SYS.1.2.4 Windows Server 2022

1. Beschreibung

1.1. Einleitung

Windows Server 2022 ist eine Server-Betriebssystemversion von Microsoft im Long-Term Servicing Channel (LTSC) und stellt die Weiterentwicklung der Windows-Server-Linie dar. Gegenüber seinen Vorgängern führt es eine Reihe neuer und verbesserter Sicherheitsfunktionen ein, die auf den Schutz vor modernen Bedrohungen abzielen. Dazu gehören insbesondere die "Secured-core"-Initiative zum Schutz der Systemintegrität auf Hardware- und Firmware-Ebene, die standardmäßige Aktivierung von TLS 1.3 zur Härtung der Transportverschlüsselung und die Unterstützung von DNS-over-HTTPS (DoH) zum Schutz der Namensauflösung.
Während der allgemeine Windows-Server-Baustein grundlegende Prinzipien abdeckt, erfordern diese spezifischen Neuerungen eine gesonderte Betrachtung, um ihr Sicherheitspotenzial voll auszuschöpfen. Dieser Baustein bietet daher gezielte Anforderungen für die sichere Konfiguration und den Betrieb von Windows Server 2022 und stellt eine versionenspezifische Vertiefung dar.

1.2. Zielsetzung

Dieser Baustein zeigt einen systematischen Weg für die sichere Installation, Konfiguration und den Betrieb von Windows Server 2022 auf. Ziel ist es, die spezifischen Sicherheitsfunktionen des Betriebssystems korrekt zu implementieren, die Angriffsfläche zu minimieren und eine robuste, gehärtete Server-Plattform bereitzustellen, die den aktuellen Bedrohungen standhält.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.2.4 ist auf alle Systeme anzuwenden, auf denen Windows Server 2022 in den Editionen Standard oder Datacenter installiert ist.
Dieser Baustein ersetzt nicht die allgemeinen Anforderungen aus SYS.1.1 Allgemeiner Server, sondern ergänzt und konkretisiert diese für Windows Server 2022. Er steht in enger Beziehung zu weiteren Bausteinen wie SYS.2.1 Active Directory Domain Services oder SYS.3.1 Public-Key-Infrastruktur. Die spezifischen Sicherheitsfunktionen von Windows Server 2022 werden hier detailliert behandelt.

2. Gefährdungslage

Für den Baustein SYS.1.2.4 sind folgende spezifische Bedrohungen und Schwachstellen von besonderer Bedeutung:

Ausnutzung von Schwachstellen in neuen oder komplexen Diensten

Neue und erweiterte Funktionen, wie die tiefere Integration in Azure-Hybrid-Dienste (z. B. Azure Arc) oder das Windows Admin Center, schaffen neue Angriffsflächen. Werden diese Dienste nicht nach sicheren Vorgehensweisen konfiguriert, können sie als Einfallstor für Angreifer dienen.

Kompromittierung durch unsichere Hybrid-Cloud-Anbindungen

Die nahtlose Anbindung an Cloud-Dienste kann zu einer Vermischung von Sicherheitsdomänen führen. Eine kompromittierte Cloud-Identität kann missbraucht werden, um auf On-Premises-Ressourcen zuzugreifen, oder umgekehrt, ein kompromittierter On-Premises-Server kann als Sprungbrett in die Cloud dienen.

Umgehung von Sicherheitsmechanismen durch veraltete Konfigurationen

Werden Konfigurationsskripte oder Gruppenrichtlinien von älteren Server-Versionen unverändert übernommen, werden die neuen Sicherheitsfunktionen von Windows Server 2022 (z. B. Secured-core-Optionen) möglicherweise nicht aktiviert. Dadurch bleibt das System auf einem veralteten Sicherheitsniveau und ist anfällig für Angriffe, die durch die neuen Mechanismen verhindert werden könnten.

Angriffe auf die Firmware-Ebene

Obwohl die Secured-core-Architektur Schutz vor Boot- und Rootkits bietet, ist dieser Schutz nur wirksam, wenn er auf kompatibler Hardware korrekt aktiviert und konfiguriert ist. Andernfalls bleibt das System anfällig für Angriffe, die unterhalb der Betriebssystemebene ansetzen.

Abhören von unverschlüsselter oder schwach verschlüsselter Kommunikation

Windows Server 2022 aktiviert TLS 1.3 standardmäßig. Ältere Anwendungen oder fehlerhafte Konfigurationen können jedoch ein Downgrade auf unsichere Protokolle erzwingen. Auch die DNS-Kommunikation bleibt ohne die aktive Konfiguration von DNS-over-HTTPS (DoH) anfällig für Ausspähung und Manipulation.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.2.4 aufgeführt.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.2.4.A1 Gesicherte Installation und initiale Konfiguration (B)

Die Installation von Windows Server 2022 MUSS von einem vertrauenswürdigen Installationsmedium erfolgen. Nach der Installation MUSS das standardmäßige Administratorkonto umbenannt und mit einem sicheren Passwort versehen werden. Der Windows Defender Antivirus MUSS aktiviert sein.

SYS.1.2.4.A2 Regelmäßiges und zeitnahes Patch-Management (B)

Es MUSS ein Prozess etabliert sein, der sicherstellt, dass die von Microsoft bereitgestellten Sicherheitsupdates regelmäßig und zeitnah auf allen Windows Server 2022 Systemen installiert werden.

SYS.1.2.4.A3 Grundlegende Härtung des Betriebssystems (B)

Nicht benötigte Serverrollen und Features MÜSSEN deinstalliert werden, um die Angriffsfläche zu reduzieren. Die Windows Defender Firewall MUSS aktiviert sein und mit einer restriktiven Regelbasis betrieben werden.

SYS.1.2.4.A4 Absicherung der Benutzerkonten und Privilegien (B)

Die Benutzerkontensteuerung (User Account Control, UAC) MUSS aktiviert sein. Administrative Berechtigungen DÜRFEN nur an einen eng begrenzten Kreis von Administratoren vergeben werden.

SYS.1.2.4.A5 Aktivierung der grundlegenden Protokollierung (B)

Die Protokollierung sicherheitsrelevanter Ereignisse (wie An- und Abmeldungen, Änderungen an Konten und Gruppenrichtlinien) MUSS aktiviert sein. Es MUSS sichergestellt werden, dass die Ereignisprotokolle vor Manipulation geschützt sind.

3.2. Standard-Anforderungen

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

SYS.1.2.4.A6 Nutzung der Secured-core Server-Funktionen (S)

Auf unterstützter Hardware SOLLTEN die Secured-core-Funktionen aktiviert werden. Dies umfasst die Virtualisierungsbasierte Sicherheit (VBS), die Hypervisor-geschützte Codeintegrität (HVCI) und den Schutz vor DMA-Angriffen beim Startvorgang.

SYS.1.2.4.A7 Konsequente Nutzung von Transportverschlüsselung (S)

Die systemweite Verwendung von TLS 1.3 SOLLTE erzwungen werden. Ältere und als unsicher eingestufte Protokolle wie SSL und TLS 1.0/1.1 SOLLTEN deaktiviert werden. Für den Zugriff auf Dateifreigaben SOLLTE die SMB-Verschlüsselung aktiviert werden.

SYS.1.2.4.A8 Härtung der Remote-Verwaltung (S)

Der Fernzugriff auf den Server SOLLTE über sichere, authentifizierte und verschlüsselte Protokolle erfolgen, wie PowerShell Remoting über HTTPS oder SSH. Wird das Windows Admin Center genutzt, SOLLTE dieses ebenfalls gehärtet und der Zugriff darauf abgesichert werden. RDP-Zugriffe SOLLTEN auf ein Minimum beschränkt und über ein RD Gateway abgesichert werden.

SYS.1.2.4.A9 Implementierung von Windows Defender Credential Guard (S)

Auf Systemen, die die Hardware-Voraussetzungen erfüllen, SOLLTE Credential Guard aktiviert werden, um zwischengespeicherte Anmeldeinformationen vor Angriffen wie "Pass-the-Hash" zu schützen.

SYS.1.2.4.A10 Absicherung der DNS-Kommunikation (S)

Der DNS-Client SOLLTE so konfiguriert werden, dass er für die Auflösung externer Namen DNS-over-HTTPS (DoH) verwendet, um die Vertraulichkeit und Integrität von DNS-Anfragen zu schützen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Die folgenden Anforderungen sind exemplarische Vorschläge für ein Schutzniveau, das über den Stand der Technik hinausgeht. Sie SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden.

SYS.1.2.4.A11 Implementierung von Windows Defender Application Control (WDAC) (H)

Es SOLLTE eine Positivliste von zulässigen Anwendungen mittels WDAC durchgesetzt werden. Dadurch wird sichergestellt, dass nur signierter und explizit vertrauenswürdiger Code auf dem Server ausgeführt werden kann.

SYS.1.2.4.A12 Sichere Anbindung an Hybrid-Dienste (H)

Wird der Server mittels Azure Arc verwaltet, SOLLTE der Onboarding-Prozess abgesichert und der Zugriff aus der Cloud streng kontrolliert werden. Sicherheitsrichtlinien SOLLTEN zentral über Azure Policy auf dem Server durchgesetzt werden.

SYS.1.2.4.A13 Umfassende Protokollierung und Detektion mit erweiterten Werkzeugen (H)

Es SOLLTE eine erweiterte Protokollierung aktiviert werden, die PowerShell Script Block Logging und die Protokollierung von Prozesserstellungen umfasst. Diese Daten SOLLTEN an ein zentrales SIEM weitergeleitet und durch eine EDR-Lösung (Endpoint Detection and Response) wie Microsoft Defender for Endpoint überwacht werden.

SYS.1.2.4.A14 Einsatz von Just-In-Time (JIT) und Just-Enough-Administration (JEA) (H)

Administrative Berechtigungen SOLLTEN nur bei Bedarf und zeitlich begrenzt über ein Privileged Access Management (PAM)-System vergeben werden (JIT). Für Routineaufgaben SOLLTEN PowerShell-Endpunkte mit Just-Enough-Administration (JEA) konfiguriert werden, die Administratoren nur die Ausführung definierter Befehle erlauben.

SYS.1.2.4.A15 Härtung des SMB-Protokolls mit SMB over QUIC (H)

Für den sicheren Zugriff auf Dateifreigaben von außerhalb des vertrauenswürdigen Netzwerks SOLLTE der Einsatz von SMB over QUIC in Betracht gezogen werden. Dieses nutzt TLS 1.3 über das QUIC-Protokoll und erfordert keinen traditionellen VPN-Tunnel.