Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.2.3 Windows Server

1. Beschreibung

1.1. Einleitung

Mit Windows Server bietet Microsoft ein Betriebssystem für Server an. Bei den Hauptversionen 2016, 2019 und 2022 von Windows Server handelt es sich um sogenannte Langzeit-Versionen (Long-Term Servicing Channel, LTSC), die jeweils auf der Codebasis des Client-Betriebssystems Windows 10 basieren. Wie bei Windows 10 liefert Microsoft auch mit Windows Server zunehmend cloudbasierte Funktionen und Anwendungen sowie Schnittstellen zur Microsoft Azure Cloud-Plattform mit aus.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist der Schutz von Informationen, die durch Server-Systeme auf Basis von Windows Server 2016, 2019 und 2022 im Regelbetrieb verarbeitet, gespeichert und darüber übertragen werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.2.3 *Windows Server* ist auf alle Server-Systeme anzuwenden, auf denen das Betriebssystem Microsoft Windows Server in den Versionen 2016, 2019 oder 2022 eingesetzt wird. Für Windows Server 2012 ist stattdessen der Baustein SYS.1.2.2 *Windows Server 2012* zu modellieren.

Dieser Baustein konkretisiert und ergänzt die plattformunabhängigen Sicherheitsaspekte für Server, die im Bausteinen SYS.1.1 *Allgemeiner Server* behandelt werden, um Besonderheiten von Windows Server in den genannten Versionen. Dementsprechend sind die beiden Bausteine immer gemeinsam anzuwenden.

In diesem Baustein geht es um die grundlegende Absicherung auf Betriebssystemebene mit bordeigenen Mitteln, unabhängig vom Einsatzzweck des Servers. Sicherheitsanforderungen möglicher Serverrollen und -funktionen wie beispielsweise Fileserver (APP.3.3 *Fileserver*) oder Webserver (APP.3.2 *Webserver*) sind Gegenstand eigener Bausteine, genauso wie das Thema Virtualisierung (SYS.1.5 *Virtualisierung*).

Darüber hinaus sind im Funktionsumfang einiger Betriebssystemvarianten auch weitere Anwendungen vorinstalliert, wie etwa der Microsoft Internet Explorer als Browser. Für diese Anwendungen sind die entsprechenden Bausteine zu modellieren.

Im Rahmen dieses Bausteins wird von einer Aufnahme als „Member Server“ in eine Active-Directory-Domäne ausgegangen, wie sie in Institutionen üblich ist. Besonderheiten von Stand-alone-Systemen

werden nur punktuell dort erwähnt, wo die Unterschiede besonders relevant erscheinen. Anforderungen zum Thema Active Directory sind Bestandteil des Bausteins APP.2.2 *Active Directory Domain Services*. Für die Nutzung der teils mitgelieferten Funktionen und Anwendungen von Cloud-Diensten sowie Schnittstellen zwischen der Microsoft Azure Cloud-Plattform und Windows Server muss der Baustein OPS.2.2 *Cloud-Nutzung* angewendet werden, in dem auch Gefährdungen und generelle Anforderungen bei der Cloud-Nutzung behandelt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.1.2.3 *Windows Server* von besonderer Bedeutung.

2.1. Unbedachte Cloud-Nutzung

Windows Server bietet an verschiedenen Stellen die Möglichkeit, Cloud-Dienste zu nutzen, ohne dass dafür Drittsoftware installiert werden muss. Hierzu gehören beispielsweise Microsoft Azure Online Backup oder die Online-Speicherung von BitLocker-Wiederherstellungsschlüsseln. Während Cloud-Dienste mögliche Vorteile, beispielsweise hinsichtlich der Verfügbarkeit, bieten können, bestehen bei unbedachtem Einsatz beispielsweise Risiken für die Vertraulichkeit sowie eine Abhängigkeit von Dienstleistenden. So können Daten über Cloud-Dienste in die Hände unberechtigter Dritter gelangen. Dabei kann es sich sowohl um Kriminelle als auch um staatliche Akteure handeln. Wird ein Cloud-Dienst durch den Anbieter beendet, kann dies erhebliche Auswirkungen auf die eigenen Geschäftsprozesse haben.

2.2. Kompromittierung von Fernzugängen

Da Windows Server über eine Vielzahl von Möglichkeiten verfügt, aus der Ferne verwaltet zu werden, können diese grundsätzlich auch missbraucht werden. Fernzugänge wie z. B. RDP- oder WinRM-Sitzungen können durch unsichere oder unsicher verwendete Protokolle, schwache Authentisierungsverfahren (z. B. schwache Passwörter) oder fehlerhafte Konfiguration für Dritte erreichbar sein. Hierdurch können der Server und die dort gespeicherten Informationen weitgehend kompromittiert werden. Oft können auf diese Weise auch weitere mit dem Server verbundene IT-Systeme kompromittiert werden.

2.3. Telemetrie von Windows Server

Windows Server sendet standardmäßig sogenannte Diagnosedaten an den Hersteller Microsoft. Zusätzlich kann Microsoft über den in Windows Server integrierten Telemetriedienst gezielt Informationen von einem Server abfragen. Abhängig vom Telemetrie-Level schließt dies beispielsweise den Zugriff auf Absturzabbilder des Speichers (sog. „Crash Dumps“) sowie den Zugriff auf Betriebssystemereignisse auf dem Server mit ein. Es besteht die Gefahr, dass die Diagnose- und Telemetriedaten schützenswerte Informationen enthalten, die auf diesem Weg an Dritte gelangen können.

2.4. Eingeschränkte Forensik bei der Nutzung des Virtual Secure Mode (VSM)

Durch die Nutzung des Virtual Secure Mode (VSM) werden forensische Untersuchungen, z. B. zur Sicherheitsvorfallbehandlung, eingeschränkt oder erschwert. Prozesse, die durch den Secure Kernel oder den Isolated User Mode (IUM) geschützt werden, sind nicht mehr zugänglich. Beispielsweise

können Speicherabbilder dieser Prozesse aufgrund kryptografischer Maßnahmen nicht ausgewertet werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.2.3 *Windows Server* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

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

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

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

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.2.3.A1 Planung von Windows Server (B)

Es MUSS eine begründete und dokumentierte Entscheidung für eine geeignete Edition von Windows Server getroffen werden. Der Einsatzzweck des Servers sowie die Einbindung ins Active Directory MÜSSEN dabei spezifiziert werden. Die Nutzung von mitgelieferten Cloud-Diensten im Betriebssystem MUSS grundsätzlich abgewogen und gründlich geplant werden. Wenn nicht benötigt, MUSS die Einrichtung von Microsoft-Konten auf dem Server blockiert werden.

SYS.1.2.3.A2 Sichere Installation von Windows Server (B)

Wenn vom Funktionsumfang her ausreichend, MUSS die Server-Core-Variante installiert werden. Andernfalls MUSS begründet werden, warum die Server-Core-Variante nicht genügt.

SYS.1.2.3.A3 Telemetrie- und Nutzungsdaten unter Windows Server (B)

Um die Übertragung von Diagnose- und Nutzungsdaten an Microsoft stark zu reduzieren, MUSS das Telemetrie-Level 0 (Security) auf dem Windows Server konfiguriert werden. Wenn diese Einstellung nicht wirksam umgesetzt wird, dann MUSS durch geeignete Maßnahmen, etwa auf Netzebene, sichergestellt werden, dass die Daten nicht an den Hersteller übertragen werden.

3.2. Standard-Anforderungen

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

SYS.1.2.3.A4 Schutz vor Ausnutzung von Schwachstellen in Anwendungen (S)

Maßnahmen zum Schutz vor Exploits SOLLTEN für alle Programme und Dienste aktiviert werden, die den Exploit-Schutz von Windows (vgl. Verweis in Kapitel 4.1 *Wissenswertes*) unterstützen.

SYS.1.2.2.A5 Sichere Authentisierung und Autorisierung in Windows Server (S)

In Windows Server SOLLTEN alle Konten von Benutzenden Mitglied der Sicherheitsgruppe „Protected Users“ sein. Konten für Dienste und Computer SOLLTEN NICHT Mitglied von „Protected Users“ sein. Dienste-Konten in Windows Server SOLLTEN Mitglied der Gruppe „Managed Service Account“ sein.

SYS.1.2.3.A6 Sicherheit beim Fernzugriff über RDP (S)

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTEN bei der Planung des Fernzugriffs berücksichtigt werden. Die Gruppe der Berechtigten und IT-Systeme für den Remote-Desktopzugriff (RDP) SOLLTE durch die Zuweisung entsprechender Berechtigungen festgelegt werden. Es SOLLTEN Mechanismen des Betriebssystems 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, von weiteren Geräten und Ressourcen, wie z. B. Smartcard-Lesegeräten.

Die eingesetzten kryptografischen Protokolle und Algorithmen SOLLTEN den internen Vorgaben der Institution entsprechen.

Sofern der Einsatz von Remote-Desktopzugriffen nicht vorgesehen ist, SOLLTEN diese vollständig deaktiviert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

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

SYS.1.2.3.A7 Verwendung der Windows PowerShell (H)

Die PowerShell-Ausführung SOLLTE zentral protokolliert werden. Die erzeugten Protokolle SOLLTEN geeignet 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 SOLLTEN deaktiviert werden. Der Einsatz des PowerShell Constrained Language Mode SOLLTE geprüft werden. Zur Einschränkung der Windows PowerShell SOLLTE bei Windows Server mithilfe von Just Enough Administration (JEA) eine rollenbasierte Administration implementiert werden.

SYS.1.2.3.A8 Nutzung des Virtual Secure Mode (VSM) (H)

Bei der Nutzung des Virtual Secure Mode (VSM) SOLLTE berücksichtigt werden, dass forensische Untersuchungen, z. B. zur Sicherheitsvorfallbehandlung, eingeschränkt oder erschwert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Der Hersteller Microsoft stellt unter anderem folgende weiterführende Informationen zu Windows Server bereit:

- Windows Server - Dokumentation
  https://docs.microsoft.com/en-us/windows-server/
- Neuerungen in Windows Server 2019:
  https://docs.microsoft.com/en-us/windows-server/get-started-19/whats-new-19
- Neuerungen in Windows Server 2022:
  https://docs.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022
- Vergleich der Standard- und Datacenter-Editionen von Windows Server 2019:
  https://docs.microsoft.com/en-us/windows-server/get-started-19/editions-comparison-19
- Vergleich der Standard- und Datacenter-Editionen von Windows Server 2022:
  https://docs.microsoft.com/en-us/windows-server/get-started/editions-comparison-windows-server-2022
- Fixed Lifecycle-Richtlinie
  https://support.microsoft.com/en-us/help/14085/fixed-lifecycle-policy
- Entfernte oder zur Ersetzung vorgesehene Features in Windows Server 2019:
  https://docs.microsoft.com/en-us/windows-server/get-started-19/removed-features-19
- Security and Assurance (Übersicht):
  https://docs.microsoft.com/en-us/windows-server/security/security-and-assurance
- Microsoft Security Compliance Toolkit 1.0:
  https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10
- Anpassen des Exploit-Schutzes
  https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-protection
- Schutz und Verwaltung von Anmeldeinformationen
  https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/credentials-protection-and-management
- Schützen von Remote Desktop Anmeldeinformationen mit Windows Defender Remote Credential Guard
  https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard
- Konfigurieren von Windows-Diagnosedaten in Ihrer Organisation
  https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization
- Liste von Sicherheitsereignissen unter Windows Server:
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
- Windows Server Guidance to protect against Speculative Execution:
  https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-speculative-execution
- Übersicht zur Windows-Authentifizierung
  https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-overview

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“, insbesondere in Area SY1.2 Server Configuration, Vorgaben für den Einsatz von Servern.

Das National Institute of Standards and Technology (NIST) stellt das Dokument „Guide to General Server Security: NIST Special Publication 800-123“, Juli 2008 zur Verfügung.

Das BSI stellt im Rahmen der Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10 (SiSyPHuS Win10), Empfehlungen zur sicheren Konfiguration und Deaktivierung von Telemetrie zur Verfügung, die auch auf Windows Server zutreffen: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html