SYS: IT-Systeme

SYS.1.2.3: Windows Server 2019

1 Beschreibung

1.1 Einleitung

Mit Windows Server 2019 hat Microsoft im November 2018 ein Betriebssystem für Server auf den Markt gebracht, das in drei Editionen (Standard, Datacenter, Essentials) angeboten wird. Windows Server 2019 ist eine Langzeit-Version (LTSC) und basiert auf der Codebasis des Client-Betriebssystems Windows 10 (Version 1809). Das Ablaufdatum für den Mainstream Support bzw. den Extended Support („End-of-Life", EOL) von Windows Server 2019 ist, nach der sogenannten Fixed Lifecycle-Richtlinie, der 09.01.2024 (Mainstream Support) bzw. der 09.01.2029 (Extended Support). Wie bereits im Client-Betriebssystem Windows 10, liefert Microsoft auch mit Windows Server 2019 zunehmend cloudbasierten Funktionen und Anwendungen sowie Schnittstellen zur Microsoft Azure Cloud-Plattform mit aus.

1.2 Zielsetzung

Das Ziel dieses Bausteins ist der Schutz von Informationen und Prozessen, die durch Server-Systeme auf Basis von Windows Server 2019 im Regelbetrieb verarbeitet bzw. gesteuert werden.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.1.2.3 *Windows Server 2019* ist für alle Server-Systeme anzuwenden, auf denen das Betriebssystem Microsoft Windows Server 2019 eingesetzt wird.

Dieser Baustein konkretisiert und ergänzt die Aspekte, die im Bausteinen SYS.1.1 *Allgemeiner Server* behandelt werden, um Besonderheiten von Windows Server 2019.

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*. Für die Nutzung der teils mitgelieferten Funktionen und Anwendungen von Cloud-Diensten sowie Schnittstellen zwischen der Microsoft Azure Cloud-Plattform und Windows Server 2019 muss der Baustein OPS.2.2 *Cloud-Nutzung* angewendet werden, in dem auch Gefährdungen und generelle Anforderungen bei der Cloud-Nutzung behandelt werden.

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

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.1.2.3 *Windows Server 2019* von besonderer Bedeutung:

2.1 Unzureichende Planung von Windows Server 2019

Windows Server 2019 ist ein komplexes Betriebssystem mit einer großen Anzahl an Funktionen und Konfigurationsoptionen. Bei der Konfiguration in der Domäne und bei der Vernetzung mit anderen IT-Systemen und Diensten gibt es sehr viele Möglichkeiten. Auch wenn moderne Windows-Versionen in vielen Bereichen gute Standardeinstellungen mitbringen, ist die Grundkonfiguration immer noch nicht in jedem Fall die sicherste. Dies kann bei unzureichender Planung zu einer Vielzahl von Schwachstellen und Schwächen durch Konfiguration führen, die von unberechtigten Dritten leicht ausgenutzt werden können. Werden außerdem nicht schon vor der Installation zentrale Entscheidungen getroffen, wird Windows Server 2019 in einem unsicheren und undefinierten Zustand ausgeführt, der sich nachträglich kaum mehr beheben lässt.

2.2 Unbedachte Cloud-Nutzung

Windows Server 2019 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 ggf. Vorteile, beispielsweise hinsichtlich der Verfügbarkeit, bieten können, bestehen bei unbedachtem Einsatz Risiken für die Vertraulichkeit sowie eine Abhängigkeit von Dienstleistern. So können Daten über Cloud-Dienste in die Hände unberechtigter Dritter gelangen. Dabei kann es sich sowohl um kriminelle Angreifer als auch um staatliche Akteure handeln. Wird ein Cloud-Dienst durch den Anbieter abgekündigt, kann dies erhebliche Auswirkungen auf die eigenen Geschäftsprozesse bzw. Fachaufgaben haben.

2.3 Fehlerhafte Administration von Windows-Servern

Windows Server 2019 wurde im Vergleich zu den Vorgängerversionen um eine Vielzahl neuer Funktionen erweitert. Bei anderen (bekannten) Features haben sich Teilfunktionen, Parameter oder Standardkonfigurationen verändert. Sind die Administratoren nicht ausreichend in den Besonderheiten der IT-Systeme geschult, drohen Konfigurationsfehler und menschliche Fehlhandlungen, die neben der Funktionalität auch die Sicherheit des IT-Systems beeinträchtigen können.

Eine besondere Gefahr stellen uneinheitliche Windows-Server-Sicherheitseinstellungen dar (z. B. bei SMB, RPC oder LDAP). Wenn die Konfiguration nicht systematisch und zentral geplant, dokumentiert, überprüft und nachgehalten wird, droht ein sogenannter Konfigurationsdrift. Je mehr sich die konkreten Konfigurationen funktional ähnlicher Systeme unbegründet und undokumentiert auseinander bewegen, desto schwieriger wird es, einen Überblick über den Status quo zu behalten und die Sicherheit ganzheitlich und konsequent aufrechtzuerhalten.

2.4 Unsachgemäßer Einsatz von Gruppenrichtlinien (GPOs)

Gruppenrichtlinien (Group Policy Objects, GPOs) sind eine nützliche und mächtige Art, viele (Sicherheits-) Aspekte von Windows Server 2019 zu konfigurieren, insbesondere in einer Domäne. Bei der großen Zahl möglicher Einstellungen passiert es leicht, versehentlich widersprüchliche oder inkompatible Einstellungen zu setzen oder Themenbereiche zu vergessen. Dies führt bei unsystematischer Vorgehensweise mindestens zu Betriebsstörungen, die teilweise nur schwer zu beheben sind, und schlimmstenfalls zu schwerwiegenden Schwachstellen auf dem Server oder auf verbundenen Clients. Insbesondere falsch verstandene Vererbungsregeln und Filter können dazu führen, dass GPOs gar nicht auf ein System angewendet werden.

2.5 Integritätsverlust schützenswerter Informationen oder Prozesse

Windows Server 2019 verfügt über eine Vielzahl von Funktionen, um die Integrität von durch das Betriebssystem verarbeiteten Informationen zu schützen. Jede einzelne dieser Funktionen kann mit Schwachstellen behaftet sein. Zudem mangelt es häufig an einer konsequenten Konfiguration, nicht zuletzt aus Gründen der vermuteten Benutzerfreundlichkeit oder Bequemlichkeit. Informationen und Prozesse können so durch unbefugte Mitarbeiter oder externe Angreifer verfälscht und oftmals sogar die Spuren verwischt werden. Häufig werden auch Schadprogramme eingesetzt, um Informationen aus der Ferne zu manipulieren.

2.6 Unberechtigtes Erlangen oder Missbrauch von Administratorrechten

Die reguläre Arbeit mit Administratorrechten, um beispielsweise Aufgaben und Tätigkeiten zu erledigen, die auf einem Client-System grundsätzlich als Standardbenutzer vorgesehen und möglich sind, stellt auf einem Server ein Sicherheitsrisiko dar. Sind gesonderte administrative Konten nicht auf die minimal notwendigen Rechte zur Durchführung administrativer Tätigkeiten beschränkt („Least Privilege"-Prinzip), können Angreifer bei Übernahme solcher Konten weitreichende Rechte auf dem Server oder weiteren IT-Systemen ausüben und hierbei hohen Schaden verursachen. Auch ein Missbrauch von Rechten durch legitime Administratoren ist ein relevantes Schadensszenario. Da die Rollen oft sehr mächtig sind, sind hier die Auswirkungen in der Regel beträchtlich, insbesondere bei Domänenadministratoren. Auch ohne Passwörter zu erraten oder zu brechen, können Angreifer z. B. durch sogenannte Pass-the-Hash-Verfahren geeignete Credentials auslesen und missbrauchen, um sich lateral im Netz weiterzubewegen.

2.7 Kompromittierung von Fernzugängen

Da Windows Server 2019 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-Benutzersitzungen können durch unsichere bzw. unsicher verwendete Protokolle, schwache Authentifizierung (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.

2.8 Telemetrie-Funktion von Windows Server 2019

Windows Server 2019 sendet fortlaufend sogenannte Diagnosedaten an den Hersteller Microsoft. Zusätzlich kann Microsoft über den in Windows Server 2019 integrierten Telemetrie-Dienst gezielt Informationen von einem Server abfragen. Im Telemetrie-Level „Enhanced" bzw. „Erweitert", der auf Windows Server 2019 die Standard-Diagnosestufe ist, schließt dies beispielsweise den Zugriff auf (vollständige) Absturzabbilder des Speichers (sog. „crash dumps") sowie den Zugriff auf Betriebssystemereignisse auf dem Server mit ein. Es besteht die Gefahr, dass die Diagnose- bzw. Telemetriedaten schützenswerte Informationen enthalten, die auf diesem Weg an Dritte gelangen können.

2.9 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 bzw. erschwert. Prozesse, die durch den Secure Kernel bzw. dem 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 2019* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der

Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	-

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.1.2.3 *Windows Server 2019* vorrangig erfüllt werden.

SYS.1.2.3.A1 Planung von Windows Server 2019 (B)

Der Einsatz von Windows Server 2012 MUSS vor der Installation sorgfältig geplant werden. Die Anforderungen an die Hardware MÜSSEN vor der Beschaffung geprüft werden. Es MUSS eine begründete und dokumentierte Entscheidung für eine geeignete Edition des Windows Server 2019 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 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 2019 (B)

Der vollständige Installations- und Konfigurationsvorgang SOLLTE innerhalb einer gesonderten und von Produktivsystemen abgetrennten Installationsumgebung („Staging-Umgebung“) vorgenommen werden. Es DÜRFEN KEINE anderen als die benötigten Serverrollen und Features bzw. Funktionen oder sonstige Software und Dienste installiert werden. Wenn vom Funktionsumfang her ausreichend, MUSS die Server-Core-Variante installiert werden. Andernfalls MUSS begründet werden, warum die Server-Core-Variante nicht genügt. Der Server MUSS bereits während der Installation auf einen aktuellen Patch-Stand gebracht werden.

SYS.1.2.2.A3 Sichere Konfiguration von Windows Server 2019 (B)

Mehrere wesentliche Funktionen bzw. Rollen SOLLTEN NICHT durch einen einzigen Server erfüllt, sondern geeignet aufgeteilt werden. Vor Inbetriebnahme SOLLTE das System grundlegend gehärtet werden. Alle sicherheitsrelevanten Einstellungen SOLLTEN bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft werden. Dafür SOLLTEN Sicherheitsrichtlinien, unter Berücksichtigung der Empfehlungen des Betriebssystemherstellers und des voreingestellten Standardverhaltens, konfiguriert werden, sofern das Standardverhalten nicht anderen Anforderungen aus dem IT-Grundschutz oder der Institution widerspricht. Die Entscheidungen SOLLTEN dokumentiert und begründet werden. Sicherheitsrichtlinien SOLLTEN in jedem Fall gesetzt werden, auch dann, wenn das voreingestellte Standardverhalten dadurch nicht verändert wird.

SYS.1.2.3.A4 Sichere Administration von Windows Server 2019 (B)

Der Server DARF NICHT zur Erledigung von Aufgaben und Tätigkeiten verwendet werden, die grundsätzlich auf einem Client-System aus- und durchgeführt werden können. Insbesondere DÜRFEN vorhandene Anwendungen, wie Webbrowser, auf dem Server NICHT für das Abrufen von Informationen aus dem Internet oder das Herunterladen von Software, Treibern und Updates verwendet werden. Die Administration des Servers SOLLTE mittels gesonderter und gehärteter administrativer Arbeitsstationen erfolgen. Das Prinzip der minimalen Rechtevergabe („Least Privilege“) SOLLTE bei der Administration eingehalten werden.

SYS.1.2.3.A5 Telemetrie und Datenschutzeinstellungen unter Windows Server 2019 (B)

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 MUSS daher durch geeignete Maßnahmen, etwa auf Netzebene, sichergestellt werden, dass diese Daten nicht an Microsoft übertragen werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.1.2.3 *Windows Server 2019*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.2.3.A6 Zentrale Verwaltung der Sicherheitsrichtlinien von Servern (S)

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 SOLLTEN dokumentiert, begründet und mit dem Sicherheitsmanagement abgestimmt werden.

SYS.1.2.3.A7 Konfiguration zum Schutz von Anwendungen unter Windows Server 2019 (S)

Maßnahmen zum Schutz vor Exploits SOLLTEN für alle Programme und Dienste aktiviert werden, die einen Exploit-Schutz unterstützen.

SYS.1.2.2.A8 Sichere Authentisierung und Autorisierung in Windows Server 2019 (S)

In Windows Server 2019 SOLLTEN alle Benutzer Mitglieder der Sicherheitsgruppe „Geschützte Nutzer“ sein. Konten für Dienste und Computer SOLLTEN NICHT Mitglied von „Geschützte Nutzer“ sein. Dienste-Konten in Windows Server 2019 SOLLTEN Mitglieder der Gruppe „Managed Service Account“ sein. Der PPL (Protected Process Light)-Schutz des Local Credential Store LSA SOLLTE aktiviert werden.

SYS.1.2.3.A9 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 Benutzer und IT-Systeme für den Remote-Desktopzugriff (RDP) SOLLTE durch die Zuweisung entsprechender Berechtigungen festgelegt werden. 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.

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 den Baustein SYS.1.2.3 *Windows Server 2019* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

SYS.1.2.2.A10 Angriffserkennung bei Windows Server 2019 (H)

Sicherheitsrelevante Ereignisse in Windows Server 2019 SOLLTEN an einem zentralen Punkt gesammelt und ausgewertet werden. Verschlüsselte Partitionen SOLLTEN nach einer definierten Anzahl von Entschlüsselungsversuchen gesperrt werden.

SYS.1.2.3.A11 Schutz der Anmeldeinformationen unter Windows Server 2019 (H)

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.

SYS.1.2.3.A12 Verwendung der Windows PowerShell (H)

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 SOLLTEN deaktiviert werden. Der Einsatz des PowerShell Constrained Language Mode SOLLTE geprüft werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Der Hersteller Microsoft stellt u. a. folgende weiterführende Informationen zu Windows Server 2019 bereit:

- Windows Server - Dokumentation
  https://docs.microsoft.com/de-de/windows-server/
- Neuerungen in Windows Server 2019:
  https://docs.microsoft.com/de-de/windows-server/get-started-19/whats-new-19
- Vergleich der Standard- und Datacenter-Editionen von Windows Server 2019:
  https://docs.microsoft.com/de-de/windows-server/get-started-19/editions-comparison-19
- Fixed Lifecycle-Richtlinie
  https://support.microsoft.com/de-de/help/14085/fixed-lifecycle-policy
- Vergleich der Features der Windows Server-Versionen:
  https://www.microsoft.com/de-de/cloud-platform/windows-server-comparison
- Entfernte oder zur Ersetzung vorgesehene Features in Windows Server 2019:
  https://docs.microsoft.com/de-de/windows-server/get-started-19/removed-features-19
- Security and Assurance (Übersicht):
  https://docs.microsoft.com/de-de/windows-server/security/security-and-assurance
- Microsoft Security Compliance Toolkit 1.0:
  https://docs.microsoft.com/de-de/windows/security/threat-protection/security-compliance-toolkit-10
- Anpassen des Exploit-Schutzes
  https://docs.microsoft.com/de-de/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-protection
- Schützen von Geräten vor Sicherheitsrisiken
  https://docs.microsoft.com/de-de/windows/security/threat-protection/microsoft-defender-atp/exploit-protection
- Schutz und Verwaltung von Anmeldeinformationen
  https://docs.microsoft.com/de-de/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/de-de/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://www.microsoft.com/en-us/download/confirmation.aspx?id=50034
- Konfigurieren von zusätzlichem LSA-Schutz:
https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
- Windows Server Guidance to protect against Speculative Execution:
https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-speculative-execution

Das Infomation 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:

- https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden.

Die folgenden elementaren Gefährdungen sind für den Baustein SYS.1.2.3 *Windows Server 2019* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler
G 0.29 Verstoß gegen Gesetze oder Regelungen
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
G 0.32 Missbrauch von Berechtigungen
G 0.33 Personalausfall
G 0.36 Identitätsdiebstahl
G 0.37 Abstreiten von Handlungen
G 0.38 Missbrauch personenbezogener Daten
G 0.39 Schadprogramme
G 0.40 Verhinderung von Diensten (Denial of Service)
G 0.41 Sabotage
G 0.42 Social Engineering
G 0.43 Einspielen von Nachrichten
G 0.45 Datenverlust
G 0.46 Integritätsverlust schützenswerter Informationen

Zuordnung elementare Gefährdungen zu Anforderungen	CIA	G 0.14	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.33	G 0.36	G 0.37	G 0.38	G 0.39	G 0.40	G 0.41	G 0.42	G 0.43	G 0.45
SYS.1.2.3.A1				X								X		X													
SYS.1.2.3.A2		X	X		X	X	X	X	X	X	X		X		X	X	X		X	X	X	X	X		X	X	X
SYS.1.2.3.A3		X	X		X	X	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X		X	X	X
SYS.1.2.3.A4		X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SYS.1.2.3.A5			X	X	X									X	X				X								
SYS.1.2.3.A6		X		X					X						X	X	X										
SYS.1.2.3.A7		X		X			X	X				X		X	X							X					
SYS.1.2.3.A8		X	X		X		X	X	X			X			X	X	X		X	X	X	X	X	X	X	X	
SYS.1.2.3.A9				X	X				X						X	X											
SYS.1.2.3.A10	CIA	X			X		X	X	X				X		X		X					X	X	X	X	X	X
SYS.1.2.3.A11	CI	X		X	X			X					X														
SYS.1.2.3.A12	CIA			X				X																			