Bundesamt
für Sicherheit in der
Informationstechnik

# Umsetzungshinweise zum Baustein SYS.1.2.2 Windows Server 2012



## 1. Einleitung

Mit Windows Server 2012 hat Microsoft im September 2012 ein Serverbetriebssystem auf den Markt gebracht, das in Bezug auf die Sicherheit diverse Verbesserungen gegenüber bisherigen Windows-Versionen (insbesondere auch Windows Server 2008 R2) mitbringt. Technisch wird dabei nicht auf dem Vorgänger aufgebaut, sondern auf der Codebasis des Client-Betriebssystems Windows 8. Mit dem Release Windows Server 2012 R2 von Oktober 2013 sind weitere Verbesserungen und Erweiterungen verfügbar, die Windows 2012 R2 zum Server-Pendant zu Windows 8.1 auf der Clientseite machen.

Dieser Baustein beschäftigt sich mit der Absicherung von Windows Server 2012 und Windows Server 2012 R2 gleichermaßen, auf relevante Unterschiede und Besonderheiten wird jeweils geeignet hingewiesen. Dabei wird die Schreibweise „Windows Server 2012 (R2)“ verwendet, wenn beide Versionen gemeint sind. Das Ablaufdatum für den Mainstream Support bzw. den Extended Support („End-of-Life“, EOL) ist in beiden Fällen der 09.01.2018 bzw. der 10.01.2023.

## 2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins SYS.1.2.2 *Windows Server 2012* sowie für weitere Bausteinen aufgeführt, die hiermit im Zusammenhang stehen:

SYS.1.1 *Allgemeiner Server* und ORP.4 *Identitäts- und Berechtigungsmanagement*.

Diese zusätzlichen Maßnahmen sollten bei der Umsetzung der genannten Bausteine berücksichtigt werden. Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

# 2.1. Maßnahmen zum Baustein SYS.1.2.2 Windows Server 2012

## SYS.1.2.2.M1 Planung von Windows Server 2012 (B)

Da Windows Server 2012 (R2) ein komplexes Betriebssystem mit einer Vielzahl von Funktionen und Konfigurationsoptionen darstellt, muss der Einsatz sorgfältig und systematisch geplant werden. Eine Dokumentation der Entscheidungen samt kurzer Begründung sollte dabei angelegt werden, etwa in Form eines Betriebskonzepts oder eines Serverhandbuchs.

### Editionen

Windows Server 2012 ist in vier Editionen verfügbar, die für unterschiedliche Einsatzgebiete vorgesehen und optimiert sind:

- Foundation
- Grundlegende Server-Funktionen
- keine Virtualisierung
- Essentials
- einfache Benutzeroberfläche
- voreingestellte Konnektivität zu Cloud-Diensten
- keine Virtualisierung
- Standard
- Voller Funktionsumfang
- max. zwei virtuelle Instanzen
- Datacenter
- wie Standard
- mit unbegrenzten virtuellen Instanzen

Weitere Beschränkungen existieren bei Foundation bzw. Essentials bezüglich Speicher (max. 32/64 GB RAM) und Lizenzierung (max. 15/25 Benutzerkonten) sowie in den installierbaren Rollen und Funktionalitäten. Über weitere Details der Unterschiede bzgl. Beschränkungen, Rollen und Funktionen informiert Microsoft auf seiner Website. Der Server-Core-Modus etwa ist erst ab Edition Standard verfügbar, die Nutzung von WSUS erst ab Essentials. Zumindest Foundation ist daher nur in sehr begrenzten Szenarien für den professionellen Einsatz im Unternehmen oder in der Behörde zu empfehlen und wird in diesem Baustein nicht näher betrachtet.

Die Editionen Standard und Datacenter sind aus Sicherheitssicht gleichwertig und unterscheiden sich im Wesentlichen in Hinsicht auf das Lizenzmodell. Es bleibt also die Frage nach der Entscheidung zwischen Essentials und Standard bzw. Datacenter.

### Eigenschaften der Essentials-Edition

Foundation und Essentials in Windows 2012 sind nicht dafür gedacht, innerhalb einer vollwertigen Domäne betrieben zu werden. Zwar ist dies für Essentials mit Windows Server 2012 R2 mittlerweile technisch möglich, jedoch richtet sich diese mit ihren Funktionen hauptsächlich an kleinere Institutionen, die nur einen einzigen Server zum Betrieb sämtlicher Funktionen einsetzen. Dies steht im Widerspruch zur etablierten Praxis in größeren IT-Umgebungen, möglichst wenige Dienste pro Server zu betreiben, um

Abhängigkeiten aufzulösen und Risiken zu streuen, ein Trend, der durch zunehmende Virtualisierung weitere Verbreitung findet.

Die Essentials-Edition bietet ohne weitere Konfiguration eine Reihe von Funktionen, welche die Einrichtung erleichtern können:

- Hinzufügen zur Domäne
  Mit Essentials ist es einfach möglich, Rechner zur Domäne hinzuzufügen, die sich an einem entfernten Standort befinden. Es genügt, dass ein neuer Mitarbeiter auf den Pfad "/connect" der Essentials-Fernzugriffswebsite zugreifen kann.
- Vorkonfiguriertes VPN
  Es ist ein vorkonfigurierter VPN-Client verfügbar. Der Benutzer kann zudem die Autoeinwahl aktivieren, sodass er immer mit dem Firmen- bzw. Behördennetz verbunden ist.
- Server-SpeicherFür Speicherorte wie etwa die Heimatverzeichnisse der Benutzer können einfach Shared Folder auf einem weiteren Server im selben Netz angelegt werden. Dabei kann eine automatische Alarmierung erfolgen, wenn die Verzeichnisse eine bestimmte Größe überschreiten.
- Health Report
  Ein grundlegender "Gesundheitscheck" der Windows Server 2012 R2 Essentials-Umgebung ist bereits integriert und muss nicht erst als Add-in installiert werden. Es lassen sich verschiedene Werte konfigurieren, die über unterschiedliche Medien angezeigt werden, etwa auch auf dem Smartphone.
- BranchCache
  Bereits in Essentials kann der Mechanismus BranchCache aktiviert werden, der die Verfügbarkeit von Daten in Außenstellen durch Caching (Zwischenspeicherung) erhöht. Er verringert darüber hinaus gleichzeitig die Bandbreitennutzung über das WAN.
- Remote Web Access
  Viele Funktionen von Windows Server 2012 Essentials lassen sich aus der Ferne über eine Weboberfläche erreichen und bedienen (Remote Web Access), die in R2 zudem modernisiert und für die Nutzung mit Tablets und ähnlichen Geräten optimiert wurde.

### Microsoft Azure Online Backup

In Windows Server 2012 ist Microsofts Cloud-Speicherlösung Azure Online Backup bereits in Essentials integriert und kann leicht aktiviert werden. Dafür muss lediglich im Essentials Dashboard das entsprechende Add-in installiert werden und ein (je nach Speichervolumen kostenpflichtiger) Account angelegt werden. In R2 ist nicht mal mehr ein Add-in notwendig, hier kann direkt per Klick die Registrierung bei Azure erfolgen.

Während dies eine sehr einfache Möglichkeit darstellt, regelmäßige Backups der auf dem Server gespeicherten Daten zu erzeugen, sollte diese Funktion keinesfalls leichtfertig aktiviert werden, sondern allenfalls nach einer umfassenden Beschäftigung mit den Themen der Bausteine OPS.2.2 Cloud-Nutzung und OPS.1.16 Datensicherung und einer erfolgten Abwägung zwischen Vertraulichkeit, Verfügbarkeit und verschiedenen Anbietern.

### Blockieren von Microsoft-Konten

Der folgende Abschnitt ist nicht anzuwenden, wenn im Rahmen der Beschäftigung mit dem Baustein OPS.2.2 Cloud-Nutzung eine begründete und dokumentierte Entscheidung für die Nutzung von Microsoft Azure in Zusammenhang mit dem Windows Server 2012 (R2)-Serversystem getroffen wurde.

Andernfalls darf während der Einrichtung des Systems kein Microsoft-Konto angelegt werden. Die Erstellung von Microsoft-Konten auf dem Server muss zudem blockiert werden. Am verlässlichsten geschieht dies zentral über das Active Directory und die folgende Sicherheitsrichtlinie:

"Windows Settings/Security Settings/Local Policies/Security Options/Accounts: Block Microsoft Accounts"

## SYS.1.2.2.M2 Sichere Installation von Windows Server 2012 (B)

Grundlegende Funktionen von Windows Server 2012 (R2) werden durch Serverrollen, Rollendienste und Features gesteuert.

### Serverrollen
Eine Serverrolle ist eine Gruppe von Programmen, mittels derer eine bestimmte Funktion für mehrere Benutzer oder für andere IT-Systeme in einem Netz ausgeführt werden kann. Mit ihr wird häufig die Hauptfunktion eines Servers beschrieben. Ein Server könnte jedoch auch mehrere Rollen ausführen, wenn diese nur selten verwendet werden. Sind Rollen korrekt installiert und konfiguriert, werden sie automatisch ausgeführt.

### Rollendienste
Rollendienste sind Programme, die die Funktionalität einer Rolle bereitstellen. Eine Rolle kann als Satz zusammenhängender, sich ergänzender Rollendienste betrachtet werden, wobei in der Regel die Installation einer Rolle die Einrichtung mindestens eines zugehörigen Rollendienstes bedingt.

Je Rolle kann festgelegt werden, welche Rollendienste für andere Benutzer und IT-Systeme mit der Rolle bereitgestellt werden. Einige Rollen (z. B. DNS-Server) haben nur eine Funktion, daher stehen für sie keine Rollendienste zur Verfügung. Andere Rollen (z. B. Remotedesktopdienste) verfügen über mehrere Rollendienste, die je nach Anforderungen installiert werden können.

### Features
Features sind Programme, die die Funktionalität des Servers oder aber einer oder mehrerer Rollen unterstützen oder verbessern. Z. B. wird mit dem Feature Failover-Clusterunterstützung die Funktionalität weiterer Rollen (u. a. Dateidienste und DHCP-Server) verbessert, da Servercluster für eine höhere Redundanz und bessere Leistung zusammengeführt werden können. Das Feature Telnet-Client hingegen ermöglicht die Fernkommunikation über das Telnet-Protokoll.

Rollen, Rollendienste und Features müssen immer so sparsam wie möglich installiert werden, um die Komplexität und Angriffsoberfläche klein zu halten. Die Regel "ein Dienst pro Server" gilt auch hier sinngemäß, es sollte in der Regel nur eine für die Institution wesentliche Serverrolle pro Server installiert sein. Die Auswahl der zu installierenden Rollen, Rollendienste und Features sollte begründet und dokumentiert werden.

### Server Core
Server Core ist eine minimale Installationsoption für Windows Server (inkl. 2012 und 2012 R2), die eine Serverumgebung mit beschränkter Funktionalität und geringerem Wartungsbedarf bereitstellt.

Seit Windows Server 2012 ist ein Wechsel zwischen Full Server und Server Core ohne Neuinstallation möglich.

Hauptunterschiede sind das Fehlen der vollständigen Windows-Shell und eine extrem begrenzte grafische Oberfläche (GUI), die sich auf ein Kommandoprompt mit PowerShell-Unterstützung beschränkt.

Verwalten lässt sich Server Core folgendermaßen:

- per PowerShell (lokal und remote)
- über eine Terminal-Server-Verbindung von einer Kommandozeile
- aus der Ferne über die Microsoft Management Console (MMC)
- aus der Ferne mit anderen Kommandozeilentools, die Fernverwaltung unterstützen

Da Server Core bezüglich der Angriffsfläche das Minimum und damit Optimum darstellt, sollte, wo immer möglich, die Server Core-Variante genutzt werden. Abweichungen sollten begründet sein. Dies fördert zudem die Zentralisierung der Verwaltung.

## SYS.1.2.2.M3 Sichere Administration von Windows Server 2012 (B)

### Sichere Passworte für lokale Administrationskonten
Es ist sicherzustellen, dass das Passwort für jedes lokale Administratorkonto nicht nur sicher ist, sondern zudem einzigartig. So wird es einem Angreifer erschwert, sich von einem kompromittierten IT-System zum nächsten lateral weiterzubewegen.

Mit dem bei Microsoft kostenlos verfügbaren Tool LAPS (Local Administrator Password Solution) ist es möglich, sichere lokale Administratorkonten automatisch per AD zu verwalten. Dessen Einsatz ist stark zu empfehlen, wenn nicht bereits eine Drittlösung hierfür bereitsteht.

### Schulung von Administratoren

Um Windows Server 2012 (R2) sicher einrichten und betreiben zu können, müssen die zuständigen Administratoren über eine Reihe von Fähigkeiten und Kenntnissen verfügen, die teilweise sehr spezifisch für dieses Betriebssystem sind. Zum Allgemeinwissen des Administrators gehören etwa Grundregeln des Arbeitens auf Serversystemen wie

- nicht von Servern aus im WWW zu surfen,
- insbesondere keine möglicherweise unsicheren Seiten anzusteuern,
- Clientsysteme für den Download von Dateien wie etwa Treibern zu verwenden und
- für sämtliche nichtadministrativen Tätigkeiten einen Standardaccount zu verwenden.

Im Folgenden werden Spezifika von Windows Server 2012 (R2) vorgestellt, mit denen sich die Administratoren auskennen sollten. Notwendige Schulungen sollten vor Installation der Serversysteme durchgeführt werden.

### Administrationsthemen

Die folgende Tabelle enthält eine Liste von Administrationsthemen mit Security-Relevanz. Administratoren von Windows Server 2012 (R2) sollten sich mit den genannten Themen und ihren Besonderheiten sowie jeweils geeigneten Tools bei Windows Server 2012 (R2) auskennen.

| **Thema** | **Aufgaben des Administrators** |
|---|---|
| Zugriff | Verwalten des Zugriffs auf Netzressourcen |
| Auditing | Verwalten des Zugriffs auf Netzressourcen |
| Zertifikatsdienste | Verwalten einer Zertifizierungsstelle (CA) und andere Active Directory-Zertifikatsdienste-Aufgaben |
| Computer | Analysieren und Verwalten von Computerprozessen und Leistung |
| Anmeldeinformationen | Verwalten von Benutzerkonten, Gruppen und Anmeldeinformationen |
| Kryptografie | Verwalten von Zertifikaten und Verschlüsselung |
| Dateien | Übernehmen oder dauerhaftes Löschen von Dateien |
| Sicherheitsrichtlinien | Analysieren und Verwalten von Sicherheitsrichtlinien |
| Sicherheitsprinzipale | Ändern oder Erstellen neuer Sicherheitsprinzipale |
| Systemsicherheit | Diagnostizieren, Planen und Berichtigen der globalen Systemsicherheit |

Darüber hinaus bietet Microsoft als Teil der Windows PowerShell Core Modules Sammlungen von PowerShell-Commandlets für Security-Aufgaben an. Administratoren sollten diese kennen, um sie für eine einfache und schlanke Sicherheitsverwaltung nutzen zu können:

- Windows PowerShell Security Cmdlets
- PowerShell Cmdlets for Active Directory
- PowerShell Cmdlets for Active Directory Rights Management Services
- PowerShell Cmdlets for AppLocker
- PowerShell Cmdlets for Group Policy

- PowerShell Cmdlets for Server Manager
- PowerShell Cmdlets for the Best Practice Analyzer

### Benutzerkontensteuerung (UAC)

Die Benutzerkontensteuerung (User Account Control, UAC) wurde in Windows Vista eingeführt. Sie sorgt dafür, dass bei administrativen Aufgaben eine Rechteerhöhung erforderlich ist. Bis dahin hatten die meisten Anwender als Administratoren gearbeitet, mit entsprechender Anfälligkeit für Schadsoftware.

Wenn sich bei aktivierter UAC ein Administrator anmeldet, arbeitet er mit eingeschränkten Rechten. Erst nach Bestätigung in einem speziellen Dialogfeld erhält eine Anwendung administrative Berechtigungen. Im Hintergrund werden dafür Rechte erhöht, indem die Identität gewechselt wird. Die UAC ist damit die Grundlage für das Sandboxing von Programmen und Verzeichnissen unter Windows. Sie regelt die Vergabe von Privilegien an Prozesse und sie isoliert Prozesse und Fenster voneinander, die auf demselben Desktop mit unterschiedlichen Rechten laufen.

Mit Windows Server 2012 und Windows 7 wurde die UAC verfeinert, um die Verwaltung der Konfiguration und der Nachrichten zu erleichtern.

Die UAC stellt einen Kompromiss zwischen Sicherheit und Bequemlichkeit dar. Sie bietet kein vollständiges Sandboxing und kann auf verschiedene Arten umgangen werden, erhöht jedoch den Aufwand für Schadsoftware und ähnliche Bedrohungen bzw. kann helfen, deren Effekte einzugrenzen.

Eine noch stärkere Absicherung würde durch das Arbeiten mit komplett getrennten Konten samt wirklichem Kontowechsel für administrative Aufgaben erreicht. Dies wird bei hohem oder sehr hohem Schutzbedarf empfohlen. Die zweitsicherste Lösung ist die Nutzung getrennter Konten mit Rechteerhöhung für Standardnutzer durch Over-the-Shoulder-Abfrage (OTS). Zumindest sollte Arbeiten im Administratorbestätigungsmodus (Admin Approval Mode, AAM) aktiviert sein. Die Abschaltung der Benutzerkontensteuerung ist mit Windows Server 2012 gar nicht mehr möglich, aber auch eine automatische Rechteerhöhung ohne Nachfrage ist nicht zu empfehlen.

Allerdings ergibt sich bei vollständiger Trennung der Accounts das Problem, dass wenn sich Administratoren zunächst als Standardnutzer auf Servern anmelden können sollen, auch die Anmeldung aller Domänennutzer auf dem Server möglich ist. Dies ist nicht gewünscht, da sich so die Angriffsfläche deutlich erhöht. Entweder muss dies mit aufwändiger Konfiguration verhindert werden oder es kann auf die Alternative getrennter Admin-Systeme, sogenannte Privileged Access Workstations (PAWs), zurückgegriffen werden. Diese besonders geschützten dedizierten Systeme kommen in der Regel allerdings erst bei höherem Schutzbedarf infrage.

Achtung: Das vordefinierte Konto "Administrator" wird durch UAC niemals eingeschränkt. Unter Client-Betriebssystemen ab Vista hat dies normalerweise keine Auswirkungen, da dieses Konto nicht zum Login verwendet werden kann; hierfür werden stattdessen weitere Konten der Gruppe "Administratoren" angelegt. Windows Server (ab 2008) hingegen erzeugt bei der Installation keine zusätzlichen Konten und erlaubt die Anmeldung als "Administrator", ohne UAC. Das Konto "Administrator" sollte daher möglichst nicht zur regelmäßigen Systemverwaltung genutzt werden. Andere lokale oder Domänen-Konten, die "Administratoren"-Mitglieder sind, werden über UAC eingeschränkt.

## SYS.1.2.2.M4 Sichere Konfiguration von Windows Server 2012 (S)

Im Folgenden werden diejenigen wichtigen Sicherheitsmechanismen, d. h. Techniken, die der Sicherheit dienen oder eine wesentliche Auswirkung auf diese haben,in Windows Server 2012 (R2) kurz vorgestellt, bei denen der Sicherheitsverantwortliche oder Administrator eine Wahl zu treffen hat. Nicht aufgeführt sind solche Mechanismen, bei denen sich nichts im Vergleich auf die Vorgängerversionen verändert hat oder keine Gestaltungsfreiheit in der Anwendung besteht.

Windows Server 2012 (R2) bringt eine Reihe von Ressourcen und Tools bereits mit, die für eine Absicherung verwendet werden können und sollten. Diese sollten sich mit Sicherheitsfunktionen anderer IT-Systeme und Drittherstellerprodukte sinnvoll ergänzen, idealerweise im Sinn einer gestaffelten Verteidigung (Defense-in-Depth) überdecken und niemals gegenseitig aushebeln oder schwächen.

### Nicht mehrere wesentliche Funktionen pro Server

Mit der Forderung, dass nicht mehrere wesentliche Funktionen durch einen Server erfüllt werden sollen, wird eine grundlegende Aufteilung kritischer Serverfunktionalität auf verschiedenen Systeme angestrebt. Das im Unix-Bereich verbreitete "ein Dienst pro Server" passt hier nicht, da Dienst im engeren Sinn eher einen einzelnen Netzdienst beschreibt (z. B. Telnet). Hier geht es eher darum, funktional unabhängige Einheiten auch technisch voneinander unabhängig zu machen. Ein Webserver sollte beispielsweise nicht gleichzeitig als Terminalserver dienen, ein Fileserver nicht gleichzeitig als WSUS-Server. Bei Mehrschichtanwendungen wird in der Regel angestrebt, die einzelnen Schichten (etwa Datenbank / Geschäftslogik / Präsentation) in getrennte Server(-Cluster) abzubilden. Dies hat den Vorteil, dass das Netzes einfacher segmentiert werden und so besser dem Schutzbedarf und der Art der Bedrohungen angepasst sein kann. Außerdem ergeben sich Vorteile in der Wartung und Verwaltung.

### Security Baseline und SCM

Viele sicherheitsrelevante Einstellungen von Windows Server 2012 (R2) lassen sich am einfachsten über GPOs verwalten. Es empfiehlt sich, für alle Serversysteme oder für Serversysteme einer bestimmten Einsatzklasse eine sogenannte Baseline zu erstellen, also eine Vorlage, die optimale Sicherheitseinstellungen enthält, regelmäßig überprüft und fortgeschrieben wird und auf alle betriebenen Serversysteme ausgerollt wird.

Der Security Compliance Manager (SCM) ist ein kostenloses Tool von Microsoft, mit dem schnell GPOs erzeugt und verwaltet werden können und zudem Sicherheitsvorlagen für verschiedene Zwecke bereits mitbringt. Diese können dann mit verschiedenen Verfahren, wie z. B. Group Policy-Editor oder System Center Configuration Manager (SCCM) bzw. DCM (Desired Configuration Management, inzwischen umbenannt in Configuration Manager Compliance Settings), zentral ausgerollt werden. Auch eine Konfiguration von Stand-alone-Maschinen ist über das GPO Pack-Feature möglich, jedoch nur für die Ausnahme von Nicht-Domänenmitgliedern zu empfehlen.

Die konsequente Nutzung von SCM oder anderer Sicherheitsvorlagen und das zentrale Deployment von GPOs und/oder DCMs verbessern die Gleichförmigkeit und Nachvollziehbarkeit und helfen damit, Konfigurationsdrift zu verhindern und die Compliance zu erhöhen. Neben Betriebssystemeinstellungen können so auch viele Anwendungen verwaltet werden.

Insbesondere die im SCM verfügbaren Sicherheitsvorlagen enthalten für sehr viele Parameter bereits sicherere Einstellungen als die Grundeinstellung in Windows Server 2012 (R2). Häufig müssen diese allerdings noch auf den jeweiligen Einsatzzweck und die Gegebenheiten der Institution angepasst werden.

Falls die Institution nicht bereits über eine grundschutzkonforme Sicherheitsvorlage verfügt, sollte im SCM die Security Baseline für Windows Server 2012 bzw. R2 ausgewählt werden. Die gepackte .cab-Datei enthält die folgenden Komponenten:

- Windows Server 2012
- AD Certificate Services Server Security
- DHCP Server Security
- DNS Server Security
- Domain Controller Security Compliance
- Domain Security Compliance
- File Server Security
- Hyper-V Security
- Member Server Security Compliance
- Network Policy and Access Services Security
- Print Server Security
- Remote Access Services Security

- Remote Desktop Services Security
- Web Server Security
- Windows Server 2012 R2
- Domain Controller Security Compliance
- Domain Security Compliance
- Member Server Security Compliance
- Folgende Attachments liegen bei beiden jeweils bei:
- Security Guide.docx: dieser enthält die Beschreibung der gewählten Einstellungen
- CCE Reference.xlsm

Die Anpassung sollte auf der Grundlage der GPOs für die avisierte Rolle des Servers 2012 (R2) stattfinden. Alle Einstellungen sollten vor dem Ausrollen auf produktive Systeme gründlich getestet werden, da sonst leicht Fehlfunktionen auftreten können.

Es sollte nach jeder großen Änderung überprüft werden, ob die Einstellung erfolgreich geändert wurde und ob die Vorlage überhaupt auf die gewünschten Server angewandt wird, da hier viele Fehlerquellen lauern. Ein einfacher Weg dies zu tun ist die Ausführung des Group Policy Results Kommandozeilentools GPResult.exe auf dem Server.

Für weitere Informationen siehe auch Baustein APP.2.2 Active Directory.

### Absicherung des Internet Explorers

Der Browser auf dem Server, im Fall von Windows Server zunächst der IE, stellt ein mögliches Einfallstor für Angriffe aus dem Internet dar. Er sollte daher besonders abgesichert werden, selbst wenn das wilde Surfen per Richtlinie organisatorisch verboten ist.

### Enhanced Security Configuration

Bei Installation von Windows Server 2012 wird IE automatisch mit aktivierter Enhanced Security Configuration (ESC) installiert. Diese Konfiguration weist den in IE 10 definierten Zonen (Internet, Intranet, Trusted, Restricted) jeweils spezifische (höhere) Sicherheitslevel zu, z. B. "hoch" im Fall von Internet und Restricted Zone. Darüber hinaus enthält die Konfiguration eine Reihe von anderen Einstellungen, etwa zum Löschen der temporären Internetdateien beim Schließen des Browsers.

Dieser Modus hilft, die Angriffsfläche im Browser zu verringern und sollte daher beibehalten werden.

### Enhanced Protected Mode

Enhanced Protected Mode (EPM), ebenfalls ab IE 10 verfügbar, ist eine Erweiterung des mit IE 7 auf Windows Vista eingeführten Protected Mode. Zu dessen Maßnahmen gegen die Installation von Software und Manipulation des Systems durch den Browser kamen weitere Beschränkungen im Bezug auf die Informationsabfluss aus dem Intranet hinzu

EPM lässt sich entweder in der Group Policy Management Console (GPMC) unter "Windows Components\Internet Explorer\Internet Control Panel\Advanced Page" oder in der Registry (computerweit) unter "HKLM\Software\Policies\Microsoft\Internet Explorer\Main!Isolation" konfigurieren.

## SYS.1.2.2.M5 Schutz vor Schadsoftware auf Windows Server 2012 (S)

Bevor ein IT-System mit möglicherweise unsicheren Netzen verbunden wird sowie bevor Wechselmedien an dem IT-System angeschlossen werden, sollte auf jedem System mit Windows Server 2012 (R2) ein Virenschutzprogramm installiert werden, wenn nicht anderweitige Vorkehrungen gegen Schadprogramme getroffen werden. Dies zu planen und zu konfigurieren ist Gegenstand des Bausteins OPS.1.1.4 Schutz vor Schadprogrammen.

Bei Verwendung eines Virenschutzprogramms auf dem Server sollten die Signaturen mindestens täglich aktualisiert werden, zudem sollten regelmäßig alle Festplatten inklusive der Betriebssystempartition

vollständig gescannt werden. Geeignete Alarme für die zuständigen Administratoren sollten bei allen Arten von Ereignissen in Bezug auf Schadsoftware konfiguriert sein.

Unabhängig vom gewählten Antivirusprodukt kann zunächst das in Windows Server 2012 (R2) integrierte Microsoft-Produkt Windows Defender verwendet werden, bis die finale Lösung zum Schutz vor Schadprogrammen aktiviert werden kann.

### Windows Defender

Windows Defender war vor Windows Server 2012 eine reine Anti-Spyware-Lösung und stellt seitdem einen vollwertigen Virenschutz dar, ist allerdings für den Consumer-Bereich optimiert. Seit R2 ist Windows Defender auf Server Core standardmäßig aktiviert.

Windows Defender sollte aktiviert bleiben, bis eine alternative vollwertige Virenschutzlösung installiert wurde. Mehrere Antivirenprogramme (einschließlich Windows Defender) parallel dürfen nur betrieben werden, wenn die Empfehlungen beider Hersteller dies ausdrücklich erlauben, in der Regel ist dies nicht der Fall. Zudem erhöht jeder Virenscanner durch potentielle eigene Schwachstellen auch die Angriffsfläche des Servers.

## SYS.1.2.2.M6 Sichere Authentisierung und Autorisierung in Windows Server 2012 (S)

Authentisierung und Autorisierung spielen als zwei grundlegende Sicherheitstechniken an verschiedenen Stellen in Windows Server 2012 (R2) wichtige Rollen. Folgende Prinzipien können dabei als allgemeine Leitlinien der Realisierung dienen:

- Beschränkung und Schutz privilegierter Domänenaccounts
- Getrennte Accounts für Administration und andere Nutzung für Administratoren
- Spezielle abgesicherte Admin-Workstations
- Einschränkung der Konten, die sich interaktiv einloggen können
- Beschränkung von Account Delegation-Rechten für administrative Accounts
- Beschränkung und Schutz lokaler Adminaccounts
- Lokale Account-Beschränkungen für Remote-Zugriff
- Kein Netz-Login für lokale Accounts
- Individuelle Passwörter für lokale Admin-Accounts

### Geschützte Benutzer

Mit R2 kam die domänenbezogene globale Sicherheitsgruppe "Geschützte Benutzer" (Protected Users) hinzu. Die Anmeldeinformationen der Mitglieder dieser Gruppe werden durch standardmäßig restriktivere Sicherheitseinstellungen zusätzlich geschützt.

Der nicht weiter konfigurierbare Schutz gilt für alle Geräten, auf denen Windows Server 2012 R2 und Windows 8.1 ausgeführt wird sowie auf Domänencontrollern in Domänen mit einem primären Windows Server 2012 R2 Domänencontroller.

Der Speicherfußabdruck von Anmeldeinformationen wird durch mehrere Einschränkungen signifikant reduziert:

- NTLM, Digestauthentifizierung oder CredSSP sind deaktiviert.
- Kerberos nutzt in der Vor-Authentifizierung nicht die schwächere DES- oder RC4-Verschlüsselung.
- Das Konto kann nicht mit der eingeschränkten und uneingeschränkten Kerberos-Delegierung delegiert werden. Das bedeutet, dass frühere Verbindungen mit anderen Systemen fehlschlagen, wenn der Benutzer Mitglied der Gruppe "Geschützte Benutzer" ist.

- Eine Ticket-Granting-Ticket-Lebensdauer von vier Stunden kann via Active Directory-Verwaltungscenter (ADAC) über Authentifizierungsrichtlinien und Silos konfiguriert werden, sodass sich der Benutzer alle vier Stunden erneut authentifizieren muss.

Alle menschlichen Benutzer sollten möglichst Mitglieder der Gruppe "Geschützte Benutzer" sein.

Achtung: Konten für Dienste und Computer sollten nicht Mitglieder von "Geschützte Benutzer" sein, da die Gruppe keinen lokalen Schutz bietet: Kennwort oder Zertifikat sind immer auf dem System verfügbar.

### Gruppe "Managed Service Accounts"

Managed Service Accounts (MSA) sind eines der besonderen Features, die mit Windows Server 2008 R2 und Windows 7 hinzugekommen sind. Es handelt sich hierbei um Konten für Dienste (z. B. SQL Server oder Exchange) im Active Directory, die an einen bestimmten Rechner gebunden sind. Das Konto verfügt über sein eigenes komplexes Passwort und wird automatisch verwaltet. So kann ein MSA einfach und sicher Dienste auf einem bestimmten System ausführen, während die Möglichkeit, als ein bestimmter Benutzer-Principal auf Ressourcen im Netz zuzugreifen, gewahrt bleibt. Die Gruppe "Managed Service Account", die mit Windows Server 2012 geschaffen wurde, bietet dieselbe Funktionalität in der Domäne, jedoch zusätzlich mit der Möglichkeit, diese über mehrere Server zu erstrecken.

Wo immer möglich sollten für Dienstkonten MSA eingesetzt werden, sowie im Sinn einer einheitlichen Konfiguration und Beschränkung der Komplexität möglichst auch die Gruppe "Managed Service Account".

### LSA-Schutz in Windows Server 2012 R2

Die Local Security Authority (LSA), die den Local Security Authority Server Service (LSASS)-Prozess umfasst, authentisiert Benutzer bei lokalen und Netzanmeldungen und setzt die lokalen Sicherheitspolicies durch. Windows 8.1 und Windows Server 2012 R2 bieten zusätzliche Schutzmechanismen dafür, die ein Auslesen von Speicher sowie eine Injektion von Code erschweren. Dies erhöht den Schutz für Credentials, die in der LSA gespeichert und verwaltet werden, etwa gegenüber Pass-the-Hash-Angriffen. Auch Smartcard-Daten inklusive PINs sind dort abgelegt.

Dazu ist in der Registry unter "HKEY_LOCAL MACHINE > SYSTEM > CurrentControlSet > Control > Lsa" ein DWORD (32-bit) des Namens "RunAsPPL" mit Inhalt "1" einzutragen und der Server neu zu starten. Alternativ geht dies auch über eine GPO (Computer Configuration > Windows Settings > Hive > HKEY_LOCAL_MACHINE > SYSTEM\CurrentControlSet\Control\Lsa).

Um die erfolgreiche Einrichtung zu überprüfen, sollte im Event Viewer unter Windows Logs > System nach folgendem WinInit-Event Ausschau gehalten werden: "LSASS.exe was started as a protected process with level: 4".

In Kombination mit Secure Boot ist der Schutz besonders sicher, da er in dem Fall in UEFI generell aktiviert ist, unabhängig vom Inhalt der Registry.

### Dynamische Zugriffsregeln

In Windows Server 2012 wurde die Möglichkeit geschaffen, für die Autorisierung dynamische Zugriffsregeln für Dateien und Ordner zu definieren. Da diese einen wesentlich schlankeren und dadurch leichter zu pflegenden Regelsatz erlauben können, sollte ihr Einsatz geprüft und bevorzugt werden, wenn nicht andere, betriebliche Gründe dagegen sprechen.

## SYS.1.2.2.M7 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

## SYS.1.2.2.M8 Schutz der Systemintegrität (S)

Secure Boot sollte aktiv sein. AppLocker sollte aktiviert und möglichst strikt konfiguriert sein.

### Secure Boot

Bei Secure Boot handelt es sich um einen Sicherheitsstandard aus den Reihen der Computerhersteller. Das Verfahren versucht sicherzustellen, dass nur Software gebootet wird, die vom PC-Hersteller als

vertrauenswürdig angesehen wird. Realisiert wird dies durch digitale Signaturen auf Softwarekomponenten sowie eine Datenbank, die der Hersteller des Computers pflegt.

Beim Start des PCs prüft die Firmware die Signatur jeder Komponente der Boot-Software einschließlich der Treiber und des Betriebssystems. Nur wenn alle Signaturen gültig sind, wird der Bootprozess vollendet, andernfalls kommen herstellerspezifische Notmaßnahmen zum Tragen.

Nicht möglich ist die Nutzung von Secure Boot bei alter, nicht kompatibler Hardware oder im für den Serverbetrieb in der Regel nicht sinnvollen Dual Boot-Modus sowie bei virtuellen Maschinen, die Secure Boot nicht unterstützen.

Heutzutage kann in aller Regel von ausreichender Hardware und Kompatibilität ausgegangen werden, sodass es keinen Grund gibt, den wertvollen Integritätsschutz, den Secure Boot anbietet, nicht zu nutzen.

### AppLocker

AppLocker bietet richtliniengesteuerte Zugriffskontrolle für Anwendungen und andere ausführbare Dateien. Hiermit können bestimmte Anwendungen erlaubt, andere wiederum blockiert werden. Mit Windows Server 2012 kam die Funktion hinzu, Regeln für Anwendungspakete zu definieren, was die Konfiguration von AppLocker für Apps aus dem Windows Store erlaubt. Seit R2 gibt es die Möglichkeit, Laufzeitinformationen von Prozessen zu beobachten und im Sicherheitsprotokoll festzuhalten, die für die zielgenaue Einstellung von AppLocker verwendet werden können (Audit-Modus). Dies sollte genutzt werden, um Ausfälle bis hin um Aussperren der Administratoren aus dem System zu vermeiden.

AppLocker ist ein mächtiges Werkzeug, um die Ausführung schädlicher Software deutlich zu erschweren. Trotz diverser Erleichterungen bleibt jedoch immer noch ein erheblicher Konfigurationsaufwand, sodass sich der Einsatz von AppLocker vor allem empfiehlt, wenn hoher Integritätsbedarf besteht oder die Konfiguration eines Servers relativ statisch ist. Dies ist bei Serversystemen unter Windows 2012 (R2), die lediglich eine Rolle anbieten, nicht selten der Fall.

### Software Restriction Policies

Software Restriction Policies (SRP) ist eine ältere Funktion, mittels derer Programme identifiziert werden können, die auf Computern in der Domäne laufen sollen. Auch diese kann wie AppLocker dazu genutzt werden, mit großer Flexibilität die erlaubte Software in der ganzen Institution zu kontrollieren. SRP wird benötigt, wenn auch für Betriebssysteme vor Windows Server 2008 R2 oder Windows 7 Softwarebeschränkungen konfiguriert werden sollen, die kein AppLocker unterstützen.

Wie AppLocker auch wird SRP über GPOs konfiguriert. Wenn sowohl SRP- als auch AppLocker-Policies in derselben Domäne durch Gruppenrichtlinien angewandt werden, so werden die SRP-Richtlinien auf Rechnern, die AppLocker unterstützen, durch die AppLocker-Richtlinien überstimmt.

Es sollten immer getrennte GPOs verwendet werden, um SRP und AppLocker zu konfigurieren, um Fehler auszuschließen und insbesondere die Fehlersuche zu erleichtern.

## SYS.1.2.2.M9 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

## SYS.1.2.2.M10 ENTFALLEN (H)

Die zugehörige Anforderung ist entfallen.

## SYS.1.2.2.M11 Angriffserkennung bei Windows Server 2012 (H)

Oft stellt sich bei der Sicherheitvorfallsbehandlung heraus, dass die Protokollierung unzureichend war, um den Vorfall aufzuklären und Gegenmaßnahmen zielgerichtet planen zu können. Häufige Fehler sind:

- fehlendes zentrales Logging,
- fehlendes Logging von Mitgliedsservern und Endpunkten (nur Domaincontroller),
- Unübersichtlichkeit durch zu viele Daten im Protokoll,

- fehlende Aufzeichnung zentraler Ereignisse,
- zu schnelles Überlaufen (Rolling / Rotating) der Protokolle.

Z. B. werden zentrale Events wie Logins standardmäßig nur auf dem System selbst geloggt. Der AD protokolliert seinerseits nur die Ticketerstellung, hat aber kein Bild von der Session als solcher (inklusive deren Anfang und Ende).

Als Mindestanforderung sollten die folgenden Ereignisse von allen Systemen protokolliert und ausgewertet werden:

- das Löschen von Sicherheits-Logs,
- Änderungen an kritischen Gruppen wie Domänenadministratoren,
- Änderungen an lokalen Admingruppen,
- das Anlegen und Löschen lokaler Benutzer,
- die Installation neuer Dienste, vor allem auf Domänencontrollern (ein mögliches Anzeichen für Schadsoftware oder laterale Bewegungen von Angreifern).

Der erste Schritt zu einer Angriffserkennung ist die zentrale Sammlung aller relevanten Ereignisdaten. Eigens dafür entwickelte Systeme wie SIEM (Security Incident und Event Management) sind in der Regel teuer und aufwändig einzurichten und zu betreiben. Sie sind nicht Thema dieses Bausteins. Jedoch lässt sich bereits mit Windows Server-Bordmitteln Wesentliches erreichen.

### Nutzung des Windows Event Frameworks (WEF)

Mit dem Windows Event Framework (WEF) verfügt Windows über eine bereits integrierte Lösung, die mindestens als Komplement für ein SIEM eingesetzt werden kann. Wichtige Basisfunktionen einer Eventüberwachung können sogar komplett mit WEF realisiert werden.

Event Forwarding, also die gezielte automatische Weiterleitung von Events, kann die Sichtbarkeit kritischer Events deutlich erhöhen, insbesondere die von dezentralen Servern oder auch Clients, die keinen Agenten eines proprietären Monitoringsystems installiert haben. Die Auswahl, welche Events zentral geloggt werden sollen, ist außerhalb dieses Bausteins und als Teil eines übergreifenden Loggingkonzepts zu sehen (siehe Baustein OPS1.1.7 Protokollierung).

WEF lässt sich mit GPOs konfigurieren. Events können im nativen .evtx-Format exportiert werden. Dieses ist XML-basiert und damit leicht auswertbar.

Im Push-Modus leiten Systeme bestimmte Ereignisse automatisch an den sogenannten Collector (-Server) weiter. Somit ist es für Administratoren, die nicht Sicherheitsverantwortliche sind, möglich, für die von ihnen verantworteten Systeme zusätzliche Events zu konfigurieren.

Für die Einrichtung wird lediglich ein Windows Server benötigt und eine GPO. Außerdem muss dem Netzdienst (lediglich dem lokalen auf dem jeweiligen System) das Leserecht am Protokoll eingeräumt werden und der WinRM-Dienst muss auf allen zu beobachtenden Systemen gestartet sein. Er braucht nicht (auto-)konfiguriert zu werden, was ihn im lauschenden, sprich eher angreifbaren Zustand belassen würde. Werden lediglich kritisch Events geloggt, so ist nicht mit sehr großen Logdateien zu rechnen.

Auf dem Collector wird die Autokonfiguration über den Befehl "winrm qc" in einem administrativen Prompt aufgerufen. Automatisches Starten des WinRM-Dienstes sollte auf Nachfrage aktiviert werden, das ebenfalls abgefragte automatische Öffnen der Firewall lässt sich noch sicherer per GPO erledigen. Nun können im Eventviewer unter "Subscriptions" eingehende Events eingesehen werden.

Anschließend können per GPO die weiterzuleitenden Events definiert werden. Systeme, die die GPO anwenden, werden beim Windows Event Collector nachfragen, ob Subskriptionen für sie vorliegen und nur in diesem Fall die gewünschten Events senden.

Es ist durchaus möglich, die Gesamtheit aller Security Events der Domäne im WEF einzusammeln. Dies kann sinnvoll sein, wenn kein anderes zentrales Loggingsystem vorhanden ist und trotzdem forensische Untersuchungen möglich sein sollen. Ansonsten besteht die Stärke des WEF hauptsächlich in der gezielten

Sammlung und Filterung kritischer Ereignisse. So kann auch ein SIEM, das sämtliche Ereignisse aufzeichnet, am besten ergänzt werden: das SIEM für die Vollständigkeit, WEF für die Sichtbarkeit, auch in Bereiche der Umgebung, die nicht vom SIEM abgedeckt sind. Das SIEM kann Ereignisse aus diesen dann wiederum beim Collector abholen und somit noch besser die einheitliche Sicht auf alles bereitstellen.

### Sperrung nach missglückten Entschlüsselungsversuchen

Benutzerkonten können mit einer Schwelle versehen sein, wie viele Anmeldeversuche möglich sind, bevor der Account gesperrt ist. Dies ist ein Standardverfahren, um Brute-Force-Angriffe zu behindern. Gleichzeitig besteht die Gefahr, dass Sperren absichtlich provoziert werden, um Denial-of-Service zu erreichen.

Da Datenträgerverschlüsselung eine Erweiterung des Zugriffsschutzes auf die Daten auf Festplatten darstellt, die ebenfalls per Brute Force angegriffen werden kann, ist hier eine vergleichbare Maßnahme möglich:

Seit Windows 8 und Server 2012 ermöglicht die Policy "\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine account lockout threshold" ein automatisches Sperren von Partitionen nach einer definierten Anzahl vergeblicher Loginversuche im Sinn der Vernichtung des primären Key Protectors. Danach lässt sich das Volume nur noch per Wiederherstellungsschlüssel entschlüsseln. Dieser muss von einem autorisierten Benutzer im sogenannten "Device Lockout-Modus", in den das System automatisch rebootet, eingegeben werden, um wieder Zugriff zu erhalten. Es zählen fehlerhafte Loginversuche sowohl auf per Strg-Alt-Entf gesperrten Systemen als auch bei passwortgeschützten Bildschirmschonern.

Der Schwellwert kann zwischen 4 und 999 gewählt werden (1-3 werden automatisch als 4 interpretiert), 0 schaltet die Sperrung ab. Der Wert sollte mit der Schwelle für die normale Accountsperre korrelieren und jedenfalls nicht niedriger als diese sein, damit nach einer normalen Accountsperre noch ein normales Entsperren des Accounts veranlasst werden kann.

## SYS.1.2.2.M12 Redundanz und Hochverfügbarkeit bei Windows Server 2012 (H)

Wenn besonders hohe Verfügbarkeitsanforderungen an ein System bestehen, das unter Windows Server 2012 (R2) betrieben wird, so ergeben sich mögliche Maßnahmen im Wesentlichen aus der jeweiligen Anwendung. Bei einem Fileserver wird ein verteiltes Dateisystem eine Lösungsvariante darstellen, bei einem Active Directory der Einsatz mehrerer Domaincontroller und bei einem Webserver z. B. Load Balancing. Für das Thema Hochverfügbarkeit sei daher vor allem auf die jeweiligen Anwendungsbausteine verwiesen.

Darüber hinaus gibt es jedoch einige Maßnahmen, die auf Betriebssystemebene von Windows Server 2012 (R2) umgesetzt werden können, um die Verfügbarkeit zu erhöhen.

### Failover Cluster

Mehrere Windows-Server können in einem Verbund betrieben werden. Analog zu den Server-Rollen, die auf einzelnen Systemen laufen, gibt es auch diverse Cluster-Rollen, die in einem Failover-Cluster betrieben werden können. Dabei ist immer jeweils einer der Knoten des Clusters verantwortlich für den Betrieb der Rolle. Fällt der Knoten aus oder verliert er die Konnektivität, übernimmt einer der anderen Knoten. Die Ausfallsicherheit kann so erhöht werden, da im Fehlerfall ein anderes System den Betrieb übernimmt. Die Liste der Rollen, die direkt auf einem Cluster ausgeführt werden können, ist relativ eingeschränkt. Allerdings können auch virtuelle Maschinen auf einem Failover Cluster betrieben werden, so dass ganze Systeme, die kritische Dienste zur Verfügung stellen, als virtuelle Maschine hochverfügbar gemacht werden können.

### Network Load Balancing

Mit der Funktion Network Load Balancing können zwei oder mehr Windows Server Netzdienste über TCP/IP unter einer gemeinsamen Adresse anbieten. Die Server und die Dienste sind unabhängig voneinander und teilen keine Ressourcen. Netzanfragen an die gemeinsame Adresse werden auf die Server im Verbund verteilt.

### NIC-Teaming

NIC-Teaming (von Network Interface Card), auch bekannt als Load Balancing/Failover (LBFO) ermöglicht es, mehrere Netzschnittstellen in sogenannte Teams zusammenzufassen um

a.) Bandbreitenkapazitäten zu bündeln und/oder

b.) im Fall eines Versagens einer Schnittstelle oder Verbindung einen Failover (Rückfall) für den Netzverkehr zu haben.

Seit Windows Server 2012 ist diese Technik nativ im Betriebssystem verfügbar.

Da das Thema NIC-Teaming vielfältig ist und stark vom konkreten Einsatzszenario abhängt, können in diesen Umsetzungshinweisen nur allgemeine Hinweise gegeben werden. Für Details zu NIC-Teaming in Windows Server 2012 (R2) bietet Microsoft daher einen "NIC Teaming User Guide" an.

### Grundfunktion von NIC-Teaming

Netzwerkkarten der gleichen Geschwindigkeit lassen sich ohne Zusatzwerkzeuge zu Teams zusammenfassen, soweit die Hersteller die Funktion unterstützen. Mit Bluetooth- oder WLAN-Adaptern ist dies nicht möglich. Die Konfiguration erfolgt im Server-Manager oder per PowerShell, auch über das Netz.

Das LBFO in Windows Server 2012 lässt sich nicht mit NIC-Teaming anderer Hersteller kombinieren. Treten in so einem Fall Störungen auf, lässt sich die Teamkonfiguration mit der PowerShell folgendermaßen löschen:

Get-NetLbfoTeam | Remove-NetLbfoTeam

Kommt Virtualisierung mit Hyper-V zum Einsatz, so muss der Teamvorgang vor der Erstellung von virtuellen Switches in Hyper-V durchgeführt werden, da sonst die physische Netzverbindung nicht mehr für den Teamvorgang verfügbar ist. Darüber hinaus sind hier weitere Besonderheiten zu beachten.

### NIC-Teaming-Architektur

Es existieren verschiedene Architekturen, in denen NIC-Teaming verwendet werden kann. Bei Switch-unabhängigem Teaming weiß der Switch nichts von Teamzugehörigkeit, die NICs können auch an verschiedenen Switches angeschlossen sein, müssen dies jedoch nicht. Beim Switch-abhängigen Teaming, bei dem das gesamte Team am selben physischen Switch hängen muss, sind Netzwerkkarten und Switch für das Teaming konfiguriert. Dies kann statisch geschehen (eine Funktion, die typischerweise von Server-geeigneten Switchen unterstützt wird) oder dynamisch vereinbart werden über das Protokoll IEEE 802.1ax (LACP: Link Aggregation Control Protocol).

### Algorithmen zur Verteilung des Datenverkehrs

Um die mögliche kombinierte Bandbreite auch nutzen zu können, ist es notwendig, den Datenverkehr sinnvoll auf die Netzwerkkarten zu verteilen. In der Regel erfolgt dies nach Adress-Hashing, einem Verfahren, das Pakete anhand ihrer Adressdaten pseudozufällig auf die Adapter verteilt. Beim Einsatz von Virtualisierung kann eine viel feingranularere Verteilung erreicht werden, wenn zusätzlich der virtuelle Hyper-V-Switchport mit in den Verteilungsalgorithmus einbezogen wird.

Je nach Setup und Anforderungen bieten unterschiedliche Kombinationen aus Architektur und Verteilungsalgorithmus verschiedene Vor- und Nachteile.

### Unterschiede zwischen Windows Server 2012 und 2012 R2

Die hauptsächlichen Unterschiede in Bezug auf NIC-Teaming betreffen

- die Ergänzung des dynamischen Load Balancing-Modus (s. o.) und
- verbesserte Interoperabilität und Leistungsfähigkeit in Zusammenhang mit Hyper-V Netzvirtualisierung (NVGRE).

### BranchCache

BranchCache ist eine Technik zur Optimierung der Nutzung von Übertragungskapazitäten im WAN, z. B. bei der Anbindung von Außenstellen. Um Bandbreite zu sparen, kopiert BranchCache Inhalte von zentralen Servern und speichert diese in der Außenstelle (englisch branch office) zwischen (sogenanntes Caching), sodass sie bei erneutem Zugriff nicht mehr übertragen werden müssen.

BranchCache basiert auf tiefliegenden Funktionen des Windows Fileservers. So werden Dateien in kleine Abschnitte eingeteilt, um Duplikate finden und eliminieren zu können. Insbesondere kleinere Änderungen in großen Dateien führen so nicht zur kompletten Neuübertragung.

Die Konfiguration kann auch für größere Institutionen durch einen einzelnen kleinen Satz von GPOs erfolgen.

Mit Windows Server 2012 (R2) erfolgt die Speicherung des Caches inzwischen verschlüsselt, sodass zumindest bei normalen Vertraulichkeitsanforderungen auf eine weitere Verschlüsselung etwa der Datenträger verzichtet werden kann.

In vorherigen Versionen wurden Serverzertifikate benötigt, was einen komplexen PKI-Betrieb voraussetzte. Inzwischen werden diese nicht mehr benötigt, da Verschlüsselung und Authentisierung anders gelöst sind.

### SYS.1.2.2.M13 ENTFALLEN (H)

Die zugehörige Anforderung ist entfallen.

### SYS.1.2.2.M14 Herunterfahren verschlüsselter Server und virtueller Maschinen (H)

Wenn Festplatten verschlüsselt sind, um die Vertraulichkeit oder Integrität von Daten zu schützen, steht idealerweise der Schlüssel zur Entschlüsselung nicht permanent bereit, sondern erfordert eine Interaktion eines Administrators oder zumindest eine protokollierte technische Anfrage im Netz bzw. am AD. Ansonsten kann ein Angreifer oder Innentäter die Daten im laufenden Betrieb auslesen bzw. manipulieren. Dafür muss BitLocker bzw. die Geräteverschlüsselung in einem Modus aktiviert sein, der nicht ausschließlich auf dem TPM basiert, und der zusätzliche Schlüsselschutz (Key Protector), etwa ein USB-Key, sollte nicht permanent gesteckt sein. Dies erhöht zwar den Aufwand im Betrieb, stellt jedoch eine deutlich höhere Hürde für Angreifer dar.

## 2.2. Maßnahmen zum Baustein SYS.1.1 Allgemeiner Server

### SYS.1.2.2.SYS.1.1.M9 Einrichtung lokaler Paketfilter (S)

Grundsätzlich werden zentrale Maßnahmen wie Segmentierung von Netzen, Zonenbildung und Paketfilterung im Unternehmens- und Behördenbereich in der Regel durch dedizierte aktive Netzkomponenten realisiert, die an geeigneten Stellen aufgestellt werden. Im Sinn einer gestaffelten Verteidigung (Defense-in-Depth) sollte jedoch bei höherem Schutzbedarf auch die lokale Firewall aktiviert werden.

Windows Server 2012 (R2) bringt für diesen Zweck eine lokale Firewall mit, die sogenannte "Windows Firewall mit Advanced Security (WFAS)". Diese sollte aktiviert und für eingehenden wie ausgehenden Verkehr möglichst strikt eingestellt sein.

Die WFAS kann durch GPOs verwaltet werden. Dies ist zu empfehlen, um die Konfiguration konsistent und zentral zu halten. Die Verwaltung der konkreten Firewallregeln ist außerhalb des Scopes dieses Bausteins. Hierfür ist der Baustein Firewall anzuwenden.

Ebenfalls durch die WFAS realisiert werden die nativen IPsec-Features von Windows Server 2012 (R2). Diese sollten verwendet werden, um die Identität und Integrität der Verbindung zu Remote-Systemen sicherzustellen, da dies mit Paketfilterfunktionen allein nicht möglich ist. Die sichere Konfiguration von IPsec-Verbindungen ist ebenfalls nicht Inhalt dieses Bausteins. Sie wird im Baustein VPN abgehandelt.

### SYS.1.2.2.SYS.1.1.M24 Sicherheitsprüfungen für Server (S)

Auch bei Windows Server 2012 (R2) sollte die tatsächlich effektiv vorhandene Sicherheit regelmäßig auditiert werden, da nur so eine vollständige Umsetzung der Maßnahmen verlässlich geprüft werden kann.

#### Tools zur Überprüfung der Sicherheitskonfiguration (Assessment Tools)

Neben den Standardmitteln technisches Konfigurationsaudit und Penetrationstest (siehe Baustein SYS.1.1 Allgemeiner Server) bringt Windows Server 2012 (R2) eine Reihe von Tools mit, mittels derer die

Administratoren die Konfiguration überprüfen können. Diese sollten regelmäßig genutzt und die Ergebnisse dokumentiert sowie für die Planung der Verbesserung genutzt werden.

### Microsoft Security Assessment Tool 4.0

Beim Security Assessment Tool handelt es sich um eine sogenannte Risikomanagement-Anwendung. Diese ist als zweiteiliger Fragebogen realisiert. Der erste, kürzere Fragebogen nennt sich Business Risk Profile und versucht zu messen, wie viel Risiko mit der Geschäftstätigkeit der Institution verbunden ist. Da im IT-Grundschutz vergleichbare Verfahren verwendet werden, kann hier auf eine Anwendung verzichtet werden. Der zweite Teil heißt "Assessment" und ist aufwändiger zu beantworten. Es entsteht eine Auswertung der Effektivität der Sicherheitsstrategie in den vier Themenbereichen Personal, Prozesse, Ressourcen und Technik, basierend auf Best Practices und Standards wie ISO 27001 und NIST-800.x. Zwar ist auch dies in der IT-Grundschutz-Vorgehensweise bereits abgedeckt, jedoch können die vom Tool generierten Empfehlungen insbesondere aufgrund der zusätzlichen Hinweise und Verweise auf Material von Microsofts Trustworthy Computing Group lohnenswerte Quellen darstellen.

Darüber hinaus besteht die Möglichkeit des anonymisierten Uploads von Ergebnissen im Austausch für den Download von Benchmarks. Im Zweifel sollte auf den Upload verzichtet werden, um die mögliche Weitergabe von internen Informationen zu unterbinden.

### Microsoft Baseline Security Analyzer 2.3

Der Baseline Security Analyzer bietet eine effiziente Methode, um eine ganze Reihe häufiger, sicherheitsrelevanter Fehlkonfigurationen zu erkennen.

Zum einen wird auf fehlende sicherheitsrelevante Updates (und ausschließlich auf solche) geprüft, und zwar bei Windows, Windows-Komponenten wie Internet Explorer, IIS, anderen Microsoft-Produkten wie SQL Server und Office-Makroeinstellungen. Die Updates werden über den Windows Update Agenten abgefragt, der seit Windows 2000 Service Pack 3 auf allen Systemen vorhanden ist. Beim Test auf sogenannte unsichere Einstellungen ("less-secure settings"), auch als Vulnerability Assessment (VA) bezeichnet, wird gegen eine Datenbank von Registry- und Dateieinstellungen geprüft. Beispielsweise könnte ein VA ausgeben, dass die Berechtigungen in einem Verzeichnis unter /www/root zu lasch gewählt sind

Der Ausführende benötigt auf dem zu scannenden Server lokale Adminrechte, zudem müssen die administrativen Freigaben aktiviert sein.

### Security Configuration Wizard

Seit Windows Server 2003 Service Pack 1 auf Windows Serversystemen vorhanden ist das Tool Security Configuration Wizard (SCW). Es dient dazu, das Serverprofil zu prüfen und Empfehlungen zur Verbesserung der Sicherheit zu generieren. Bei Windows Server 2012 (R2) findet sich der SCW im neuen Server Manager-Dashboard.

Allgemein anerkannte grundlegende Empfehlungen wie "unbenutzte Dienste deaktivieren" oder "unbenutzte Features deinstallieren" werden auch in diesem Baustein genutzt. Wie aber ist in der Praxis nachprüfbar, dass bei einer großen Anzahl von Servern mit möglicherweise dutzenden von Rollen auf dem Netzserver und vielen unterschiedlichen Gruppen von Fileservern, Webservern, Datenbanken etc. alle nach Security Best Practice konfiguriert sind?

SCW kann helfen die Angriffsfläche zu verkleinern, indem Policies generiert werden, die einen Server auf die minimale Funktionalität beschränken, die für seine Rolle(n) benötigt wird.

Generierte Policies lassen sich direkt anwenden oder, dies ist zu empfehlen, als XML-Datei abspeichern. Aus diesen lässt sich über die PowerShell via

scwcmd transform /p:TemplateMeinServer.xml /g:GPO-Hardening-MeinServer

eine Policy (GPO) erzeugen, die dann auf alle Server mit derselben Charakteristik angewandt werden kann. Wie immer sollten neue Einstellungen kritisch begutachtet und vor Ausrollen auf Produktivsysteme getestet werden. Die Chance ist, dass so eine stärkere Standardisierung der Policies entsteht und die Konfigurationsdrift abnimmt.

## SYS.1.2.2.SYS.1.1.M34 Festplattenverschlüsselung (H)

Ein geeignetes Mittel zum Schutz der Vertraulichkeit von Daten im Ruhezustand, also nicht während des Transports, ist die Verschlüsselung von Festplatten und sonstigen Datenträgern. Dabei ist zu beachten, dass die Daten für die Bearbeitung entschlüsselt werden müssen (z. B. im Fall der Verschlüsselung des Bootmediums bereits während des Bootvorgangs) und grundsätzlich lesbar bleiben, bis das System heruntergefahren oder in den Ruhemodus versetzt wird. Da Serversysteme häufig rund um die Uhr laufen, ist der Schutz letztlich beschränkt, kann aber gegen physische Angriffe wie Diebstahl von Datenträgern gleichwohl hilfreich sein, wenn er mit geeigneten anderen Maßnahmen kombiniert wird. Windows bringt zu diesem Zweck das Tool BitLocker mit, das auch in Windows Server 2012 (R2) in allen Editionen verfügbar ist.

BitLocker unterstützt Geräteverschlüsselung auf x86- und x64-basierten Systemen, welche die Anforderungen des Windows Hardware Certification Kit (HCK) für ein TPM (Trusted Platform Module) und Secure Boot mit sogenannter "Connected Stand-by"-Funktion erfüllen. Die Geräteverschlüsselung schützt sowohl das Betriebssystem als auch weitere angeschlossene Festplatten. Grundsätzlich kann Geräteverschlüsselung mit einem Microsoft-Account oder einem Domänen-Account genutzt werden.

BitLocker unterstützt mit Windows Server 2012 (R2) die Algorithmen AES-128-CBC und AES-256-CBC. Zur Verschlüsselung mit BitLocker wird ein Key Protector benötigt, der vorhanden sein muss, um das Laufwerk entschlüsseln zu können. In der Standardkonfiguration sind dies ein TPM-Modul und ein zusätzlicher Wiederherstellungsschlüssel, mit dessen Hilfe das Laufwerk auch ohne das TPM-Modul entschlüsselt werden kann. Bei Enterprise-Umgebungen mit einem Active Directory kann der Wiederherstellungsschlüssel auch im Active Directory abgelegt werden.

### Windows Server 2012

Bezüglich Vorgängerversionen haben sich die Möglichkeiten von BitLocker in Windows 8 und Server 2012 erweitert:

### Installation

BitLocker kann nun Festplatten bereits während der Installation verschlüsseln. Dies ist zu empfehlen, da so das System nicht für gewisse Zeit im Klartext vorliegt.

Administratoren können dazu BitLocker vor der Installation vom Windows Preinstallation Environment (WinPE) aktivieren. Dies geschieht mit einem zufälligen Klartext-Schlüssel, der auf die frisch formatierte Festplatte angewendet wird, bevor der Setup-Prozess startet. Neu hinzugekommen ist auch die Option "Used Disk Space Only", bei der nur der bisher tatsächlich verwendete Speicher verschlüsselt wird. Dies benötigt an dieser Stelle in der Regel nur wenige Sekunden und behindert so den Installationsprozess nicht merklich.

Den BitLocker-Status einer Partition kann der Administrator im BitLocker-Control Panel oder auch im Windows Explorer prüfen. Wurde eine Festplatte während der Installation zunächst mit Klartext-Schlüssel verschlüsselt, wird der Status "Waiting For Activation" mit einem gelben Ausrufezeichen angezeigt. Dies bedeutet, dass für einen vollständigen Schutz der Partition der Schlüssel noch geschützt werden muss. Dafür fügt der Administrator über das Control Panel, das manage-bde-Tool oder die WMI-APIs einen geeigneten Schlüsselschutz hinzu.

### Schlüsselschutz (Key Protector)

Für einen vollständigen BitLocker-Schutz muss der zufällige Verschlüsselungsschlüssel seinerseits geschützt werden. Hierfür gibt es verschiedene Varianten:

| Speichermedium | Schlüsselschutz (Key Protector) |
|---|---|
| Betriebssystem | • TPM<br>• TPM+PIN<br>• Startup Key (für Systeme ohne TPM) (z. B. VMs)<br>• Password (für Systeme ohne TPM) (z. B. VMs) |
| andere Festplatte | • Automatischer Unlock<br>• Passwort<br>• Smartcard |
| Wechselfestplatte | • Passwort<br>• Smartcard |

### Used Disk Space Only

BitLocker bietet nun zwei Verschlüsselungsmethoden, "Used Disk Space Only" und "Full Volume Encryption". Ersteres arbeitet viel schneller während der Erstverschlüsselung, da zunächst nur die bereits genutzten Blöcke der Partition verschlüsselt werden. Die Vollverschlüsselung verschlüsselt immer alle Blöcke einschließlich des freien Speicherplatzes.

Folgende GPOs für BitLocker, die Used Drive Encryption bzw. Full Volume Encryption erzwingen, sind verfügbar unter \Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption

- Fixed Data Drives\Enforce drive encryption type on fixed data drives
- Operating System Drives\Enforce drive encryption type on operating system drives
- Removable Data Drives\Enforce drive encryption type on removable data drives

Ist hier nichts konfiguriert, kann der Administrator frei entscheiden, wenn er BitLocker aktiviert.

Bei normalen und hohen Vertraulichkeitsanforderungen genügt in der Regel die Teilverschlüsselung. Bei sehr hohen Vertraulichkeitsanforderungen sollte immer eine Vollverschlüsselung gewählt werden, da bereits die sich ändernde Datenmenge, die in dem Fall leicht ablesbar ist, Informationen über die Daten preisgeben kann (ein sogenannter Seitenkanalangriff). Auch für die Erreichung des Ziels Abstreitbarkeit ist eine Vollverschlüsselung zu empfehlen.

Wenn der erhöhte Zeitbedarf für die Vollverschlüsselung keine negative Auswirkung auf den Deploymentprozess hat, sollte grundsätzlich voll verschlüsselt werden.

### PIN- und Passwortänderung für Standardnutzer

Diese Funktion erlaubt einem Standardnutzer, die BitLocker-PIN bzw. das Passwort auf Betriebssystempartitionen bzw. das BitLocker-Passwort auf Datenpartitionen selbst zu ändern, was helfen kann, Anfragen an den Support zu reduzieren.

### Network Unlock

Diese Funktion ermöglicht, ein BitLocker-geschütztes System während des Bootvorgangs automatisch über das Netz zu entschlüsseln. Auch dies kann Anfragen beim Support vermeiden und trägt zur Benutzerfreundlichkeit bei.

Technisch handelt es sich bei Network Unlock um eine neue Option für den Schlüsselschutz. Benötigt wird dafür ein in der UEFI-Firmware implementierter DHCP-Treiber.

Betriebssystempartitionen, die mit TPM+PIN geschützt sind, verlangen die manuelle Eingabe der PIN beim Booten und Erwachen aus dem Ruhemodus (Hibernation), z. B. bei konfiguriertem Wake-on-LAN. Dies

macht es aufwändig, etwa automatisiert Patches auszurollen. Network Unlock bietet eine Möglichkeit, die Rechner trotzdem ohne Interaktion hochzufahren.

Ähnlich wie bei TPM+StartupKey wird hier ein verschlüsselter Startup Key aus dem Netz heruntergeladen und mit Hilfe des TPMs entschlüsselt. Der Netzschlüssel ist auf einem Systemlaufwerk im Netz gespeichert und mit einem AES 256-Bit-Sessionkey sowie dem 2048-Bit-RSA-Publickey des Serverzertifikats verschlüsselt. Ist Network Unlock nicht verfügbar, wird wie gehabt der normale TPM+PIN-Eingabebildschirm angezeigt. Serverseitig wird die Verteilung eines RSA-Schlüsselpaars per Group Policy Management Console auf dem Server 2012 Domain Controller benötigt.

### Unterstützung von Hardwareverschlüsselung

Mit Windows Server 2012 ist es möglich, auch andere, per Hardwareverschlüsselung verschlüsselte Festplatten in der BitLocker-Konsole zu verwalten, um eine gemeinsame Verwaltungsoberfläche zu schaffen.

### Windows Server 2012 R2

Mit Windows 8.1 und Server 2012 R2 kamen folgende Erweiterungen der BitLocker-Funktionalität hinzu:

Anders als die bisherige BitLocker-Implementierung ist die sogenannte Geräteverschlüsselung (Device Encryption), die im Hintergrund ebenfalls auf BitLocker basiert, automatisch aktiviert, sodass das Gerät von Anfang an verschlüsselt wird. Dies geschieht folgendermaßen:

Während einer Neuinstallation von Windows Server 2012 R2 wird der Server für die erste Verwendung vorbereitet. Dabei werden auch die Geräteverschlüsselung initialisiert und der Datenträger des Betriebssystems sowie die anderen Festplatten zunächst mit einem im Klartext gespeicherten Schlüssel verschlüsselt. Die Sicherheit der Daten zu diesem Zeitpunkt entspricht einer BitLocker-Verschlüsselung im Standby-Modus (Suspended), bei der der Schlüssel im Klartext auf der Festplatte vorliegt.

Falls der Server nicht zu einer Domäne hinzugefügt wird, wird ein Microsoft-Account benötigt, dem administrative Rechte auf dem Server eingeräumt wurden. Sobald der Administrator sich mit dem Microsoft-Account anmeldet, wird der Klartextschlüssel gelöscht, ein Wiederherstellungsschlüssel in den Microsoft-Account (online) hochgeladen und der TPM-Schutz erstellt. Sollte der Wiederherstellungsschlüssel später benötigt werden (z. B. bei einem Schaden des TPM), kann der Administrator diesen über ein Zweitgerät und das Microsoft-Konto wieder beziehen.

Meldet sich der Benutzer über einen Domänenaccount an, wird der Klartextschlüssel erst in dem Moment gelöscht, wenn der Server die Domäne betreten hat und der dann erzeugte Wiederherstellungsschlüssel erfolgreich in die Active Directory Domain Services gesichert wurde. Die GPO "Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives" muss aktiviert und die Option "Do not enable BitLocker until recovery information is stored in AD DS for operating system drives" sollte ausgewählt sein. Erst danach aktiviert sich der TPM-Schutz und schließt so die Geräteverschlüsselung ab.

Im Einsatz in Behörden und Unternehmen sollte der Wiederherstellungsschlüssel im AD gespeichert und auf die Online-Variante mit dem Microsoft-Konto verzichtet werden, da im letzteren Fall keine Kontrolle darüber besteht, was mit diesem Schlüssel geschieht.

### FIPS-Unterstützung für das Recovery-Passwort

Seit Windows Server 2012 R2 existiert ein FIPS-Modus, der es erlaubt, BitLocker kompatibel mit dem US-amerikanischen öffentlichen Krypto-Standard (Federal Information Processing Standard) zu betreiben.

### BitLocker auf virtuellen Maschinen

Die Verschlüsselung von virtuellen Maschinen bietet sich an, wenn entweder das Hostsystem nicht verschlüsselt werden kann oder soll oder aber der Vertraulichkeitsbedarf der Daten in der VM höher ist oder diese aus anderen Gründen vom Hostsystem abgeschirmt werden sollen. Auch hier gilt, dass Festplattenverschlüsselung (FDE: Full Disk Encryption) keinen wirksamen Schutz gegen Auslesen von Daten im laufenden Betrieb, d. h. mit entschlüsselten Datenträgern, darstellt. Als Zusatzmaßnahme kann daher organisatorisch festgelegt werden, dass verschlüsselte VMs erst dann entschlüsselt werden dürfen, wenn sie benötigt werden und nach Benutzung möglichst schnell wieder heruntergefahren werden müssen.

Da virtuelle Maschinen nicht über ein TPM verfügen, müssen folgende zwei Schritte ausgeführt werden, bevor BitLocker (das auf dem Server installiert sein muss) aktiviert werden kann:

1. In der GPO "Computer Configuration/Administrative Templates/Windows Components/BitLocker Drive Encryption/Operating System Drives" muss "Require additional authentication at startup" auf "Enable" und "Allow BitLocker without a compatible TPM" konfiguriert sein (z. B. mit dem lokalen Gruppenrichtlinieneditor gpedit.msc).

2. Nach einem Neustart der VM ist im Control Panel BitLocker zu aktivieren.

## 2.3. Maßnahmen zum Baustein ORP.4 Identitäts- und Berechtigungsmanagement

Dieser Abschnitt enthält allgemeine Informationen zum Identitäts- und Berechtigungsmanagement unter Windows Server 2012.

Für Windows Server 2012 sollte ein rollenbasiertes Administrations-Modell für die Administration unterschiedlicher Serverfunktionen entworfen und umgesetzt werden. Für kritische Dienste sollte eine Zwei-Faktor-Authentifizierung implementiert sein.

### Rollenbasiertes Administrationskonzept

Die Unterscheidung in Administratoren und normale Benutzer ist wichtig, allerdings relativ grob. Sie missachtet, dass es in der Realität verschiedene Arten administrativer Aufgaben oder, allgemeiner gesprochen, hierarchischer und teilweise auch überlappender Rollen und Verantwortlichkeiten gibt. Um das Prinzip des Least Privilege konsequenter durchzusetzen, ist daher ein feingranulareres rollenbasiertes Administrationskonzept zu entwickeln. Dies ist insbesondere für größere Institutionen sinnvoll und realistisch.

Ein solches Administrationskonzept kann nicht allein mit Blick auf Windows Server 2012 (R2) aufgestellt werden. Vielmehr sind unterschiedliche Rollen (verschiedene Arten von Domain Controllern, Mitgliedsserver, Clientsysteme etc.) zu betrachten. Dieser Versuch wird im Baustein APP.2.2 Active Directory unternommen.

### Smartcards

Smartcards eignen sich als schwer zu fälschende mobile Sicherheitsmerkmale, etwa in der Zwei-Faktor-Authentifizierung oder für Signaturen. Mit Windows Server 2012 wurde die Nutzung von Smartcards im Sinn der stärkeren Integration in eine größere Anzahl von Anwendungen verbessert. Zudem kam die Möglichkeit hinzu, sogenannte virtuelle Smartcards zu verwenden.

### Virtuelle Smartcards

Virtuelle Smartcards ermöglichen Multi-Faktor-Authentifizierung in vielen Arten von Infrastrukturen auch in dem Fall, dass Benutzer keine physische Karte mit sich führen. Hierfür wurde der Prozess vereinfacht, beliebige Geräte mit TPM als virtuelles Smartcard-Gerät zu registrieren, unabhängig davon, ob sie Domänenmitglieder sind und wie ihre Hardware ansonsten beschaffen ist. Dies setzt die Hürde für den Einsatz von Smartcards als weiteres Authentifizierungsmerkmal deutlich herab.

### Windows Biometric Framework

Auch das Windows Biometric Framework (WBF), ein Satz an Diensten und Schnittstellen für biometrische Devices, wurden erweitert. Fast User Switching und die Synchronisation von Passwörtern mit Fingerabdrücken sind nun möglich.

Es ist jedoch zu beachten, dass biometrische Daten einige Nachteile haben, die sie als Identifikations- und Authentifizierungsmerkmale aus Sicherheitssicht weitgehend unbrauchbar machen. Neben der Tatsache, dass viele biometrische Merkmale weltweit nicht eindeutig sind, sind sie häufig relativ leicht zu fälschen und können vor allem, einmal bekannt geworden, nicht geändert werden.

# 3. Weiterführende Informationen

## 3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

## 3.2. Quellenverweise

Für diese Umsetzungshinweise sind keine Quellenverweise vorhanden.