, konfigurieren und regelmäßig auswerten. Zusätzlich muss eine automatisierte Auswertung der Alarme geprüft werden, da so Sicherheitslücken zeitnah erkannt und behandelt werden können.

Der Malware-Schutz muss die Szenarien „Hyper-V-Hosts“ und „Hochverfügbarkeitscluster“ berücksichtigen. Bei einem erhöhten Schutzbedarf muss für jeden Windows Server 2019 ein hostbasiertes Intrusion Detection oder Prevention System eingesetzt werden.

#### Enhanced Threat Detection unter Windows Server 2019 (SYS.bd.2.A11)

Um bösartiges Verhalten besser überwachen zu können sollte „Enhanced Threat Detection“ eingesetzt werden. Die gesammelten Informationen der „Enhanced Threat Detection“ sind an ein zentrales Analysetool und an ein SIEM weiterzuleiten. Eine Alarmierung bei böswilligem Verhalten beziehungsweise vorliegenden Bedrohungen ist einzurichten.

#### Sicherer Umgang mit Containern unter Windows Server 2019 (SYS.bd2.A12)

Bei „Windows Server Containern“ und „Hyper-V Containern“ sind ausschließlich OS Images zu nutzen. In Abhängigkeit vom Einsatzzweck und Schutzbedarf ist die zu verwendende Container-Variante zu wählen. Die Entscheidung für eine Variante sollte begründet und dokumentiert werden.

#### Einsatz von Containern unter Windows Server 2019 (SYS.bd.2.A13)

Beim Einsatz von Containern sollten die Anforderungen an die Sicherheit von Anfang an berücksichtigt werden. Beim Betrieb von Containern auf Basis von Windows Server 2019 sollte die Umsetzungsvariante mittels Hyper-V-Containern bevorzugt werden.

Beim Betrieb einer Containerlösung müssen die Verantwortlichen sicherstellen, dass der innerhalb des Containers verwendete Code aus einer bekannten und vertrauenswürdigen Quelle stammt. Es müssen in regelmäßigen Abständen Schwachstellen-Tests unter Zuhilfenahme von Schwachstellen-Analyse-Tools durchgeführt werden.

#### Einsatz von Shielded Virtual Machines von Windows Server 2019 (SYS.bd.2.A14)

Auf Basis des Schutzbedarfes und der Einsatzszenarien muss der Einsatz von „Shielded Virtual Machines“ geprüft werden. Für den Einsatz von „Shielded Virtual Machines“ muss ein vertrauenswürdiger Hyper-V-Host eingerichtet sein. Für die Verschlüsselung „Shielded Virtual Machines“ wird eine Guarded-Fabric-Instrastruktur vorausgesetzt, demzufolge müssen Host Guardian Services (HGS) und Guarded Hosts eingerichtet werden.

#### Einsatz von Credential Guard und Remote Credential Guard unter Windows Server 2019 (SYS.bd.2.A15)

Für die Sicherheit von Zugangsdaten sollte „Credential Guard“ oder „Remote Credential Guard“ bei Windows Server 2019 eingesetzt werden. Die Hardware-Sicherheit, die virtualisierungsbasierte Sicherheit und der Schutz gegen fortgeschrittene dauerhafte Bedrohungen sind bei „Credential Guard“ oder „Remote Credential Guard“ zu berücksichtigen. Für „Credential Guard“ ist auf domänenverbundenen Systemen das „Trusted Platform Module (TPM)“ zu aktivieren.

#### Einsatz von Device Guard unter Windows Server 2019 (SYS.bd.2.A16)

Der Schutz vor nicht vertrauenswürdiger Software sollte durch „Device Guard“ gewährleistet werden. Die Konfiguration von „Device Guard“ darf nur durch geschulte und verantwortliche Administratoren erfolgen. Bei erhöhtem Schutzbedarf von domänenverbundenen Systemen in virtuellen Umgebungen ist „Device Guard“ zu aktivieren. Der Einsatz von „Device Guard“ muss den Vorgaben des Patch- und Änderungsmanagements der <Institution> unterliegen.

#### Einsatz vom Control Flow Guard unter Windows Server 2019 (SYS.bd.2.A17)

Sofern Windows Server 2019 als Terminal-Server eingesetzt wird, ist zum Schutz vor Browser-Malware „Control Flow Guard“ zu etablieren. Die Kontrolle von „Indirect Calls“ in Programmen sind zum Schutz vor Exploits zu aktivieren.

#### Schutz der Systemintegrität von Windows Server 2019 (SYS.bd.2.A18)

Secure Boot sollte aktiv sein. AppLocker ist zu strikt zu konfigurieren und zu aktiviert. Die Auswirkungen der Einstellungen und deren Änderungen sollten vorab getestet werden.

#### Prüfung der Sicherheitskonfiguration von Windows Server 2019 (SYS.bd.2.A19)

Die Sicherheitskonfiguration von Windows Server 2019 ist mittels geeigneter Tools regelmäßig zu überprüfen, zu dokumentieren und kontinuierlich zu verbessern.

#### Lokale Kommunikationsfilterung von Windows Server 2019 (SYS.bd.2.A20)

Die lokale Firewall des Windows Server 2019 sollte für eingehenden und ausgehenden Netzverkehr aktiviert und möglichst strikt eingestellt sein. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen sollte kryptografisch abgesichert sein.

Die lokale Windows Server 2019 Firewall oder ein installierte Firewall eines Dritt-Herstellers sind zentral zu administrieren.

#### Verschlüsselung von virtuellen Netzwerken unter Windows Server 2019 (SYS.bd.2.A21)

Zur Vermeidung des unberechtigten Belauschens (mitschneiden bzw. abhören) der Netzkommunikation sollte die Verschlüsselung von virtuellen Netzwerken eingesetzt werden. Hierdurch wird die Sicherheit der Netz-Virtualisierungsplattform deutlich erhöht, da Daten im vollen Umfang verschlüsselt werden können, sowohl in der Ruhephase als auch im Transit.

#### Zentrale Verwaltung der Sicherheitsrichtlinien von Servern (SYS.bd.2.A22)

Alle Einstellungen des Servers sollten durch Nutzung eines zentralen Managementsystems verwaltet und entsprechend dem ermittelten Schutzbedarf sowie auf den internen Richtlinien basierend konfiguriert sein. Technisch nicht umsetzbare Konfigurationsparameter sind zu dokumentieren und mit dem Sicherheitsmanagement abgestimmt sowie begründet werden.

#### Sicherheit beim Fernzugriff über RDP unter Windows 2019 (SYS.bd.2.A23)

Die Auswirkungen auf die Konfiguration der lokalen Firewall sollten bei der Planung des Fernzugriffs berücksichtigt werden. Die Gruppe der berechtigten Benutzer und IT-Systeme für den Remote-Desktopzugriff (RDP) ist durch die Zuweisung entsprechender Berechtigungen festzulegen. Es sollten Konzepte berücksichtigt werden, um die übertragenen Anmeldeinformationen zu schützen (z.B. Remote Credential Guard oder RestrictedAdmin). In komplexen Infrastrukturen sollte das RDP-Zielsystem nur durch ein dazwischengeschaltetes RDP-Gateway erreicht werden können. Für die Verwendung von RDP sollte eine Prüfung und deren Umsetzung sicherstellen, dass die nachfolgend aufgeführten Komfortfunktionen im Einklang mit dem Schutzbedarf des Zielsystems stehen:

* die Verwendung der Zwischenablage,
* die Einbindung von Wechselmedien und Netzlaufwerken sowie
* die Nutzung der Dateiablagen, weiteren Geräten und Ressourcen, wie z.B. Smartcard-Lesegeräten.

Es sind die freigegebenen kryptografischen Protokolle und Algorithmen der <Institution> einzusetzen.

Sofern der Einsatz von Remote-Desktopzugriffen nicht vorgesehen ist, ist dieser vollständig zu deaktivieren.

## Maßnahmen bei erhöhtem Schutzbedarf

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

### Allgemeiner Server

#### Mehr-Faktor-Authentisierung (SYS.1.1.A26 - CIA)

Bei höherem Schutzbedarf ist eine sichere Mehr-Faktor-Authentisierung für den Zugang zum Server einzurichten. Insbesondere gilt dies für alle administrativen Zugänge zum Server.

#### Hostbasierte Angriffserkennung (SYS.1.1.A27 - CA)

Hostbasierte Angriffserkennungssysteme (Host-based Intrusion Detection Systems (HIDS) bzw. Host-based Intrusion Prevention Systems (HIPS)) sollten eingesetzt werden, um das Systemverhalten des Servers auf Anomalien und Missbrauch hin zu überwachen. Sofern HIDS/HIPS-Mechanismen eingesetzt werden, sind diese geeignet auszuwählen, zu konfigurieren und ausführlich zu testen. Im Falle einer Angriffserkennung sind die Verantwortlichen für den Server in geeigneter Weise zu alarmieren.

Über Betriebssystem-Mechanismen oder geeignete Zusatzprodukte sollten Veränderungen an Systemdateien und Konfigurationseinstellungen überprüft, eingeschränkt und gemeldet werden.

#### Steigerung der Verfügbarkeit durch Redundanz (SYS.1.1.A28 - A)

Server mit hohen Verfügbarkeitsanforderungen sind gegen Ausfälle in geeigneter Weise zu schützen. Hierzu sollten mindestens geeignete Redundanzen verfügbar sein sowie Wartungsverträge mit den Lieferanten abgeschlossen werden. Es ist zu prüfen, ob bei sehr hohen Anforderungen GEO-redundante Hochverfügbarkeitsarchitekturen mit automatischem Failover erforderlich sind.

#### Einrichtung einer Testumgebung (SYS.1.1.A29 - CIA)

Um Veränderungen am System oder der Konfiguration des Servers testen zu können ohne den produktiven Betrieb zu gefährden, sind entsprechende Testsysteme (bspw. funktionale und architektonische Referenzen der produktiven Server) vorzuhalten oder bei Bedarf bereitzustellen. Für Anwendungssysteme sollten geeignete Testdaten generiert werden, die keine vertraulichen oder personenbezogenen Inhalte der produktiven Daten enthalten.

Die Ergebnisse der durchgeführten Tests sind geeignet zu dokumentieren.

#### Ein Dienst pro Server (SYS.1.1.A30 - CIA)

Abhängig von der Bedrohungslage und dem Schutzbedarf der Dienste ist auf einem Server nur jeweils ein Dienst (Service) zu betrieben.

#### Application Whitelisting (SYS.1.1.A31 - CA)

Über eine Application-Freigabeliste ist sicherzustellen, dass auf dem Server nur freigegebene Software installiert und ausgeführt wird. Die Anwendungssoftware wird nur in dafür vorgesehene Verzeichnisse installiert. Anwendungen außerhalb dieser Verzeichnisse können nicht ausgeführt werden.

#### Zusätzlicher Schutz von privilegierten Anmeldeinformationen (SYS.1.1.A32 - CA)

Passwörter für administrative Konten sollten in mehrere Teile zerlegt werden. Um diese Anmeldeinformationen zusätzlich zu schützen, sollte das Vier-Augen-Prinzip angewendet werden. Auch administrative Konten sollten so eingerichtet werden, dass diese nach einer vorher festgelegten Anzahl fehlerhafter Anmeldeversuche gesperrt werden.

#### Aktive Verwaltung der Wurzelzertifikate (SYS.1.1.A33 - CIA)

Im Zuge der Beschaffung und Installation des Servers sollte dokumentiert werden, welche Wurzelzertifikate für den Betrieb des Servers notwendig sind. Auf dem Server sollten lediglich die für den Betrieb notwendigen und vorab dokumentierten Wurzelzertifikate enthalten sein. Es sollte regelmäßig überprüft werden, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der <Institution> entsprechen. Es sind alle auf dem Server vorhandenen Zertifikatsspeicher in die Prüfung einzubeziehen.

#### Festplattenverschlüsselung (SYS.1.1.A34 - CI)

Bei erhöhtem Schutzbedarf sollten die Datenträger des Servers mit einem als sicher geltenden Produkt bzw. Verfahren verschlüsselt werden. Dies sollte auch für virtuelle Maschinen mit produktiven Daten gelten. Es sollte nicht nur ein TPM allein als Schlüsselschutz dienen. Das Wiederherstellungspasswort ist an einem geeigneten sicheren Ort zu speichern. Bei sehr hohen Anforderungen an die Vertraulichkeit oder Abstreitbarkeit ist eine Full Volume Encryption zu etablieren.

### Windows Server 2012 R2

#### Festplattenverschlüsselung bei Windows Server 2012 R2 (SYS.1.2.2.A10 - CI)

Entsprechend des Schutzbedarfs des Windows Servers 2012 R2 sollten die Festplatten verschlüsselt werden. Sofern die Festplattenverschlüsselung eingesetzt wird, sind hierfür die von der <Institution> freigegeben kryptographischen Algorithmen und Protokolle zu verwenden.

#### Angriffserkennung bei Windows Server 2012 R2 (SYS.1.2.2.A11 - CIA)

Der Windows Server 2012 R2 ist in das zentrale Monitoring einzubinden. Bei Überschreitung von Grenzwerten sollte eine Alarmierung erfolgen.

Wird der Grenzwert für gescheiterte Entschlüsselungsversuche von verschlüsselten Festplatten-Partitionen überschritten, ist diese Partitionen zu sperren.

#### Redundanz und Hochverfügbarkeit (SYS.1.2.2.A12 - CIA)

Sind die Anforderungen an die Verfügbarkeit entsprechend hoch, ist zu prüfen, welche Verfügbarkeitsanforderungen durch Betriebssystemfunktionen wie Distributed File System (DFS), ReFS, Failover Cluster und Network Load Balancing bzw. NIC-Teaming (LBFO) umgesetzt oder unterstützt werden können. Für Außenstellen ist der Branch Cache zu aktivieren.

#### Starke Authentifizierung bei Windows Server 2012 R2 (SYS.1.2.2.A13 - CIA)

Ist der Schutzbedarf eines Servers entsprechend hoch, ist der kompromittierende Zugang zum Server durch die Verwendung einer Mehrfaktorauthentisierung zu verhindern.

Die rollenbasierte Administration für verschiedene Serverfunktionen ist zu definieren und umzusetzen.

#### Herunterfahren verschlüsselter Server und virtueller Maschinen (SYS.1.2.2.A14 - C)

Nichtbenötigte Server mit verschlüsselten Daten sind herunterzufahren oder befinden sich im Ruhezustand.

### Windows Server 2016

#### Herunterfahren verschlüsselter Server und virtueller Maschinen (SYS.bd.1.A21 )

Die Schlüssel für die Entschlüsselung von Festplatten sind erst nach einer Interaktion durch einen berechtigten Administrator bereitzustellen. Falls diese Lösung nicht in Frage kommt, sollte die Bereitstellung durch eine protokollierte technische Anfrage im Netz oder an dem Active-Directory erfolgen. Für den geregelten Prozess sollten „BitLocker“ beziehungsweise die „Geräteverschlüsselung“ in einem nicht ausschließlich TPM-basierten Modus aktiviert werden. Der „Key-Protector“ sollte nicht permanent angesteckt sein. Alle nicht benötigten Server und virtuellen Maschinen sollten heruntergefahren oder in einen Ruhezustand versetzt werden. Das Herunterfahren oder Aktivieren des Ruhezustands von Servern oder virtuellen Maschinen erfolgt immer möglichst automatisiert.

#### Einsatz eines zentralen und programmierbaren Automatisierungspunktes (SYS.bd.1.A22)

Die Verwaltung, Konfiguration, Überwachung und Behebung der virtuellen beziehungsweise physischen Netzinfrastruktur sollten mittels Netzwerk-Controller nur durch berechtigte Mitarbeitenden erfolgen. Die Verwendung von Features zum „Firewall Management“, „Software Load Balancer Management“, „Virtual Network Management“ und „RAS Gateway Management“ ist festzulegen, zu dokumentieren und regelmäßig zu aktualisieren.

#### Paralleles Betriebssystemupgrade eines Clusters (SYS.bd.1.A23)

Mit dem parallelen Betriebssystemupgrade eines Windows-Server-Clusters sollte sichergestellt werden, dass vereinbarte Ausfallzeiten in Service Level Agreements eingehalten werden. Die Administratoren der Windows Server 2016 binden beim Cluster-Update von Windows Server 2012 R2 zu Windows Server 2016 die bestehenden Knoten optimal in Windows Server 2016 ein. Ältere benötigte Cluster-Knoten werden bei Aktualisierung übernommen und dürfen nicht ausgesperrt werden. Der Vorgang für das parallele Cluster-Betriebssystemupgrade muss dokumentiert werden. Diese dokumentierten Anforderungen werden regelmäßig aktualisiert.

#### Schutz der Anmeldeinformationen unter Windows Server 2016 (SYS.bd.1.A24)

Sofern Windows Server 2016 auf einem Hardware-System direkt (nativ) installiert ist oder Nested Virtualization zur Verfügung steht, sollte der Virtual Secure Mode (VSM) aktiviert werden. Dabei sollte berücksichtigt werden, dass Prozesse, die durch den Secure Kernel bzw. den Isolated User Mode (IUM) geschützt werden, nicht mehr für forensische Untersuchungen zugänglich sind. Zusätzlich sollte der Windows Defender Credential Guard gegen Angriffe auf die im System gespeicherten Authentisierungstoken und -hashes aktiviert werden. Die Netzanmeldung von lokalen Konten sollte verboten werden.

#### Verwendung der Windows PowerShell (SYS.bd.1.A25)

Die PowerShell-Ausführung sollte zentral protokolliert und die Protokolle überwacht werden. Die Ausführung von PowerShell-Skripten sollte mit dem Befehl "Set-ExecutionPolicy AllSigned" eingeschränkt werden, um zu verhindern, dass unsignierte Skripte (versehentlich) ausgeführt werden. Ältere Windows PowerShell-Versionen sind zu deaktivieren. Der Einsatz des PowerShell Constrained Language Mode sollte geprüft werden.

### Windows Server 2019

#### Herunterfahren verschlüsselter Server und virtueller Maschinen (SYS.bd.2.A24 )

Die Schlüssel für die Entschlüsselung von Festplatten sind erst nach einer Interaktion durch einen berechtigten Administrator bereitzustellen. Falls diese Lösung nicht in Frage kommt, sollte die Bereitstellung durch eine protokollierte technische Anfrage im Netz oder an dem Active-Directory erfolgen. Für den geregelten Prozess sollten „BitLocker“ beziehungsweise die „Geräteverschlüsselung“ in einem nicht ausschließlich TPM-basierten Modus aktiviert werden. Der „Key-Protector“ sollte nicht permanent angesteckt sein. Alle nicht benötigten Server und virtuellen Maschinen sollten heruntergefahren oder in einen Ruhezustand versetzt werden. Das Herunterfahren oder Aktivieren des Ruhezustands von Servern oder virtuellen Maschinen erfolgt immer möglichst automatisiert.

#### Einsatz eines zentralen und programmierbaren Automatisierungspunktes (SYS.bd.2.A25)

Die Verwaltung, Konfiguration, Überwachung und Behebung der virtuellen beziehungsweise physischen Netzinfrastruktur sollte mittels Netzwerk-Controller nur durch berechtigte Mitarbeitenden erfolgen. Die Verwendung von Features zum „Firewall Management“, „Software Load Balancer Management“, „Virtual Network Management“ und „RAS Gateway Management“ ist festzulegen, zu dokumentieren und regelmäßig zu aktualisieren.

#### Schutz der Anmeldeinformationen unter Windows Server 2019 (SYS.bd.2.A26)

Sofern Windows Server 2019 auf einem Hardware-System direkt (nativ) installiert ist oder Nested Virtualization zur Verfügung steht, sollte der Virtual Secure Mode (VSM) aktiviert werden. Dabei sollte berücksichtigt werden, dass Prozesse, die durch den Secure Kernel bzw. den Isolated User Mode (IUM) geschützt werden, nicht mehr für forensische Untersuchungen zugänglich sind. Zusätzlich sollte der Windows Defender Credential Guard gegen Angriffe auf die im System gespeicherten Authentisierungstoken und -hashes aktiviert werden. Die Netzanmeldung von lokalen Konten sollte verboten werden.

#### Verwendung der Windows PowerShell (SYS.bd.2.A27)

Die PowerShell-Ausführung sollte zentral protokolliert und die Protokolle überwacht werden. Die Ausführung von PowerShell-Skripten sollte mit dem Befehl "Set-ExecutionPolicy AllSigned" eingeschränkt werden, um zu verhindern, dass unsignierte Skripte (versehentlich) ausgeführt werden. Ältere Windows PowerShell-Versionen sind zu deaktivieren. Der Einsatz des PowerShell Constrained Language Mode sollte geprüft werden.