Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.2.2 Windows Server 2012

1. Beschreibung

1.1. Einleitung

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.

Dieser Baustein beschäftigt sich mit der Absicherung von Windows Server 2012 und Windows Server 2012 R2 gleichermaßen. Wenn beide Versionen gemeint sind, wird die einheitliche Schreibweise „Windows Server 2012“ verwendet. Unterschiede in der Version R2 werden gesondert erwähnt. Das Ablaufdatum für den Mainstream Support bzw. den Extended Support („End-of-Life“, EOL) ist für beide Betriebssysteme der 09.10.2018 bzw. der 10.10.2023.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist der Schutz von Informationen und Prozessen, die durch Server-Systeme auf Basis von Windows Server 2012 im Regelbetrieb verarbeitet bzw. gesteuert werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.2.2 *Windows Server 2012* ist für alle Server-Systeme anzuwenden, auf denen das Betriebssystem Microsoft Windows Server 2012 eingesetzt wird. Für neuere Versionen von Windows Server gibt es den Baustein SYS.1.2.3 *Windows Server*.

Dieser Baustein konkretisiert und ergänzt die Aspekte, die im Bausteinen SYS.1.1 *Allgemeiner Server* behandelt werden, um Besonderheiten von Windows Server 2012. Dementsprechend sind die beiden Bausteine immer gemeinsam anzuwenden.

Im Rahmen dieses Bausteins wird von einer Standardeinbindung 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*.

Sicherheitsanforderungen möglicher Serverrollen und -funktionen wie Fileserver (APP.3.3 *Fileserver*), Webserver (APP.3.2 *Webserver*) oder Microsoft Exchange und Outlook (APP.5.2 *Microsoft Exchange und Outlook*) 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

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.1.2.2 *Windows Server 2012* von besonderer Bedeutung.

2.1. Unzureichende Planung von Windows Server 2012

Windows Server 2012 ist ein komplexes Betriebssystem mit einer großen Anzahl an Funktionen und Konfigurationsoptionen. Bei der Einbindung in die Domäne und bei der Vernetzung mit anderen IT-Systemen und Diensten gibt es sehr viele Spielräume. Auch wenn moderne Windows-Versionen in vielen Bereichen gute Standardeinstellungen mitbringen, ist die Grundkonfiguration nicht in jedem Fall die sicherste. Dies kann bei unzureichender Planung zu einer Vielzahl von Angriffsvektoren führen, die von unberechtigten Dritten leicht ausgenutzt werden können. Werden außerdem nicht schon vor der Installation zentrale Entscheidungen getroffen, wird Windows Server 2012 in einem unsicheren und undefinierten Zustand ausgeführt, der sich nachträglich kaum mehr beheben lässt.

2.2. Unbedachte Cloud-Nutzung

Windows Server 2012 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 grundsätzlich Vorteile, beispielsweise hinsichtlich der Verfügbarkeit, bieten können, bestehen bei unbedachtem Einsatz Risiken für die Vertraulichkeit sowie eine zusätzliche Abhängigkeit. So können Daten über Cloud-Dienste in die Hände unberechtigter Personen gelangen. Dabei kann es sich sowohl um kriminell als auch um staatlich Agierende handeln. Wird ein Cloud-Dienst eingestellt, kann dies erhebliche Auswirkungen auf die eigenen Geschäftsprozesse haben.

2.3. Fehlerhafte Administration von Windows-Servern

Windows Server 2012 und Windows Server 2012 R2 haben im Vergleich zu den Vorgängerversionen viele neue sicherheitsrelevante Funktionen hinzubekommen. Bei anderen (bekannten) Features haben sich Teilfunktionen, Parameter oder Standardkonfigurationen verändert. Ist der IT-Betrieb nicht ausreichend in den Besonderheiten der Systeme geschult, drohen Konfigurationsfehler und menschliche Fehlhandlungen, die neben der Funktionalität auch die Sicherheit des 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 2012 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 2012 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 Bequemlichkeit. Informationen und Prozesse können so durch Unbefugte 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 Administrationsrechten

Die reguläre Arbeit unter Standardberechtigungen ist inzwischen gängige Praxis. Da Administrierende jedoch an bestimmten Stellen trotzdem ihre Rechte erhöhen müssen, können Angreifende dort potenziell privilegierte Rechte erlangen. Auch ein Missbrauch von Rechten durch legitime Administrierende ist ein relevantes Schadensszenario. Da die Rollen oft sehr mächtig sind, sind hier die Auswirkungen in der Regel beträchtlich, insbesondere bei sogenannten Domänenadministratoren. Auch ohne Passwörter zu erraten oder zu brechen, können z. B. durch sogenannte Pass-the-Hash-Verfahren geeignete Credentials ausgelesen und missbraucht werden, um sich lateral im Netz weiterzubewegen.

2.7. Kompromittierung von Fernzugängen

Da Windows Server 2012 über eine Vielzahl von Möglichkeiten verfügt, aus der Ferne verwaltet zu werden, können diese grundsätzlich auch missbraucht werden. Fernzugänge wie z. B. RDP-Sitzungen 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.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.2.2 *Windows Server 2012* 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.1.2.2.A1 Planung von Windows Server 2012 (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 2012 getroffen werden. Der Einsatzzweck des Servers sowie die Einbindung ins Active Directory MÜSSEN dabei spezifiziert werden. Die Nutzung von ins Betriebssystem integrierten Cloud-Diensten MUSS grundsätzlich abgewogen und geplant werden. Wenn nicht benötigt, MUSS die Einrichtung von Microsoft-Konten auf dem Server blockiert werden.

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

Es DÜRFEN KEINE anderen als die benötigten Serverrollen und Features bzw. Funktionen installiert werden. Wenn es vom Funktionsumfang her ausreichend ist, 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 Administration von Windows Server 2012 (B)

Alle Administrierenden, die für das Server-System zuständig sind, MÜSSEN in den sicherheitsrelevanten Aspekten der Administration von Windows Server 2012 geschult sein. Webbrowser auf dem Server DÜRFEN NICHT zum Surfen im Web verwendet 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.1.2.2.A4 Sichere Konfiguration von Windows Server 2012 (S)

Mehrere wesentliche Funktionen bzw. Rollen SOLLTEN NICHT durch einen einzigen Server erfüllt, sondern geeignet aufgeteilt werden. Vor Inbetriebnahme SOLLTE das System grundlegend gehärtet werden. Dafür SOLLTEN funktionsspezifische und institutionsweite Sicherheitsvorlagen erstellt und gepflegt werden, die auf die Server ausgerollt werden. Der Internet Explorer SOLLTE auf dem Server nur in der Enhanced Security Configuration und im Enhanced Protected Mode genutzt werden.

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

Außer bei IT-Systemen mit Windows Server 2012, die als Stand-alone-Gerät ohne Netzanschluss und Wechselmedien betrieben werden, SOLLTE vor dem ersten Verbinden mit dem Netz oder Wechselmedien ein Virenschutzprogramm installiert werden. Im Konzept zum Schutz vor Schadsoftware SOLLTE vorgesehen werden, dass regelmäßig alle Festplatten vollständig gescannt werden. Es SOLLTEN Alarme für Virenfunde konfiguriert sein.

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

In Windows Server 2012 R2 SOLLTEN alle Konten von Benutzenden Mitglied der Sicherheitsgruppe „Geschützte Nutzer“ sein. Konten für Dienste und Computer SOLLTEN NICHT Mitglied von „Geschützte Nutzer“ sein. Dienste-Konten in Windows Server 2012 SOLLTEN Mitglied der Gruppe „Managed Service Account“ sein. Der PPL-Schutz des Local Credential Store LSA SOLLTE aktiviert werden. Der Einsatz dynamischer Zugriffsregeln auf Ressourcen SOLLTE bevorzugt werden.

SYS.1.2.2.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.2.2.A8 Schutz der Systemintegrität (S)

AppLocker SOLLTE aktiviert und möglichst strikt konfiguriert sein.

SYS.1.2.2.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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.1.2.2.A10 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.2.2.A11 Angriffserkennung bei Windows Server 2012 (H)

Sicherheitsrelevante Ereignisse in Windows Server 2012 SOLLTEN an einem zentralen Punkt gesammelt und ausgewertet werden. Verschlüsselte Partitionen SOLLTEN nach einer definierten Anzahl von Entschlüsselungsversuchen gesperrt werden.

SYS.1.2.2.A12 Redundanz und Hochverfügbarkeit bei Windows Server 2012 (H)

Es SOLLTE geprüft werden, welche Verfügbarkeitsanforderungen durch Betriebssystemfunktionen wie Distributed File System (DFS), ReFS, Failover Cluster und Network Load Balancing bzw. NIC-Teaming (LBFO) erfüllt oder unterstützt werden können. Für Außenstellen SOLLTE BranchCache aktiviert werden.

SYS.1.2.2.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.2.2.A14 Herunterfahren verschlüsselter Server und virtueller Maschinen (H)

Um verschlüsselte Daten zu schützen, SOLLTEN nicht benötigte Server (inklusive virtuelle Maschinen) immer heruntergefahren werden. Dies SOLLTE möglichst automatisiert erfolgen. Die Entschlüsselung der Daten SOLLTE einen interaktiven Schritt erfordern oder zumindest im Sicherheitsprotokoll festgehalten werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Der Hersteller Microsoft stellt unter anderem folgende weiterführende Informationen zu Windows Server 2012 bereit:

- Secure Windows (für Windows 8/8.1, gilt größtenteils auch für Windows Server 2012 / 2012 R2): https://technet.microsoft.com/en-us/library/hh832031.aspx
- Secure Windows Server 2012 R2 and Windows Server 2012: https://technet.microsoft.com/en-us/library/hh831360.aspx
- Security and Protection: https://technet.microsoft.com/en-us/library/hh831778.aspx
- Liste von Sicherheitsereignissen unter Windows 8.1 und Windows Server 2012: 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 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.