ERNW Newsletter 40 / Juli 2012

Liebe Partner, liebe Kollegen,

willkommen zur 40. Ausgabe des ERNW Newsletters mit dem Thema:

Windows Server 2008 R2 und Active Directory BSI-compliant {gehärtet}

Version: 1.0

Datum: 19.07.2012

Autoren: Friedwart Kuhn, Dominik Phillips

ERNW Enno Rey Netzwerke GmbH

Carl-Bosch-Str. 4

69115 Heidelberg

Tel. +49 6221 480390

Fax +49 6221 419008

www.ernw.de

1 EINLEITUNG

Dieser Newsletter stellt die (anonymisierte und abstrahierte) Kurzfassung eines Kundenprojekts in einer großen öffentlichen Organisation vor, das die folgende Zielstellung hatte: Windows Server 2008 R2-basierte Systeme und ein Windows Server 2008 R2-basiertes Active Directory sollte gemäß Anforderungen des Grundschutzes gehärtet und vom BSI abgenommen werden. Einige der im Active Directory integrierten Systeme hatten aufgrund der Verarbeitung von personenbezogenen oder personenbeziehbaren Daten im Sinne des BDSG über den Grundschutz hinausgehende Anforderungen zu erfüllen. Die Abnahme der Gesamtumgebung fand im vergangenen Jahr statt.

Das Problem bei der Erfüllung der Zielstellung, ein Server 2008 R2-basiertes Active Directory „Grundschutz-compliant" zu machen, hat zwei Hauptkomponenten:

- Zum einen befinden sich die vom BSI empfohlenen Maßnahmen auf unterschiedliche Bausteine der (mehrere tausend Seiten umfassenden) Grundschutzkataloge verteilt. Für den mit den Grundschutzkatalogen nicht vertrauten (aber Windows-versierten) Leser ergibt sich daraus dann immer noch die Schwierigkeit, sich von allgemeinen Maßnahmen wie etwa aus den Baustein „Allgemeiner Server" und „Allgemeiner Verzeichnisdienst" zu spezielleren Maßnahmen wie etwa „Active Directoy" oder „Planung von Gruppenrichtlinien" mühsam durchzuarbeiten (vgl. [8]). So dass es zur Abnahme von gemäß Grundschutz gehärteten Systemen im Grunde genommen zwei spezifische Fachkenntnisse braucht: die eines Windows-Spezialisten und die eines Grundschutz-Spezialisten.
- Zum anderen gab es bis vor etwa zwei Monaten überhaupt keinen Baustein zu Windows Server 2008 (R2).

Das erste Problem besteht nach wie vor. Das zweite Problem beginnt sich zu lösen, da das BSI seit kurzem einen Entwurf für einen Baustein zu Windows Server 2008 (R2) bereitstellt (vgl. [6]). Dieser Newsletter möchte nun eine grundsätzliche Orientierung und einen Leitfaden für ein gemäß BSI-Grundschutz (und teilweise darüber hinaus ;-)) gehärtetes Windows Server 2008 R2-basiertes Active Directory und darin integrierte Windows Server 2008 R2-basierte Systeme geben. Da dieses Thema naturgemäß zu umfangreich für eine detaillierte Behandlung ist, seien auch gleich die in dem Newsletter vorgenommen Einschränkungen benannt:

- Es werden die für die Abnahme durch das BSI benötigten Aspekte, nicht jedoch sämtliche Konfigurationen im Detail besprochen.
- Die Betrachtung beschränkt sich auf das Active Directory, die dort integrierten Windows Server 2008 R2-basierten Server-Systeme und zugeordnete administrative /operative Prozesse. Die Betrachtung von Grundschutzkatalog-konformen Clients ist einem späteren Newsletter vorbehalten.
- Wichtige allgemeine ISMS-Prozesse (etwa Incident Response, Business Continuity Management, Legal Compliance) werden aufgrund ihres allgemeinen Charakters nicht in diesem Newsletter diskutiert.

Die Einleitung soll mit einer Bemerkung der ‚Kompatibilität der hier empfohlenen Maßnahmen' zu Maßnahmen aus ISO 27001/2 abgeschlossen werden: Sämtliche in diesem Newsletter genannten Aspekte der sicheren Konfiguration und des sicheren Betriebs von Windows Server 2008 (R2)-basiertem Active Directory sind konform zu (unterschiedlichen) Anforderungen von ISO 27001/2. Die Zuordnung der im Folgenden genannten Maßnahmen zur Absicherung gemäß Grundschutz zu ISO 27001/2 und ihre diesbezügliche Diskussion sind ebenfalls einem zukünftigen Newsletter vorbehalten.

Schließlich noch eine Lesehilfe: Konformität der empfohlenen Maßnahme zu den Grundschutzkatalogen und dem Entwurfsbaustein zu Windows Server 2008 (R2) finden unter jeder Maßnahme durch Verweis auf eine Referenz zu den Grundschutzkatalogen, bzw. dem Entwurfsbaustein (die Referenz enthält aufgrund des Entwurfcharakters ein „x"), sofern sich das BSI in den genannten Werken dazu äußert.

Wir wünschen Ihnen viel Spaß und Erkenntnisgewinn bei der Lektüre!

2 GERÄTE- UND ZUGANGSSCHUTZ

Der Physische Zugriff sowie das sichere Booten des Betriebssystems soll durch geeignete Verfahren geregelt werden. Die Maßnahmen reichen hierbei von physisch und logisch geschützten Hardware-Anschlüsse bis zu BIOS-Einstellungen. Die Unterpunkte dieses Abschnitts geben einen Überblick hierüber.

2.1 Physischer Schutz

Eine vom BSI abgenommene Möglichkeit des physischen Schutzes könnte wie folgt aussehen: Jedes System befindet sich in einem nach ISO 27001 zertifizierten Rechenzentrum und dort in einem sicheren Rack mit physischem und elektronischem Schloss (etwa von Rittal). Anmeldungen in dem Rechenzentrum dürfen (auf der Kunden-Seite) nur von dazu autorisierten Personen und auch nur für autorisiertes administratives Personal getätigt werden. Der Zugang zu dem Schlüssel für das (in einem Cage befindliche) abschließbare Rack erfolgt nach dem Vier-Augen-Prinzip. In dem Rack befindet sich etwa ein Blade-Enclosure-System für die Server-Systeme. Das System wird über iLO[1], bzw. den HP Onboard Administrator administriert (siehe Abschnitt: 0)

- Maßnahme ist konform zu M2.17

2.2 Physisch geschützte Hardware-Anschlüsse

Da sich das System (im Fall des durchgeführten Projekts) in einer Blade-Enclosure befindet, deren Zugang physisch und logisch geschützt ist, müssen Hardware-Anschlüsse nicht mehr gesondert im BIOS deaktiviert werden.

- Vergleiche B2.7

2.3 Sicheres Booten

Das Booten des Betriebssystems von anderen Medien als der installierten Festplatte soll nicht möglich sein. Hierzu sollten die folgenden Bios-Einstellungen definiert werden:

- Es sollte nur von der Festplatte gebootet werden können, auf der sich %Systemroot% befindet.
- Die Auswahl eines Bootmenüs sollte Benutzern nicht möglich sein.

Für den Bootprozess des Systems sollte ausschließlich der Windows-eigene Bootmanager (bootmgr) verwendet werden. D. h. es sollte kein weiterer Bootmanager für das Booten eines anderen Betriebssystems installiert sein.

- Maßnahme ist konform zu M4.84

1 Integrated Lights Out (iLO) ist eine Systemverwaltungseinheit, welche die aktive Verwaltung und Überwachung von Serversystemen ermöglicht. Siehe http://h20341.www2.hp.com/integrity/w1/en/software/integrity-lights-out.html?jumpid=ex_r11294_us/en/large/tsg/go_integrityilo.

3 PASSWORTSCHUTZ

Für sämtliche Zugriffspunkte, an denen ein Passwort eingegeben werden muss, sollte eine angemessene Password-Policy definiert werden, die aktuelle Best Practice erfüllt.[2]

3.1 BIOS-Passwortschutz

Der Zugang zum BIOS soll durch ein Passwort geschützt sein. Für dieses Passwort wird die folgende Richtlinie empfohlen:

Minimale Passwortlänge: 7 Zeichen

Verwendung von Groß- und Kleinschreibung: Ja

Verwendung von alpha-numerischen Zeichen: Ja

Verwendung von Sonderzeichen: Nein

- Maßnahme ist konform zu M4.84

3.2 Passwortrichtlinie für den Systemzugang

Der Zugang zum System muss durch ein Passwort geschützt sein. Jedes Benutzerkonto (und auch Dienstkonto) auf dem System ist durch ein Passwort geschützt. Für dieses Passwort gelten gemäß Best Practices die folgenden Richtlinien.

- Maßnahme ist konform M4.48, M4.133, M2.11

Für den Systemzugang sollte eine Passwortrichtlinie definiert werden. Eine angemessen sichere Passwortrichtlinie könnte hierbei wie folgt aussehen:

- Kennwort muss Komplexitätsanforderungen[3] entsprechen: Aktiviert
- Kennwortchronik erzwingen: 6 gespeicherte Kennwörter
- Kennwörter mit umkehrbarer Verschlüsselung speichern: Deaktiviert
- Maximales Kennwortalter: 90 Tage
- Minimale Kennwortlänge: 8 Zeichen
- Minimales kennwortalter: 1 Tag

Die Kontosperrungsrichtlinie sieht dabei wie folgt aus:

- Kontensperrungsschwelle: 3 ungültige Anmeldeversuche
- Kontosperrdauer: 60 Minuten
- Zurücksetzungsdauer des Kontosperrungszählers: 30 Minuten

2 Gemäß Empfehlung BSI zum Erstellen und Verwalten von sicheren Kennwörtern, aus den Bausteinen „Regelung des Passwortgebrauchs" M 2.11 und „Passwortschutz für IT-Systeme" M4.1.

Das Rekonstruieren unzureichend komplexer Passworte ist unter Zuhilfenahme verschiedener Methoden möglich, deren bekannteste wohl das sog. „Brute-Forcing" ist. Die interessante Arbeit „Adaptive Password-Strength Meters from Markov Models" untersucht Metriken, zur Bestimmung der Komplexität von Passworten (siehe [Referenz].

3 Hier sind die Microsoftschen Komplexitätsanforderungen gemeint, nach denen mindestens drei der folgenden vier Bedingungen erfüllt sein müssen: Passwort muss Groß- und Kleinschreibung enthalten, Passwort muss Zahl(en) enthalten, Passwort muss Sonderzeichen enthalten, Benutzeranmeldename darf nicht im Passwort enthalten sein.

3.3 Granulare Passwortrichtlinie (fine grained password policy) für priviligierte Konten

Auf Windows-Systemen bietet sich seit Windows Server 2008 die Möglichkeit, für privilegierte Konten (etwa administrative Konten) eine eigene (strengere) Passwortrichtlinie per Gruppenrichtlinienobjekt (im Folgenden kurz „GPO) zu definieren.

Für privilegierte Konten[4] sollte eine granulare Passwortrichtlinie definiert werden. Die granulare Passwortrichtlinie kann dabei wie folgt aussehen:

- Kennwort muss Komplexitätsanforderungen genügen: Aktiviert
- Kennwortchronik erzwingen: 10 gespeicherte Kennwörter
- Kennwörter mit umkehrbarer Verschlüsselung speichern: Deaktiviert
- Maximales Kennwortalter: 180 Tage
- Minimale Kennwortlänge: 12 Zeichen
- Minimales kennwortalter: 1 Tag

Die Kontosperrungsrichtlinie sieht dabei wie folgt aus:

- Kontensperrungsschwelle: 6 ungültige Anmeldeversuche
- Kontosperrdauer: 30 Minuten
- Zurücksetzungsdauer des Kontosperrungszählers: 10 Minuten

In dem Entwurf des Bausteins zu Windows Server 2008 (R2) wird die granulare Passwortrichtlinie zwar erwähnt (vgl. M4.x-8), es gibt jedoch keine konkrete Empfehlung vom BSI, grundsätzlich gelten daher M4.48, M4.133 und M2.11.

4 Das gilt mindestens für die folgenden Konten: Administratoren (lokal und auf den Domänencontrollern), Domänen-Admins, Organisations-Admins, Schema-Admins. Nach Bedarf können weitere Konten – sofern verwendet – eingeschlossen werden wie etwa die DNS-Admins.

4 Sichere Konfiguration des Betriebssystems

4.1 Abschalten nicht benötigter Komponenten und Funktionen

4.1.1 Deinstallation nicht benötigter Server-Rollen und Features

Jede installierte Serverrolle und jedes installierte Feature erhöhen durch zusätzlichen Code auf dem System und zusätzliche Funktionalität des Systems dessen Angriffsfläche. Deshalb sollten auf jedem System nur die für die spezifische Funktionalität des Servers benötigten Rollen und Features installiert sein. Wird eine Server 2008 R2-basiertes System neu installiert, so sind – anders als etwa bei Systemen vor Windows Server 2008 – kaum zusätzliche Komponenten installiert, so dass die Organisation die Möglichkeit hat, benötigte Rollen und Features nach Notwendigkeit zu installieren. Handelt es sich um ein System, dessen Rolle oder Funktion verändert wird, dann können und sollten (!) nicht benötigte Features und Rollen (wieder) deinstalliert werden. Eine besondere Rolle spielt hierbei die Server Core-Installation, bei der das sog. „Minimal-Machine"-Prinzip in besonders hohem Maße umgesetzt werden kann.[5]

- Vergleiche M4.95, M4.x-8 [6]

4.1.2 Deaktivierung nicht benötigter Dienste

Jeder Dienst der auf einem System ausgeführt wird, erhöht (ebenso wie jede Serverrolle und jedes Feature) dessen Angriffsfläche. Nicht benötigte Dienste sollen daher deaktiviert werden. Diese Frage ist in der Praxis nicht immer leicht zu beantworten. Im Vergleich zu Windows Server 2003 sind auf einem Windows Server 2008 R2-basierten System per Default weniger Dienste aktiviert als auf einer Standardinstallation von Windows Server 2003. Die hier vorgenommen Einstellungen beruhen auf folgenden (im zugehörigen Projekt) definierten Anforderungen: Ausgangspunkt sind die Dienste einer Standard-Installation von Windows Server 2008 R2, von denen die nicht-benötigten deaktiviert werden sollen. Die hier vorgenommen Einstellungen gelten für das Basis-Server-System, und zwar zunächst einmal ohne die Installation weiterer Rollen. Die Installation besonderer Rollen und Features erfordert dann eine Betrachtung der notwendigen Dienste für die jeweilige Serverrolle. Die hier vorgenommenen Einstellungen lassen sich jedoch auch auf die Rollen „Domänencontroller" und „Anwendungsserver" übertragen[6]. Bei zusätzlich installierten Diensten – als Beispiel sei hier der PC/SC-Dienst für einen Smartcard-Kartenleser genannt – sollte geprüft werden, ob der Dienst auch noch dann fehlerfrei arbeitet, wenn statt der Startart „automatisch" die Startart „manuell" gewählt wird. Im vorgenannten Beispiel ist dies etwa der Fall.

Die folgende Liste deaktivierter Dienste geht über die Grundschutzempfehlungen hinaus, und beschreibt ein fortgeschrittenes Hardening, das Zugunsten einer Reduktion der Angriffsfläche (leichte) Einschränkungen in der Funktionalität in Kauf nimmt.[7] Wenn dies auf jeden Fall vermieden werden soll, dann ist man mit einer Default-Konfiguration der Dienste unter Windows Server 2008 (R2) immer noch auf einer ziemlich sicheren Seite, da Dienste und Sonderfunktionalitäten (Features) in diesen Betriebssystemversionen erst explizit hinzugefügt oder aktiviert werden müssen. Vor einer individuellen Umsetzung der in der Liste vorgenommenen Deaktivierungen wird dringend empfohlen, zu prüfen, ob die Deaktivierung zu unerwünschten Komplikationen oder einem erhöhten Betriebsaufwand (etwa durch zu überprüfende Meldungen im Ereignisprotokoll) führt.

- Vergleiche M4.95, M4.x-8 [6]

[5] Weitere Informationen zur Server Core-Installation finden sich z. B. unter: http://technet.microsoft.com/de-de/library/cc771345(v=ws.10)

[6] Hier müsste ggf. der Druckwarteschlangendienst wieder aktiviert werden.

[7] Sichtbar etwa am Fall des deaktivierten Dienstes „Shell Hardware Detection", dessen Deaktivierung dafür sorgt, dass angeschlossene Medienlaufwerke keine (sichtbare) Meldung über die GUI ausgeben.

Dienstname	*Server 2008 R2 Default-Einstellung für die Startart des Dienstes*	*Vorgenommene Einstellung*
Application Layer Gateway Service (Gatewaydienst auf Anwendungsebene)	manuell (gestartet)	deaktiviert
Application Experience Lookup Service (Awendungserfahrung)	manuell (gestartet)	deaktiviert
Application Management (Anwendungsverwaltung)	manuell	deaktiviert (wenn in der Umgebung keine Anwendungen über GPOs veraltet werden)
Audio Server /Windows Audio	manuell	deaktiviert
Dot3svc (Automatische Konfiguration)	manuell	deaktiviert
IPSec Policy Agent [8]	manuell	manuell
Remote Access Auto Connection Manager (Verwaltung für automatische RAS-Verbindung)	manuell	deaktiviert (nicht benötigt auf Servern im LAN)
Remote Access Connection Manager (RAS-Verbindungsverwaltung)	manuell	deaktiviert (nur im Zusammenhang mit VPN-Verbindungen benötigt)
Smart Card	manuell	deaktiviert (wenn keine Smartcards auf den Servern verwendet werden)
Smart Card Removal Policy	manuell	deaktiviert (wenn keine Smartcards auf den Servern verwendet werden)
TPM Base Services	manuell	deaktiviert (wenn TPM nicht benötigt wird)
Windows Audio Endpoint Builder	manuell	deaktiviert
WinHTTP Web Proxy Auto Discovery Service	manuell	deaktiviert
Certificate Propagation (Zertifikatverteilung)	manuell	deaktiviert (wenn keine Smartcards auf den Servern verwendet werden)
Print Spooler (Druckwarteschlange)	automatisch	deaktiviert (wenn keinerlei Druckfunktionalität benötigt wird)
Shell Hardware Detection (Shellhardwareerkennung)	automatisch	deaktiviert (wenn keinerlei Autoplay oder Media-Device-Automatik auf dem Server benutzt werden soll)

[8] Achtung: Dieser Dienst ermöglicht nicht nur IPSec, sondern auch die Remoteverwaltung der Windows-Firewall (deshalb sollte dieser Dienst i. d. Regel nicht deaktiviert werden).

4.1.3 Deaktivierung nicht benötigter Freigaben

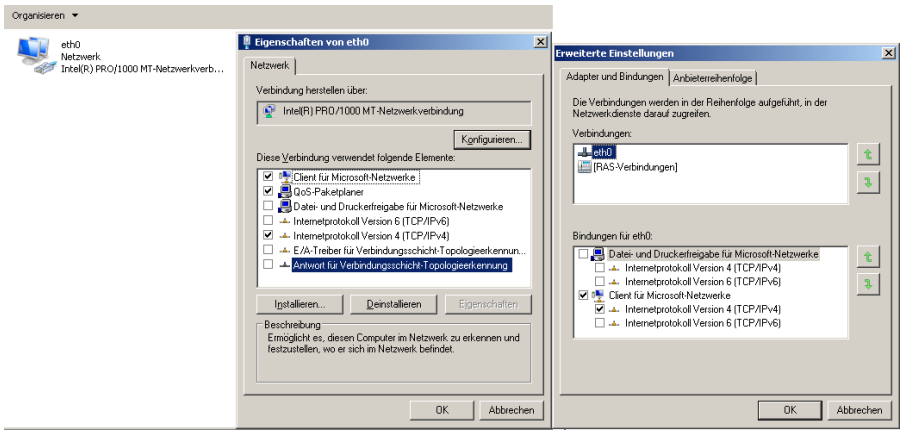
Das Betriebssystem vergibt standardmäßig spezielle versteckte Freigaben (die sog. „administrativen Freigaben"), welche im Wesentlichen von Administratoren, aber auch Anwendungen und Diensten verwendet werden können [2]. Ob ein System automatisch administrative Freigaben erstellt, definiert der Parameter „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\ AutoShareServer". Es wird empfohlen, nur die vom System vordefinierten administrativen Freigaben zu verwenden.

Auf Systemen mit Hochsicherheitsanforderungen kann es notwendig sein, die administrativen Freigaben dauerhaft zu deaktivieren.

4.2 Sichere Netzwerkkonfiguration[9]

In den Netzwerkverbindungen (ncpa.cpl) ist definiert, welche Netzwerkschnittstellen vom System verwendet werden und welche Dienste und Protokolle an diese Netzwerkschnittstellen gebunden sind.

Die folgende Abbildung zeigt, die Netzwerkschnittstelle *eth0* mit den folgenden Einstellungen.



Es gelten nun die grundsätzlichen Empfehlungen:

- Nicht benötigte Netzwerkschnittstellen sollten deaktiviert werden
- Nicht benötigte Bindungen von Protokollen an (benötigte Netzwerkadapter) sollten deaktiviert werden[10]

In diesem Zusammenhang wird häufig die Frage gestellt, ob IPv6 auf Windows-Systemen aktiviert bleiben (Default-Einstellung) oder deaktiviert[11] werden soll. Die reine Sicherheitsperspektive empfiehlt die Deaktivierung von IPv6 (wg. Reduktion der Angriffsfläche), wenn es nicht benötigt wird und/oder wenn Netzwerkgeräte (Router, Switche, Firewalls) verwendet werden, die (noch) nicht korrekt mit den von IPv6 verwendeten „Transition"-Technologien umgehen können.[12] Auf der anderen Seite gibt es in Windows 7 und in Windows Server 2008 (R2) Komponenten, die IPv6 für die korrekte Funktion benötigen (etwa Direct Access, Remote Assistance, Home Groups...), und es gibt eine *klare* Empfehlung von Microsoft, IPv6 nicht zu deaktivieren.[13] Daher sollte eine Deaktivierung von IPv6 in Windows Vista, Windows 7, Windows Server 2008 und Windows Server 2008 R2 wohlüberlegt und wohlbegründet sein.

- Vergleiche M5.123

[9] Zur Frage der Verwendung einer lokalen Firewall siehe Abschnitt .

10 Das typische, in diesem Zusammenhang bei Client-Systemen genannte Beispiel ist die Datei- und Druckfreigabe für den WLAN-Adapter auf Notebooks von Außendienstmitarbeitern. Bei Windows Servern könnte es etwa ein älteres, nicht mehr benötigtes Netzwerkprotokoll sein (IPX/SPX), das möglicherweise noch an einen Adapter gebunden ist.

11 Wie das geht, entnimmt man http://support.microsoft.com/kb/929852.

12 Oder wenn das hierzu benötigte Know-How noch nicht in der Organisation vorhanden ist.

13 Siehe: http://technet.microsoft.com/en-us/library/2009.07.cableguy.aspx Möglicherweise erlischt gar der offizielle Support, wenn IPv6 deaktiviert wird; siehe dazu: http://technet.microsoft.com/en-us/network/cc987595.aspx.

5 Sichere Konfiguration des Verzeichnisdienstes

5.1 Sicheres Gesamtstrukturdesign

Die grundsätzliche Empfehlung für ein sicheres Design der Gesamtstruktur (Forest) ist recht einfach:

- So wenig Domänen und Forets wie möglich, so viel wie minimal nötig

Aus der Perspektive einer Planung „vom grünen Tisch" bedeutet dies: falls möglich sollte die Gesamtstruktur aus genau einer Domäne bestehen. Die Vorteile eines solchen „Designs" sind:

- im Vergleich zu komplexeren Designs geringster Betriebsaufwand[14]
- einfachste Upgrade-Möglichkeiten und dadurch flexibelstes Design gegenüber zukünftigen Anforderungen
- geringste TCO

Gleichwohl gibt es in der Realität gewachsene Strukturen mit in der Regel mehreren Domänen oder aus Organisationszusammenschlüssen entstandene miteinander verzahnte Gesamtstrukturen. Oder es gibt besondere Anforderungen wie die der administrativen (leeren) Forest-Root-Domäne oder die aufgrund von dedizierten Isolationsanforderungen notwendige Trennung eines Active Directory in zwei lediglich über einen Cross-Forest-Trust mit selektiver Authentifizierung verbundene Gesamtstrukturen[15]. Unabhängig vom Active Directory-Design sollten die nachfolgenden Aspekte als Faktoren einer sicheren Konfiguration des Verzeichnisdienstes beherzigt werden.

- Vergleiche M 2.229

5.2 Höchstmögliche Funktionsebene

Sämtliche in Windows Server 2008 R2-basiertem Active Directory möglichen Sicherheitsfunktionen (wie etwa das „last Logon Timestamp"-Attribut, der mit den um sicherheitsrelevante Funktionen verbesserte Papierkorb, die granulare Passwortrichtlinie oder AES-128-Bit-basierte Verschlüsselung für Kerberos) stehen erst dann zur Verfügung, wenn die Gesamtstruktur in der höchstmöglichen Funktionsebene ausgeführt wird.

- Dies ist die Gesamtstrukturfunktionsebene *Windows Server 2008 R2*.

Die folgende, wegen ihres komprimierten Informationsgehalts zitierte Tabelle *Active Directory Features- Windows Server 2008 R2* aus [1] - [Tabelle von S. 558] listet wichtige Features von Windows Server 2008 R2 unabhängig von einer Funktionsebene sowie abhängig von der Domänen- und von der Gesamtstrukturfunktionsebene:

Active Directory Features- Windows Server 2008 R2
Funktionsebenenunabhängige Merkmale
Install from Media (Replika-Erstellung durch Installation von einem Datenträger)
Zwischenspeicher der universellen Gruppenmitgliedschaft
Anwendungsverzeichnispartitionen, z.B. beim DNS-Server
Active Directory-Quotas (Kontigente für Eigentümer von Objekten)

14 In der ERNW hat sich hierfür die sinnfällige Bezeichnung der "operational feasibility" herausgebildet. Eine Erläuterung dieses Begriffs findet sich auf unserem Blog unter: http://www.insinuator.net/2011/05/evaluating-operational-feasibility/

15 Ein solches Design wird notwendig, wenn nur ausgewählte Identitäten einer Gesamtstruktur auf ausgewählte Ressourcen einer anderen Gesamtstruktur Zugriff erhalten sollen (etwa Mitarbeiter einer unabhängigen Tochtergesellschaft auf ausgewählte Ressourcen der Konzernmutter oder einer anderen Tochtergesellschaft).

Keine vollständige Synchronisation des globalen Katalogs bei Attributänderungen
Schnelles Entfernen eines GC Servers
Single Instance Store zur Speicherung der Sicherheitsbeschreibung
Installierbar als vollständige oder Server Core-Installation
Neustartfähige Active Directory-Domänendienste
Active Directory Database Mounting Tool
Active Directory-Webdienste
Active Directory-Modul für Windows PowerShell
Active Directory-Verwaltungscenter
Active Directory-Best Practices Analyzer
Offline-Domänenbeitritt
Spezifische Merkmale von Domänenfunktionsebenen
Domänencontroller umrennen
Universelle (Sicherheits-)Gruppen mit Verschachtelung
SID-History
Attribut >> last Logon Timestamp <<
Kennwort für inetOrgPerson-Objekte
Andere Standardcontainer als Computers und Users für neue Computer- und Benutzer- Objekte
Eingeschränkte Delegierung
Ausgewählte Authentifizierung
Replikation des System- Volume SYSVOL mittels DFS-R
AES- Algorithmus mit 128 und 256 Bit für Kerberos
Read-Only Domain Controller >> RODC << bzw. schreibgeschützter Domänencontroller
Granulare Kennwortrichtlinien für Benutzer innerhalb einer Domäne
Informationen zur letzten erfolgreichen interaktiven Anmeldung und zu fehlgeschlagenen Anmeldeversuchen
Authentifizierungsmechanismussicherung[16]
Register PERSÖNLICHER VIRTUELER DESKTOP im Eigenschaften- Dialogfeld eines mit dem MMC-Snap-In ACTIVE DIRECTORY- BENUTZER- UND- COMPUTER bearbeiteten Benutzerkontos
Spezifische Merkmale von Gesamtstrukturfunktionsebenen
Linked-Value Replication für Gruppen mit mehr als 5000 Mitgliedern

[16] Beinhaltet die Möglichkeit, Autorisierungen von Benutzern im Active Directory von der Art ihrer Authentifizierung (etwa Zertifikats-basiert) abhänig zu machen. Siehe dazu: http://technet.microsoft.com/de-de/library/dd391847(v=ws.10).aspx

Verbesserter ISTG- Algorithmus bei KCC für die standortübergreifende Replikation
Umbenennung von Domänen
Gesamtstrukturvertrauensstellungen
Dynamische Einträge mit begrenzter Lebensdauer
Deaktivierung sowie Reaktivierung von Objekten und Attributen
Standortinterne Replikation alle 15s
Active Directory-Papierkorb

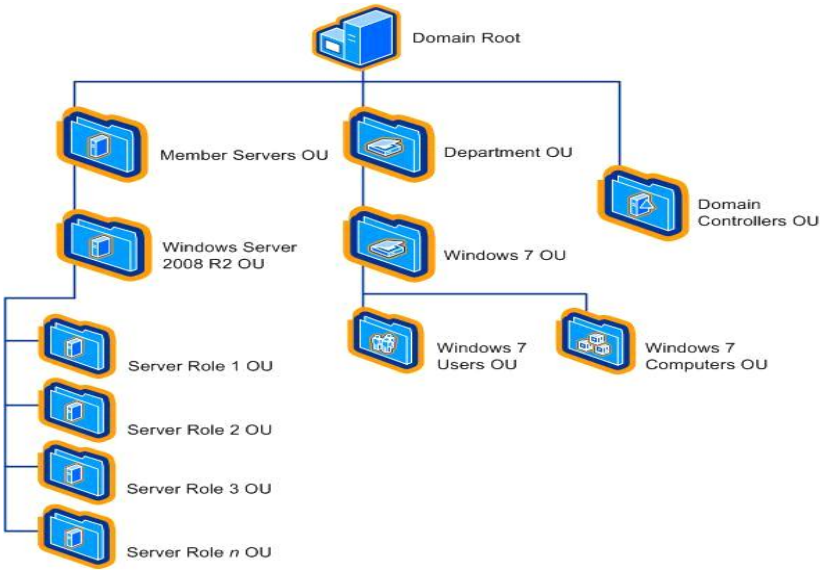
5.3 Sicheres OU-Design

Organisationseinheiten (OUs) werden im Active Directory verwendet, um Ressourcen zu strukturieren, damit Gruppenrichtlinien (GPOs) auf geeignete Weise mit den OUs verknüpft werden können und auf die in den OUs enthaltenen Benutzer- und Computer-Identitäten wirken (= ihnen Konfigurationseinstellungen zuordnen).

Grundsätzlich gilt:

- Das OU-Design so flach wie möglich (wenn möglich zweistufig) gehalten, um die Administration einfach und übersichtlich zu gestalten.

Eine flache und übersichtliche Struktur für das OU-Design, die sich im Wesentlichen auch das BSI aneignet, bietet der *Windows Server 2008 R2 SP1 Security Guide* [4] – [Grafik von S. 26].



Unterhalb der Domäne finden sich die unterschiedlichen manuell erstellen OUs[17]:

- für Serverrollen
- für Abteilungen
- für Client-Computer
- für Benutzer

[17] Lediglich die OU "Domain Controllers" ist bereits vordefiniert. In diese OU werden Domänencontroller (DCs) bei ihrer Erstellung verschoben. Grundsätzlich sollte diese OU weder umbenannt noch verschoben werden. Darüber hinaus sollten DCs in dieser OU verbleiben, da sie über das mit ihr verknüpfte Default Domain Controller GPO DC-spezifische Einstellungen erhalten.

Je nach Größe der Organisation kann es noch sinnvoll sein, OUs für besondere Clientrollen (Außendienstcomputer, VIP-Computer) zu definieren. Das OU-Design sollte darüber hinaus sauber (präzise und aktuell) dokumentiert sein.

- Vergleiche auch M 2.229

5.4 Sicherheit durch Gruppenrichtlinien (GPOs)

Gruppenrichtlinien (GPOs) gestatten eine hierarchische und zentralisierte Verwaltung von Benutzer- und Computer-Objekten im Active Directory. Im Zusammenhang dieses Dokuments ist vor allem wichtig, dass Sicherheits-spezifische Einstellungen über GPOs gezielt an definierte Benutzer und Computer im Active Directory verteilt werden können.

5.4.1 Grundsätzliches zum GPO-Design

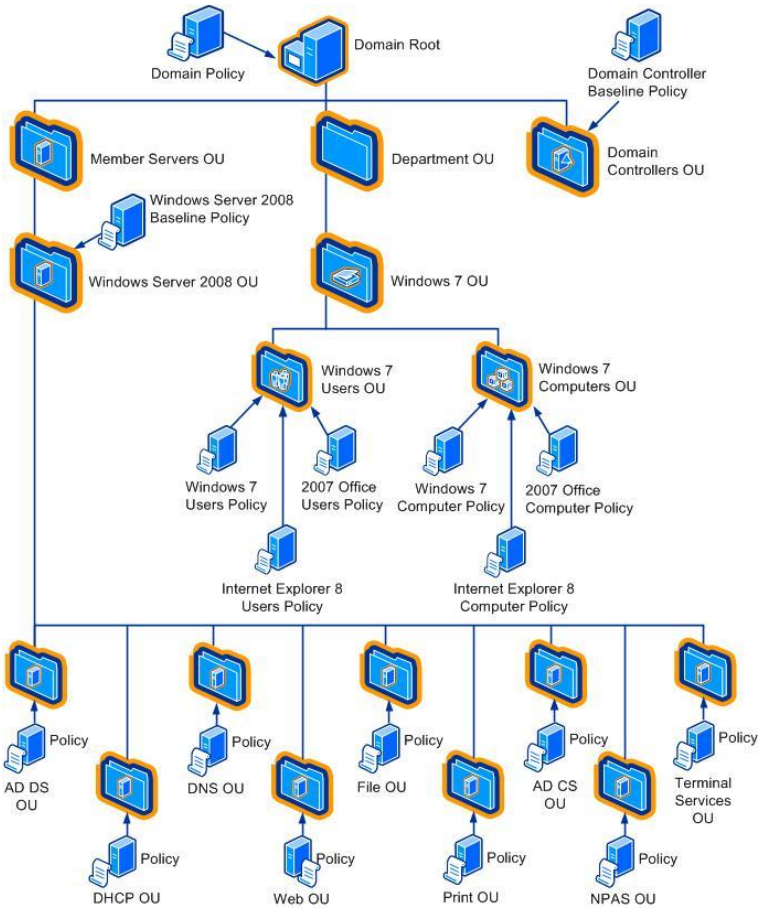
Die Anzahl der GPOs und ihrer Verknüpfungen sollte gemäß Empfehlungen von Microsoft aus dem „*Windows Server 2008 R2 SP1 Security Guide*[18]"[4] und Empfehlungen des BSI aus dem Baustein M 2.231 („Planung der der Gruppenrichtlinien unter Windows") so gering wie nötig gehalten werden.[19] Gemäß den Empfehlungen von Microsoft (auf die sich das BSI in M 4.283 beruft) wird eine effektive Administration der GPOs wie folgt erreicht (gleichzeitig werden die vom BSI explizit unerwünschten Mehrfachüberdeckungen vermieden):

- Windows Server 2008 (R2)-basierte Member Server erhalten eine „Baseline Security Policy", in der Basis-Sicherheitseinstellungen stehen, die für sämtliche 2008 (R2)-basierten Member Server gelten. Analoges gilt für Client-PCs
- Jede spezifische Serverrolle erhält ein eigenes GPO mit den dort verorteten und spezifisch für diese Rolle gültigen Einstellungen. Mögliche Rollen müssen sich nicht nur nach Windows Serverrollen (im Sinne der Microsoft-Definition) richten, sondern es können OUs (und dann damit verknüpfte GPOs) auch nach Funktionen erzeugt werden (etwa Backup-Server, SCOM-Server, WSUS-Server, Citrix-Server etc.). Denn häufig bietet Zusatzsoftware Integration mit Gruppenrichtlinien (SCOM, SCCM, WSUS, aber auch Drittherstellersoftware wie etwa Citrix).
- Wenn eine geforderte Sicherheitseinstellung dem Default-Wert des Betriebssystems entspricht, wird sie so belassen, wie sie ist, und in dem GPO belassen, in dem sich diese Einstellung befindet.
- Wenn eine geforderte Sicherheitseinstellung von dem Default-Wert abweicht, wird sie in dem GPO „Basis-Sicherheitseinstellungen" vorgenommen.
- Default Domain Policy und Default Domain Controllers Policy bleiben gemäß Best Practices bis auf die Passwort- und die Überwachungsrichtlinie (beide Einstellungen werden in der Default Domain Policy vorgenommen) unangetastet. Auf Domänen- und Domänencontroller-Ebene notwendige zusätzliche Einstellungen werden in zusätzlich zu definierenden GPOs vorgenommen.
- Für die weitere Einschränkung bestimmter Komponenten (Internet Explorer, Office, etc.) sollten eigene GPOs definiert und an der geeigneten Stelle mit einer OU verknüpft werden.

Unter Berücksichtigung der genannten Aspekte ergibt sich der folgende grundsätzliche Entwurf für ein im Sinne des BSI (und auch im Sinne von Microsoft) sichere GPO-Design [4]:

[18] Windows Server 2008 R2 Security Baseline: http://technet.microsoft.com/library/gg236605.aspx

[19] Dabei ist ein zwecks sicherer und effektiver Administration immer ein Kompromiss bei der Anzahl der zu definierenden GPOs zu finden: Ein einziges GPO lässt sich sowohl wegen der unterschiedlichen Einstellungen für verschiedene Server (etwa Domänencontroller und Server) als auch wegen zu hohem Informationsgehalt nicht realisieren; zu viele GPOs führen zu Unübersichtlichkeit (und haben weitere administrative und ‚technische Nebenwirkungen'). Daher empfiehlt es sich zum einen, ähnliche Einstellungen (etwa Basis-Sicherheitseinstellungen) in einem GPO zusammen zu fassen, zum anderen besonders prägnante oder folgenschwere Einstellungen (etwa ‚Firewall global ein oder aus' oder ‚Ping-Antwort global ein oder aus') in separaten mit einem sprechenden Namen versehenen GPOs vorzunehmen.



- Maßnahme ist konform zu M 2.231 und M 4.283

5.5 (Verwaltete) Dienstkonten

Dienstkonten erfüllen im IT-Betrieb eine wichtige Rolle. Bei der Definition von Dienstkonten sind häufig die beiden folgenden sicherheitsrelevanten Anforderungen zu bewältigen:

- Möglichst niedrige Privilegien: ein Dienst soll nur mit den von ihm benötigten Privilegien laufen

Dieses Problem wurde in der Vergangenheit häufig und vollkommen unzureichend dadurch gelöst, dass das Dienstkonto im Active Directory zum Mitglied einer möglichst hoch privilegierten Benutzergruppe (etwa der Domänen-Admins) gemacht wurde. Oder dadurch, dass der Hersteller der Software den Dienst unter dem Konto *Local System* laufen ließ.

- Regelmäßige Passwortwechsel gemäß Passwort-Policy: auch für ein Dienstkonto sollte die Passwort-Policy gelten

Dieses Problem wurde in der Vergangenheit häufig ebenso unvollkommen gelöst und zwar dadurch, dass für das Dienstkonto ein Passwort vergeben wurde, das nie wieder geändert wurde.

Es gilt daher die folgende Empfehlung: Mit den sog. verwalteten Dienstkonten (MSA für Managed Service Account), die auf Windows Server 2008 R2 (und Windows 7) -basierten Systemen im Active Directory (unabhängig von der Funktionsebene) zur Verfügung stehen, können beide Anforderungen erfüllt werden.[20]

- Dienste sollten daher wenn möglich *immer* als verwaltete Dienstkonten konfiguriert werden.[21]

- Vergleiche M4.x-8 in [6]

[20] Technisch wird dies dadurch realisiert, dass ein MSA ein Konto vom Typ „Computer" ist. Dadurch wird eine automatisierte Erfüllung der Passwort-Policy möglich. Darüber ermöglicht die Verwendung eines Dienstes für ein solches Konto sowohl die Isolation des Dienstes von anderen Diensten als auch eine möglichst niedrige Privilegienstufe.

[21] Der Autor hat dies in der Umgebung, die diesem Newsletter zugrunde liegt, erfolgreich und ohne weitere Schwierigkeiten für eine weitverbreitete Backup-Software durchgeführt.

5.6 Zeitsynchronisation

Die Zeitsynchronisation ist eine elementare Funktions- und Sicherheitsanforderung an den Betrieb des Active Directory.

- Funktionsanforderung:
  - Domänencontroller replizieren nicht mehr, wenn die Zeit zwischen ihnen mehrere Minuten differiert.
  - Clients können sich nicht anmelden, wenn ihre Zeit zu der des Domänencontrollers mehrere Minuten differiert.
- Sicherheitsanforderung:
  - Ereignisse aus Protokollen verschiedener Systeme können nicht oder nur unzureichend korreliert werden, wenn ihre Zeiten differieren

- Vergleiche M4.227

Jedes System sollte deshalb die eigene Systemzeit in regelmäßigen Abständen mit einem unabhängigen Zeitgeber abgleichen. Für die Zeitsynchronisation im Active Directory gilt:

- Der Zeitgeber für Mitgliedsrechner der Domäne ist der Domänencontroller, über den die Anmeldung am Active Directory erfolgt
- Der Zeitgeber aller Domänencontroller außer dem PDC-Emulator ist der PDC-Emulator der Domäne
- Für PDC-Emulator einer untergeordneten Domäne fungiert den PDC-Emulatur der übergeordneten Domäne als Zeitgeber
- Die letzte Instanz in einer Gesamtstruktur ist der PDC-Emulatur der Forest-Root-Domäne

Als Zeitgeber für ihn könnten z.B. die Atomuhr-basierten Zeitserver der Physikalisch-Technischen Bundesanstalt (PTB) dienen. Die DNS-Namen der PTB Zeitserver lauten:[22]

- ptbtime1.ptb.de
- ptbtime2.ptb.de
- ptbtime3.ptb.de

Zum Einrichten der ersten beiden Zeitserver der PTB im Active Directory muss am PDC-Emulator folgender Befehl eingegeben werden:

w32tm /config /manualpeerlist:ptbtime1.ptb.de,ptbtime2.ptb.de /Syncfromflags:manual /reliable:yes /update

[22] Siehe: http://www.ptb.de/de/org/q/q4/q42/_ntp_main.htm

6 SICHERE ADMINISTRATION

6.1 Minimale Berechtigungen für Administratoren durch aktivierte Benutzerkontensteuerung

Die Benutzerkontensteuerung (oder auch User Account Control[23], kurz „UAC") ist eine immer noch kontrovers diskutierte Sicherheitsfunktionalität von Windows-Betriebssystemen seit Windows Vista. Zusammen mit der Benutzerkontensteuerung implementierte Microsoft mit Windows Vista eine bestimmte Form von Multilevel Security, die eine grundsätzliche neue Sicherheitsarchitektur der Windows-Betriebssysteme einläutete. Das dahinter stehende Modell wird als „Mandatory Integrity Control (MIC)", manchmal auch als „Windows Integrity Control (WIC)" bezeichnet.[24] Mit aktivierter Benutzerkontensteuerung sind gleichzeitig diese Integritätsmechanismen aktiv. Die Benutzerkontensteuerung soll dafür sorgetragen, dass Benutzer (auch Administratoren) stets mit minimalen Privilegien (landläufig auch als „Berechtigungen" bezeichnet) arbeiten. Gewährleistet wird dies dadurch, dass bei der Anmeldung eines Administrators nicht nur das übliche vollständige Access-Token erzeugt wird, sondern zusätzlich ein weiteres, gefiltertes Access-Token. Dieses ist in Bezug auf die gewährten Privilegien mit dem Access-Token eines Standart-Benutzers identisch. Der Administrator arbeitet bei aktivierter Benutzerkontensteuerung mit dem gefilterten Token und damit mit den Privilegien eines Standard-Benutzers. Erst dann, wenn er höhere Privilegien benötigt (z. B. für den Aufruf der Datenträgerverwaltung oder eines anderen administrativen Werkzeugs), gewährt ihm die Benutzerkontensteuerung diese. Dabei ist der Prozess der Privilegien-Gewährleistung abhängig von der Detaillkonfiguration der Benutzerkontensteuerung: sie reicht von einer „stummen" Gewährung ohne weitere Nachfrage bis hin zur Aufforderung zur Passworteingabe vor der Gewährung der erhöhten Privilegien. Während die Aktivierung der Benutzerkontensteuerung auf Server-Systemen heute nicht mehr ernsthaft in Frage gestellt wird[25], gibt es bei der Detaillkonfiguration an bestimmten Punkten durchaus noch Diskussionsbedarf. Daher werden die Detailkonfigurationen im Folgenden kurz vorgestellt und mit Empfehlungen versehen:

Grundsätzlich gilt:

- Die Benutzerkontensteuerung sollte auf allen Server-Systemen aktiviert sein.

Für die Detailkonfiguration der Benutzerkontensteuerung gelten die folgenden Empfehlungen:

- Einstellung: *Benutzerkontensteuerung: Administratorbestätigungsmodus für das eingebaute Administratorkonto*
  Beschreibung: Diese Einstellung definiert, ob die Benutzerkontensteuerung auch auf das standardmäßige integrierte Administratorkonto angewendet wird.
  Grundsätzliche Empfehlung: **Aktiviert**
  Diskussion: Während der Installation und Basis-Konfiguration des Server-Systems in einer abgetrennten Umgebung kann diese Richtlinie (vorübergehend) deaktiviert werden. Nach Durchführung der Treiber-Installation und Basis-Konfiguration des Systems, sollte die Richtlinie wieder aktiviert werden.

- Einstellung: *Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen*
  Beschreibung: Dieser Parameter bestimmt, dass auf alle Benutzer, die Mitglieder der Administratorgruppe sind, die Benutzerkontensteuerung angewendet wird.
  Grundsätzliche Empfehlung: **Aktiviert**
  Diskussion: Über diese Einstellung wird die Benutzerkontensteuerung und es werden die zu ihr gehörenden Sicherheitsmechanismen aktiviert oder deaktiviert. Die Benutzerkontensteuerung sollte grundsätzlich aktiviert sein.
- Maßnahme ist konform zu M4.340

23 Siehe dazu: Inside Windows 7 User Account Control http://technet.microsoft.com/en-us/magazine/2009.07.uac.aspx

24 Eine immer noch aktuelle Beschreibung und Diskussion von MIC hat der Autor in diesem ERNW-Newsletter veröffentlicht: Newsletter 17 / Juli 2007 "Mandatory Integrity Control", http://www.ernw.de/content/e15/e28/index_ger.html [7].

25 Für Clients gilt dies (leider) nicht so eindeutig. Die aktivierte Benutzerkontensteuerung durchläuft in größeren Organisationen wegen ihrer Auswirkungen auf ältere Software oder auf gewachsene Strukturen (Benutzer arbeiten mit administrativen Privilegien) häufig einen schwierigen Implementierungsprozess.

- Einstellung: *Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern*
  Beschreibung: Die Richtlinie steuert, ob das System Heuristik verwendet, um Anwendungsinstallationspakete zu erkennen, für die möglicherweise Rechteerweiterungen notwendig sind. Führt ein Benutzer eine Installationsanwendung aus, die vom System als eine erkannt wird, die administrative Privilegien benötigt, wird der Benutzer aufgefordert seine Administrativen Rechte nachzuweisen.
  Grundsätzliche Empfehlung: **Aktiviert**

- Einstellung: *Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln*
  Beschreibung: Diese Einstellung bestimmt, dass alle Anhebungsaufforderungen entweder auf dem sog. „sicheren Desktop" angezeigt werden.
  Grundsätzliche Empfehlung: **Aktiviert**
  Diskussion: In den Anfängen der Benutzerkontensteuerung, konnte der abgedunkelte „sichere" Desktop möglicherweise noch für etwas Verwirrung sorgen, heute sollte er das nicht mehr tun. Durch diese Einstellung wird außerdem sichergestellt, dass keine weitere Anwendung gleichzeitig auf den Desktop zugreifen (und etwa durch einen verdeckten Mausklick die Privilegienerhöhung bewirken) kann.

- Einstellung: *Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerspeicherorte virtualisieren*
  Beschreibung: Diese Richtlinie steuert, ob durch MIC oder NTFS-Berechtigungen geschützte Orte, auf die die Anwendung lesend oder schreibend zugreifen möchte, an (durch die Benutzerkontensteuerung) virtualisierte Orte in der Registry und ins Dateisystem umgeleitet werden. Dadurch sollen die Auswirkungen von Anwendungen, die unter einem hoch privilegierten Benutzer ausgeführt werden und Laufzeitanwendungsdaten in *ProgramFiles%, %Windir%, %Windir%|system32* oder *HKLM|Software* schreiben verringert werden [3].
  Grundsätzliche Empfehlung: **Aktiviert**

- Einstellung: *Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind*
  Beschreibung: Dies Sicherheitseinstellung steuert, ob UIAccess- Anwendungen, welche sich nicht an besonders geschützten Speicherorten befinden ausgeführt werden dürfen. UIAccess- Anwendungen werden unabhängig vom Status dieser Richtlinie immer einer Signaturprüfung unterzogen.
  Besonders geschützte Speicherorte sind:
  - ...\Programme\, einschließlich Unterverzeichnissen
  - ...\Windows\system32
  - ...\Programme (x86)\, einschließlich Unterverzeichnissen für 64-Bit-Versionen

  Grundsätzliche Empfehlung: **Aktiviert**

- Einstellung: *Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind*
  Beschreibung: Dieser Parameter definiert, ob das System eine Signaturüberprüfung durchführt, bevor eine Anwendung angehoben werden kann. Die Anwendung wird erst gestartet, wenn die Validierung der Signatur erfolgreich war. Das heißt:
  - die (herauf zu stufende) Anwendung wird nicht startet, wenn sie nicht signiert ist (es kommt zu einer kryptischen Fehlermeldung[26])

[26] Die Fehlermeldung lautet in der Regel: „ShellExecuteEx failed; code 8235. A referral was returned from the server" und gibt keinen direkten Aufschluss auf die Ursache. Administratoren sollten dies bei der Aktivierung der Richtlinie im Hinterkopf behalten.

- die (herauf zu stufende) Anwendung wird nicht startet, wenn die Signatur als ungültig validiert wird (es kommt zu einer kryptischen Fehlermeldung)

Grundsätzliche Empfehlung: **Aktiviert**

Diskussion: Diese Einstellung ist per Default deaktiviert, nach erfolgter Installation des Server-Systems sollte sie jedoch aktiviert werden. Die Einstellung bietet einen starken Schutz gegen „Privilege Escalation" (nicht autorisierte Privilegienerhöhung) von Malware.[27]

- Einstellung: *Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern*
  Beschreibung: Diese Einstellung definiert, ob UIAccess- Anwendungen ihr Integritätsebene im Hintergrund, ohne Eingabeaufforderung verlassen dürfen.
  Grundsätzliche Empfehlung: **Deaktiviert**

- Einstellung: *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus*
  Beschreibung: Diese Einstellung bestimmt, wie die Benutzerkontensteuerung Administratoren zur Rechte Erhöhung auffordert.
  Grundsätzliche Empfehlung: **Eingabeaufforderung zur Zustimmung auf dem sicheren Desktop**
  Diskussion: Auch diese Einstellung sollte nach der Installation (und Grundkonfiguration) des Server-Systems vorgenommen werden. Die Erhöhung ohne Bestätigung stellt ein unnötiges Sicherheitsrisiko dar; die Aufforderung zur Passworteingabe erhöht den Betriebsaufwand dagegen unnötig.

- Einstellung: *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer*
  Beschreibung: Diese Einstellung definiert, wie und ob die Benutzerkontensteuerung Standardbenutzer zur Rechte Erhöhung auffordert.
  Grundsätzliche Empfehlung: **Anforderung für erhöhte Rechte automatisch ablehnen**
- Maßnahme ist konform zu M4.340

6.2 Sicheres Management

Die Administration von Windows Server 2008 R2 soll auf sichere Art und Weise erfolgen. Das umfasst den Einsatz sicherer (verschlüsselter) Verfahren/Protokolle, personalisierter Accounts, die Restriktion der Anzahl der Benutzer mit administrativen Privilegien und ggf. die Restriktion der Administration auf eine eigenes Admin-LAN[28].

- Vergleiche: M 2.364, M2.370

[27] Es gibt bisher wenig signierte Malware; und selbst wenn diese signiert ist, muss die Signatur auch noch als gültig vom Betriebssystem validiert werden, bevor die Heraufstufung erfolgt. Dies zu verhindern ist Aufgabe eines korrekten Zertifikatsmanagements.

[28] Das Thema Admin-LAN ist nicht Bestandteil dieses Dokuments.

6.2.1 Minimale Anzahl von administrativen Benutzern auf dem System

Die Anzahl der Benutzer mit administrativen Berechtigungen sollte auf ein Minimum beschränkt sein. Die Benutzerberechtigungen sollten gemäß dem Least Privilege-Prinzip vergeben werden, d.h. Benutzer sollen nur über die Berechtigungen verfügen, die zur Durchführung der ihnen zugedachten Aufgaben notwendig sind und auch nur in dem Zeitraum, in dem sie diese Berechtigungen benötigen.

- Vergleiche: M 2.364, M2.370

6.2.2 Anmeldung am System auf administrative Benutzer beschränkt

Nur Mitglieder administrativer Gruppen dürfen sich lokal am System anmelden.[29]

- Vergleiche: M 2.364, M2.370

6.2.3 Personalisierung von administrativen Konten

Jedes Konto mit administrativen Berechtigungen muss personalisiert sein (außer natürlich das Konto des vordefinierten Administrators).

- Vergleiche: M 2.364, M2.370

6.2.4 Überwachung der Mitgliedschaft in administrativen Gruppen

Im Active Directory gibt es wegen ihrer umfassenden Privilegien vier besonders sicherheitskritische Gruppen: „Organisations-Admins", „Schema-Admins", „Domänen-Adminis" und die Gruppe der „lokalen Adminstratoren" auf den Domänencontrollern. Über das GPO „Eingeschränkte Gruppen" sollten diese vier Gruppen als eingeschränkte Gruppen definiert werden.

Mithilfe der Richtlinie *Eingeschränkte Gruppen* können die Gruppenmitgliedschaft gesteuert und überwacht werden.

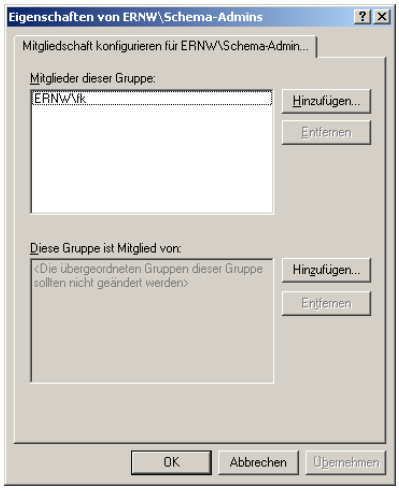
Diese Sicherheitseinstellung ermöglicht Administratoren die Definition von zwei Eigenschaften für sicherheitssensitive Gruppen und ihre Mitglieder:

- Die Liste *Mitglieder* definiert, wer zur eingeschränkten Gruppe gehört und wer nicht.
- Die Liste *Mitglied von* definiert, die Gruppenzugehörigkeit der eingeschränkten Gruppe.

Wird eine Richtlinie für *Eingeschränkte Gruppen* erzwungen, werden alle aktuellen Mitglieder einer eingeschränkten Gruppe, die nicht in der Liste *Mitglieder* aufgeführt sind, entfernt. Alle in der Liste *Mitglieder* aufgeführten Benutzer, die momentan kein Mitglied der eingeschränkten Gruppe sind, werden hinzugefügt.

(Screenshot nächste Seite)

[29] In der jeweiligen Umgebung verwendete administrative Gruppen sollten hier definiert werden; mindestens jedoch die Gruppen der lokalen Administratoren und der Domänen-Admins (vgl. Abschnitt 6.2.4).



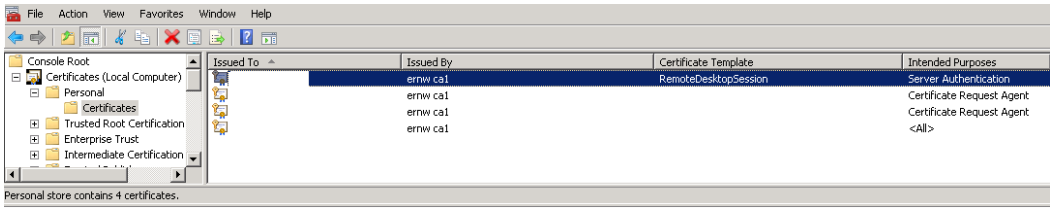
Beispiel: Überwachung der Mitgliedschaft in der Gruppe der Schema-Admins.

6.2.5 Remotezugriff

Die Remote-Administration des Systems sollte über sicheres Netzwerkprotokoll erfolgen. In Windows-Umgebungen bietet sich dazu das *„Remote Desktop Protocol* (RDP)" an. Damit die Anforderungen an Integrität und Authentizität der Verbindung erfüllt werden können, sollte RDP in der Version 6 oder höher eingesetzt werden.

RDP in der Version 6 oder höher verwendet zur Serverauthentifizierung *„Transport Layer Security (TLS)"* (in der Version 1.0). Dadurch wird nicht nur die Integrität der Daten während der Übertragung, sondern auch die Authentizität der Kommunikationspartner gewährleistet.[30] Die Serverauthentifizierung beruht dabei auf X.509-Zertifikaten. Theoretisch können dabei (vom Server) selbst signierte Zertifikate verwendet werden; dies wird jedoch nicht empfohlen. Empfohlen wird der Einsatz eines Zertifikats, das von einer vertrauenswürdigen Root-CA ausgestellt wurde. Das impliziert:

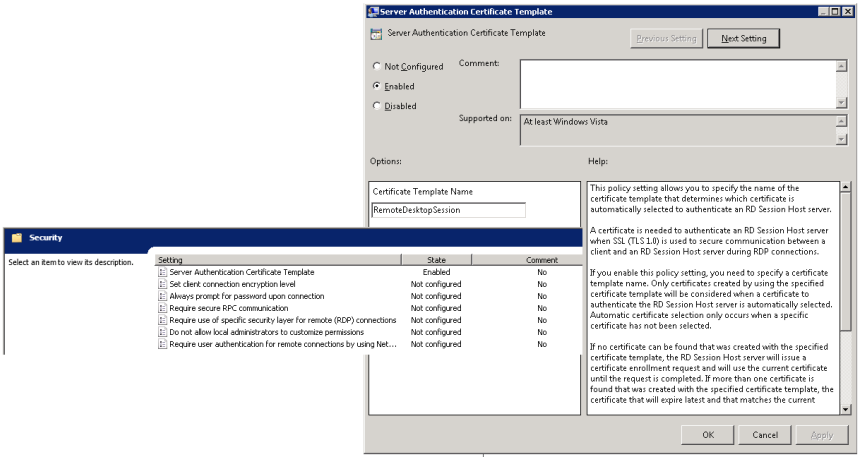
- Die Definition einer vertrauenswürdigen (Root-) CA[31] und die Aufnahme ihres Zertifikats in den Speicher für vertrauenswürdigen Stammzertifizierungsstellen.
- Die Implementierung des speziell für die RDP-Sitzung ausgestellten Serverzertifikats (nachfolgender Screenshot):



- Und es impliziert die Konfiguration eines GPO, dieses Zertifikat auch zu verwenden (in: Computerkonfiguration \Richtlinien\Administrative Vorlagen\WindowsKomponenten\Remotedesktopdienste\Remotedesktop-Sitzungshost \Sicherheit\ Zertifikatvorlage für Serverauthentifizierung). Siehe nächste Seite:

[30] TLS ist eine Weiterentwicklung des SSL-Protokolls. Der wesentliche Unterschied liegt darin, dass TLS einen „Keyed-Hashing for Message Authentication (HMAC)"-Algorithmus einsetzt, bei dem die Konstruktion der Hashfunktion wesentlich verbessert wurde und somit die Entschlüsselung erschwert.

[31] Diese kann sich innerhalb oder außerhalb des Unternehmens befinden. Die jeweiligen Betriebsprozesse sind dabei zu berücksichtigen.


Server Authentication Certificate Template
Server Authentication Certificate Template
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
Certificate Template Name
RemoteDesktopSession
This policy setting allows you to specify the name of the certificate template that determines which certificate is automatically selected to authenticate an RD Session Host server.
A certificate is needed to authenticate an RD Session Host server when SSL (TLS 1.0) is used to secure communication between a client and an RD Session Host server during RDP connections.
If you enable this policy setting, you need to specify a certificate template name. Only certificates created by using the specified certificate template will be considered when a certificate to authenticate the RD Session Host server is automatically selected. Automatic certificate selection only occurs when a specific certificate has not been selected.
If no certificate can be found that was created with the specified certificate template, the RD Session Host server will issue a certificate enrollment request and will use the current certificate until the request is completed. If more than one certificate is found that was created with the specified certificate template, the certificate that will expire latest and that matches the current
OK
Cancel
Apply
Security
Select an item to view its description.
Setting
State
Comment
Server Authentication Certificate Template
Enabled
No
Set client connection encryption level
Not configured
No
Always prompt for password upon connection
Not configured
No
Require secure RPC communication
Not configured
No
Require use of specific security layer for remote (RDP) connections
Not configured
No
Do not allow local administrators to customize permissions
Not configured
No
Require user authentication for remote connections by using Net...
Not configured
No

7 Integritätsschutz für das Betriebssystem und verarbeitete Daten

Windows Server 2008 R2 implementiert einen Integritätsschutz im Betriebssystem[32]. Der Integritätsschutz gilt für das Betriebssystem und die im Dateisystem des Servers gespeicherten Daten.

- Vergleiche: M 4.341

7.1 Aktivierte Benutzerkontensteuerung

Die Benutzerkontensteuerung dient nicht nur der sicheren Administration, sondern setzt Multi Level Security für alle Benutzer des Systems um. Die Benutzerkontensteuerung sollte dringend aktiviert bleiben (Default-Einstellung des Betriebssystems) und mit den bereits diskutierten Einstellungen konfiguriert werden. Siehe dazu Abschnitt 6.1.

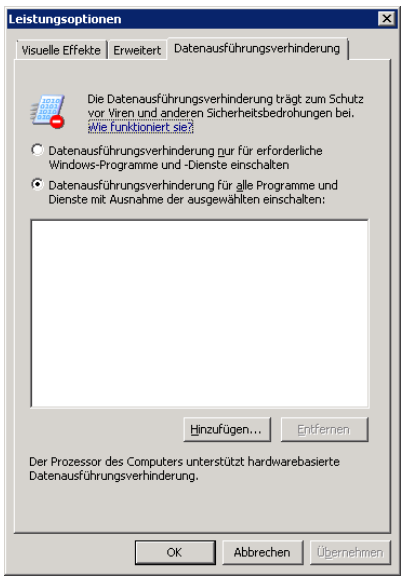
7.2 Ausschließlich NTFS als Dateisystem

Alle Partitionen des Servers sollten mit dem NTFS-Dateisystem formatiert sein.

- Vergleiche: M 4.280

7.3 Aktivierte Datenausführungsverhinderung

Die Datenausführungsverhinderung (Data Execution Prevention (DEP)) unterstützt die Integrität von Daten im RAM des Systems. Die Datenausführungsverhinderung sollte ausnahmslos für alle installierten Programme und Dienste aktiviert werden (Default-Einstellung des Betriebssystems). Auf aktuellen Systemen lässt sich Hardware-unterstütztes DEP häufig im System-BIOS aktivieren. Wenn dies möglich ist, dann sollte dies auch umgesetzt werden.



[32] Microsoft bezeichnet diesen Schutz als Mandatory Integrity Control (MIC). Dieser Schutz steht in den Microsoft-Betriebssystemversionen ab Windows Vista zur Verfügung, siehe auch [7].

9 VULNERABILITY MANAGEMENT

9.1 Patchmanagement

Da immer noch die meisten Angriffe/Malware-Infektionen auf fehlerhaften Software-Komponenten basieren, kommt dem Patchlevel eines Systems eine sehr hohe Bedeutung für die Gesamtsicherheit zu. Um den Schutz des Betriebssystems vor Malware sicherzustellen, empfiehlt es sich, den Softwarestand (Patchlevel) des Betriebssystems möglichst aktuell zu halten.

In diesem Zusammenhang sollte es einen definierten und implementierten Patchmanagement-Prozess geben, der dafür Sorge trägt, dass Updates innerhalb eines definierten[33] Zeitraums überprüft und bereitgestellt werden.

Grundsätzliche Phasen des Patchmanagement-Prozesses können sein (hier in Anlehnung an Empfehlungen von Microsoft):

- Prüfen und Planen: Während der Prüfungs- und Planungsphase muss entschieden werden, ob das Softwareupdate bereitgestellt werden soll und wie die großflächige Verteilung zu erfolgen hat. Außerdem sollte das Softwareupdate in einer produktionsähnlichen Umgebung (etwa der „QS-Umgebung") getestet werden, um sicherzugehen, dass keine geschäftskritischen Systeme und Anwendungen gefährdet werden. Die auf die Produktionssysteme aufzuspielenden Patche durchlaufen einen Genehmigungsprozess.
- Bereitstellen: Ziel ist hier die erfolgreiche Durchführung der Verteilung von genehmigten Patches in der Produktionsumgebung. Anforderungen an die Bereitstellungs-SLAs (Service Level Agreements, Dienstvereinbarungen), die sich vor Ort befinden, sollten dabei beachtet und erfüllt werden.

- Vergleiche: M 2.273

9.2 AV-Software

Jeder Windows Server 2008 R2 sollte über Antivirus-Software mit tagesaktuellen Virensignaturen verfügen. Hierzu muss ein Verwaltungsprozess vergleichbar dem Patchmanagement-Prozess definiert, implementiert und gelebt werden.

- Maßnahme ist konform zu M4.3

Die Auswahl des richtigen Produkts spielt eine wichtige Rolle für den Schutz vor Malware-Infektion. Da die ERNW ein unabhängiges Prüf- und Beratungsinstitut ist, werden an dieser Stelle keine Produktempfehlungen gegeben, sondern es wird auf einschlägige Benchmarks aus einschlägigen Quellen verwiesen. Grundsätzlich kann jedoch gesagt werden, dass in Organisationen häufig zwei verschiedene Produkte eingesetzt werden, und zwar:

- eine Lösung für Server.
- eine Lösung für Clients.

Dadurch können die Scan-Ergebnisse in der Erkennungsrate in der Regel verbessert werden.[34]

- Vergleiche: M 2.157

33 Wie groß dieser „definierte" Zeitraum ist, hängt von der Umgebung der Organisation ab. In großen Organisationen ist eine Zeitverzögerung von sechs bis acht Wochen (ggf. mit Sonderverfahren für hochkritische Systeme in der DMZ) nach Erscheinen des Patches vertretbar.

34 Die Verwendung von unterschiedlichen Produkten kann sich u. U. erübrigen, wenn ein Produkt unterschiedliche Scan-Engines gleichzeitig einsetzt.

9.3 Lokale Firewall aktiviert

Die Windows Firewall erlaubt die Filterung sowohl ein- als auch ausgehenden Netzwerkverkehrs auf Basis definierter Regeln und Einstellungen. Bei der in Windows Server 2008 (R2) integrierten Firewall handelt es sich um eine sog. Stateful Inspection Firewall, die eine sehr granulare Filterung gestattet. In der Standard Einstellung werden alle eingehenden Verbindungen geblockt. Diese Einstellung sollte auf allen Systemen beibehalten werden. Unter Umständen müssen – wie die Erfahrung gezeigt hat – für Zusatzsoftware (nicht nur von Drittherstellern, sondern auch von Microsoft) manuell Firewallregeln erstellt werden (etwa für den SCOM-Server oder den Backup-Server), die dann per Gruppenrichtlinie an die betroffenen Systeme verteilt werden können. Darüber hinaus empfiehlt es sich, ein GPO anzulegen, in dem die Firewall (zu Troubleshooting-Zwecken) global ausgeschaltet werden kann. Und es empfiehlt sich die Anlage eines weiteren GPOs, das PING-Echo-Antworten in der gesamten Domäne gestattet.[35]

Auf die Filterung von ausgehendem Netzwerkverkehr durch die lokale Firewall sollte verzichtet werden. Sie ist per Default deaktiviert und sollte es auch bleiben (nach Ansicht des Autors würde eine solche Maßnahme auf Windows Servern unter die Kategorie „Security Theatre" fallen).

- Vergleiche: M 4.280, M 4.x-2

9.4 Einsatz von Enhanced Mitigation Experience Toolkit (EMET)

Das Enhanced Mitigation Experience Toolkit (EMET) ist ein kostenloses Softwareprodukt von Microsoft und enthält eine Reihe Speicherschutzmechanismen wie „Data Execution Prevention"(DEP), „Mandatory Address Space Layout Randomization"(ASLR) und weitere Technologien.[36]. Diese Sicherheitstechnologien sollen dabei helfen, dass eine Software-Schwachstelle von Malware möglichst nicht ausgenutzt werden kann. Die genannten Technologien bewirken, dass die Ausnutzung der Schwachstelle unter Umständen erheblich erschwert wird. ERNW hat im eigenen LAB die Effizienz von EMET als Schutz vor sog. 0-Day-Exploits (Exploits für Schwachstellen, für die es keinen Patch gibt oder für die sich ein Patch nicht anwenden lässt) überprüfen können.

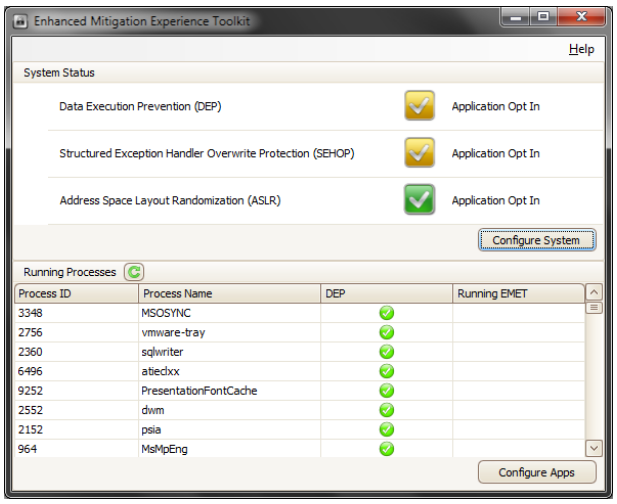
Organisationen stellen sich nun die Frage, ob mit dem Einsatz von EMET zusätzliche Geschäftsrisiken (etwa Inkompatibilität zu Anwendungsprogrammen) verbunden sind? Dies lässt sich grundsätzlich wie folgt beantworten:

- Der Einsatz von EMET auf Windows Servern ist grundsätzlich zu empfehlen. Dies betrifft besonders Systeme die ein erhöhtes Angriffspotential besitzen (Systeme in der DMZ, dort etwa IIS, Exchange, BES (BlackBerry Enterprise Server, ältere Windows-Betriebssystemversionen)
- Die durch EMET bereitgestellten Sicherheitstechnologien können zu Anwendungsinkompatibilitäten führen. Denn einige (unsauber programmierte) Anwendungen beruhen exakt auf dem Verhalten, das durch diese Schutzmechanismen unterbunden werden soll. Deshalb sollten Anwendungen, die nicht durch Microsoft oder einer andere validen Quelle freigegeben wurden, einem intensiven Funktionstest unterworfen werden, bevor sie in der Produktiv-Umgebung zusammen mit EMET zum Einsatz kommen. EMET kann so konfiguriert werden, dass es Anwendungen, die nicht kompatibel zu EMET sind, nicht von EMET behandelt werden.
- Die durch EMET bereitgestellten Speicherschutzmechanismen garantieren natürlich keinen 100-%igen Schutz. Die Wahrscheinlichkeit eines erfolgreichen Angriffs kann jedoch erfahrungsgemäß deutlich gemindert werden.
- EMET bietet Enterprise-Funktionalität durch die Integration in die Gruppenrichtlinien.

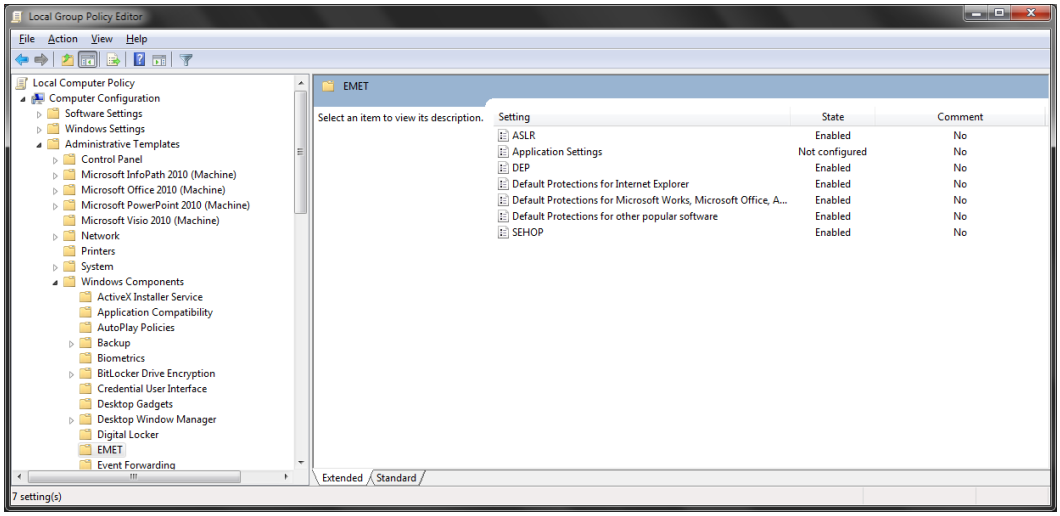
Der folgende Screenshot zeigt das (GUI) von EMET:

[35] Per Default ist dies nur auf Domänencontrollern und Applikationsservern (Fileservern) erlaubt.

[36] Wie etwa „Structured Exception Handling Overwrite Protection", „Heapspray Allocation", „NULL Page Allocation", „Export Address Table Filter" und „Bottom-up". Eine Erläuterung dieser Technologien finden sich in [11]. Download: http://www.microsoft.com/en-us/download/details.aspx?id=29851



EMET in der Version 3.0 bietet zusätzlich die Integration in Gruppenrichtlinien:



9.5 Zusätzlich installierte Software

9.5.1 Installierte Zusatzsoftware

Auf den Systemen soll nur die minimal benötigte Software installiert werden. Dies gilt nicht nur für Erweiterungen (Rollen, Features) des Betriebssystems, sondern auch für Zusatz- und Drittherstellersoftware.[37]

- Vergleiche M4.95

9.5.2 Aktualität /Patchlevel von Zusatzsoftware

Auch Drittherstellersoftware soll dem Patchmanagement-Prozess unterliegen. Siehe Abschnitt 9.1.

- Vergleiche M4.

[37] So hat etwa ein Mediaplayer oder ein Acrobat Reader nichts auf einem Server-System zu suchen.

10 Überwachung

10.1 Überwachungsrichtlinie

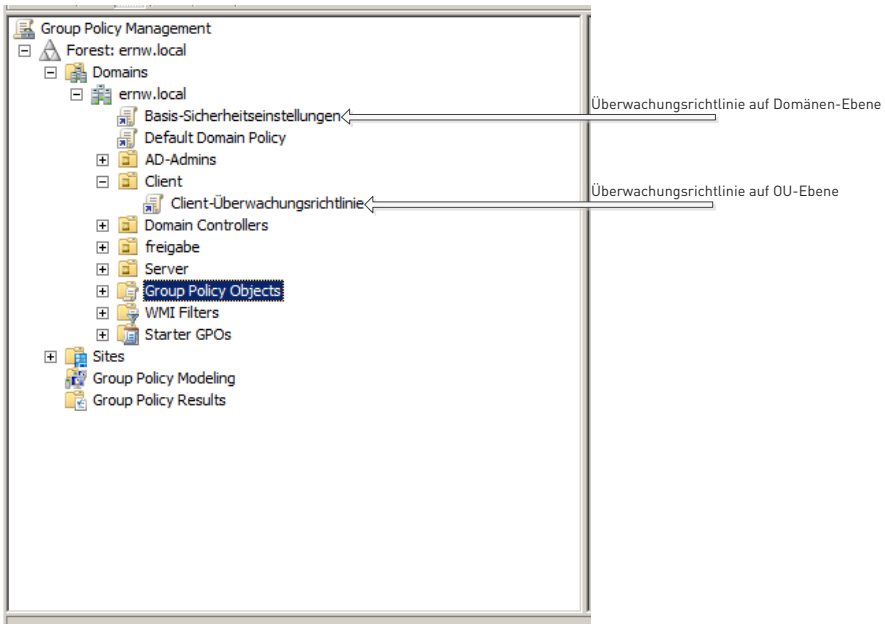
Zu einem funktionalen Sicherheitskreislauf gehören auch stets die Überwachung (Monitoring) sicherheitsrelevanter Parameter sowie die Auswertung von Logfiles. Darüber hinaus wird die Auswertung von (Sicherheits-) Logfiles (nicht nur) im Behördenkontext als Security Best Practice angenommen.

- Vergleiche: M 4.344, M 2.x-1

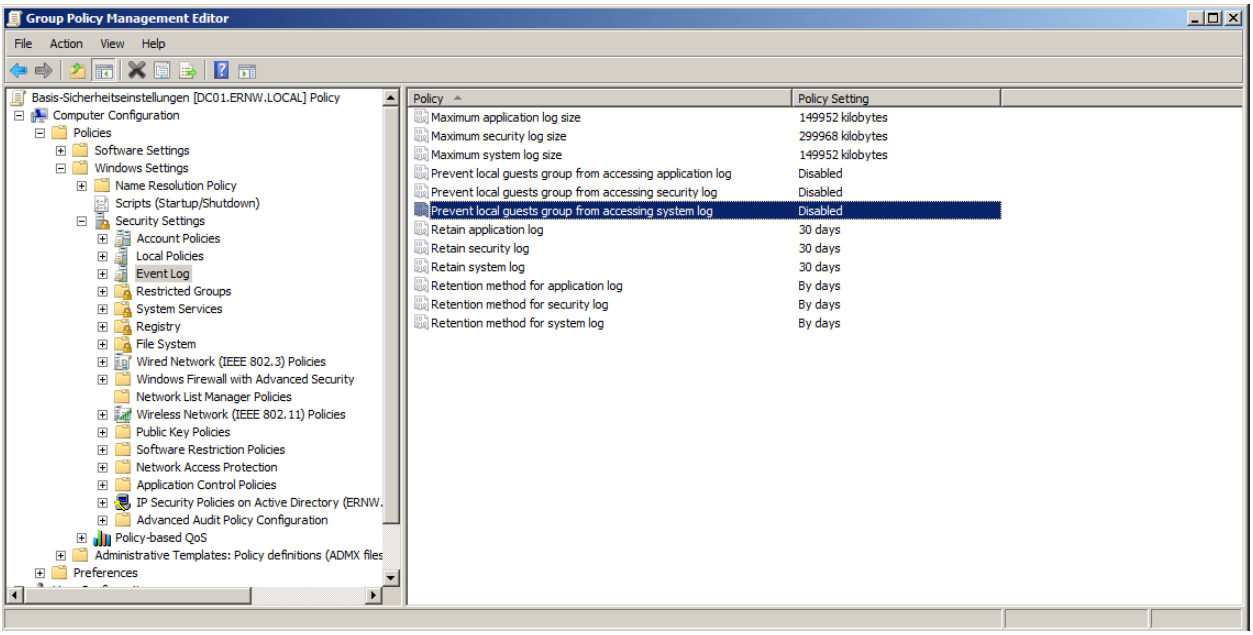
Ein funktionales Monitoring unterstützt dabei sowohl die Nachvollziehbarkeit von Aktionen wie auch die Lauffähigkeit eines Systems. Bei der Überwachung sollten grundsätzlich die folgenden Aspekte behandelt werden:

- Definition einer angemessenen Audit-Richtlinie
- Technische Umsetzung dieser Richtlinie
- Regelmäßige Auswertung der Audit-Log-Files
- Audit-Logs sollten zentral gespeichert werden

Die Definition einer angemessenen Basis-Auditrichtlinie sollte auf der höchst möglichen Ebene (idealerweise der Domänen-Ebene) erfolgen. System-spezifische Abweichungen können dann auf der OU-Ebene definiert werden. Der folgende Screenshot zeigt die Basis-Audit-Policy, die auf Domänenebene verknüpft wurde:



Das lokale Speichern (und die damit verbundene Definition einer Aufbewahrungsrichtlinie), sowie das zentrale Archivieren des Ereignisprotokolls sind wesentlich für die Nachvollziehbarkeit von Aktionen. Deshalb sollten angemessene Aufbewahrungszeiträume definiert werden, und zwar sowohl für die lokale Speicherung als auch die (zentrale) Archivierung des Ereignisprotokolls. Für die zentrale Archivierung ist Zusatzsoftware von Microsoft (etwa SCOM) oder Drittherstellersoftware einzusetzen.



Beispiel-Aufbewahrungsrichtlinie für die Ereignisprotokolle eines Windows Server-Systems

Die hier relevanten Sicherheitsereignisse werden von Microsoft nach folgenden Kategorien kategorisiert:

- Kontoanmeldung
- Account-Management
- Detaillierte Überwachung
- DS-Zugriff
- Anmelden/Abmelden
- Objektzugriff
- Richtlinienänderung
- Rechteverwendung
- System

Für jede dieser Kategorien gibt es eine Reihe von möglichen (sicherheitsrelevanten) Events, deren IDs und Bedeutung bei Microsoft nachgeschlagen werden können (vgl. [5]).

11 ZUSÄTZLICHE SICHERHEITSEINSTELLUNGEN

In diesem Abschnitt wird eine Reihe von typischen Sicherheitseinstellungen genannt, auf die das BSI bei der Prüfung zu schauen pflegt. Diese Liste erhebt selbstverständlich keinen Anspruch auf Vollständigkeit. Was die „Zuweisung von Benutzerrechten" (im GPO unter: Computer Einstellungen – Windows Einstellungen – Sicherheitseinstellungen – Lokale Richtlinien) und die „Sicherheitsoptionen" (im GPO ebenfalls unter: Computer Einstellungen – Windows Einstellungen – Sicherheitseinstellungen – Lokale Richtlinien) betrifft, so sollen an dieser Stelle nur die folgenden grundsätzlichen Bemerkungen gemacht werden:

- Einstellungen sollten nicht undefiniert bleiben (einige sind es per Default); darauf achtet das BSI
- Default-Einstellungen – sofern definiert – unter Windows Server 2008 (R2) erfüllen häufig schon die Anforderungen des Grundschutzes
- Die Veränderung mancher Einstellungen hat weitreichende Folgen (etwa die erzwungene SMB- und LDAP-Signatur) und/oder ist sehr System-spezifisch (wie etwa die Privilegien *Create a token object* oder *Trusted for delegation*)[10] und erfordert daher eine individuelle Betrachtung

11.1 Verstärkte Sicherheitskonfiguration des Internet Explorer

Die verstärkte Sicherheitskonfiguration des Internet Explorer sollte für alle Benutzer aktiviert sein.[38]

- Maßnahme ist konform zu M 4.280

11.2 Aktivierter Protected Mode für den Internet Explorer

Der Protected Mode des Internet Explorer ist per Default stets aktiviert und unterstützt den Integritätsschutz (MIC) des Betriebssystems; er sollte aktiviert bleiben.

- Vergleiche M 4.341

11.3 Autorun und Autoplay für alle Laufwerke und Protokolle deaktiviert[39]

Der automatische Start von Setup- und Audio-Dateien sollte für alle auf dem Rechner installierten Laufwerke, sowie Protokolle deaktiviert werden.

- Vergleiche M 4.339

Für die Detailkonfiguration der Automatischen Wiedergabe gelten die folgenden Empfehlungen:

Einstellung: Autoplay deaktivieren
Beschreibung: Diese Einstellung definiert, ob bei der Verwendung von Wechselmedien die Setupdateien sofort gelesen werden.
Standardwert: Nicht konfiguriert
Grundsätzliche Empfehlung: **Aktiviert**

Einstellung: Kein Kontrollkästchen „Vorgang immer durchführen" festlegen
Beschreibung: Dieser Parameter bestimmt, ob das Kontrollkästchen „Vorgang immer durchführen" im Dialogfeld der automatischen Wiedergabe angezeigt wird.

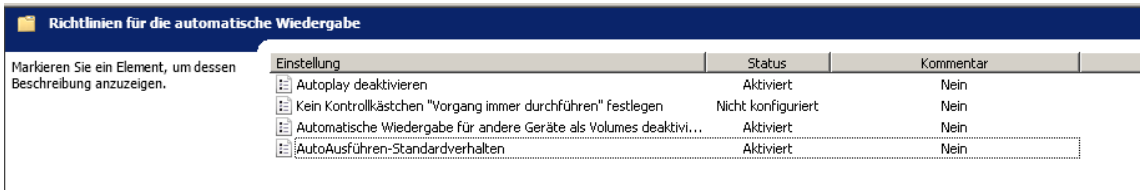
[38] Zum Thema Internet Explorer gibt es einen eigenen ERNW-Newsletter (Nr. 31) mit dem Titel: „Secure Configuration of Microsoft Internet Explorer, Version 8. Siehe http://www.ernw.de/content/e15/e26/e1489/download1495/ERNW_Newsletter_31_Secure_IE8_Configuration_en_ger.pdf.

[39] Die Konfiguration sollte in einem sog. „Basis-Sicherheitseinstellungen"- GPO vorgenommen werden, das auf höchst möglicher Ebene (Domänen-Ebene) verknüpft wird.

Standardwert: Nicht konfiguriert

Einstellung: Automatische Wiedergabe für andere Geräte als Volumes deaktivieren
Beschreibung: Dies Sicherheitseinstellung steuert, ob die automatische Wiedergabe auf Speichermedien, wie z.B. „Media Transfer Protocol (MTP)"-Geräte (Smartphone) reagieren soll.
Standardwert: Nicht konfiguriert
Grundsätzliche Empfehlung: **Aktiviert**

Einstellung: AutoAusführen-Standardverhalten
Beschreibung: Dies Sicherheitseinstellung definiert, ob AutoAusführen-Befehle, die sich z.B. in „*.inf" Dateien befinden können, ausgeführt werden.
Standardwert: Nicht konfiguriert
Grundsätzliche Empfehlung: **Aktiviert**



11.4 Sperrung des Computers[40]

Der Desktop eines angemeldeten Benutzers sollte nach spätestens 10 Minuten gesperrt werden. Für die Entsperrung des Desktops muss der zuvor angemeldete Benutzer sein Passwort eingeben. Alternativ kann ein Mitglied der Gruppe der Administratoren den Desktop durch die Eingabe seines Benutzernamens und seines Passwortes entsperren.

- Vergleiche: M 4.2

11.5 Namen des zuletzt angemeldeten Benutzers nicht anzeigen[41]

Der Name des zuletzt angemeldeten Benutzers darf aus Sicherheitsgründen vom System nicht angezeigt werden.

11.6 Nachricht für Benutzer, die sich anmelden wollen[42]

Benutzer, die sich am System anmelden möchten, erhalten aus rechtlichen Gründen auf dem Anmeldebildschirm eine Meldung wie etwa:

„Dieses System ist nur für autorisierte Benutzer der ERNW zugelassen. Für alle anderen Benutzer ist die Anmeldung an diesem System verboten."

- Vergleiche M4.244

[40] Ebenso.
[41] Ebenso.
[42] Ebenso.

11.7 Nachrichtentitel für Benutzer, die sich anmelden wollen[43]

Der Nachrichtentitel für die im vorausgegangenen Abschnitt beschriebene Meldung lautet:

„Bitte beachten“

Das kann so oder ähnlich konfiguriert werden.

- Vergleiche M4.244

12 DOKUMENTATION

12.1 Dokumentation

Last but not least: Alle technische und organisatorische Komponenten eines Windows Server 2008 R2-Systems sowie des Active Directory sollten ausreichend dokumentiert sein und die Dokumentation sollte aktuell gehalten werden. Änderungen sollten ebenso dokumentiert werden (Changemanagement). Für die Dokumentation sollte es idealerweise ein Dokumentenmanagement (-System) geben. Die Dokumentation sollte sowohl generelle Aspekte des Was und des Wie enthalten als auch Betriebshandbücher der technischen Komponenten, Architekturdokumente und Notfallpläne.

Dabei sollte die Dokumentation stets die folgenden drei Anforderungen erfüllen:

- Vollständigkeit
- Aktualität
- Präzision

- Vergleiche M4.280

Für weitere Fragen steht Ihnen das Windows Security-Team von ERNW gern zur Verfügung.

Herzliche Grüße,

Friedwart Kuhn und Dominik Phillips.

Friedwart Kuhn

Senior Security Consultant

ERNW GmbH - Carl-Bosch-Str. 4 - 69115 Heidelberg - www.ernw.de

Tel. +49 6221 480390 - Fax 6221 419008 - Cell +49 151 52411855

[43] Ebenso.

13 ANHANG

13.1 Quellen

[1] Eric Tierling, Windows Server 2008 R2, Einrichtung Verwaltung Referenz, Addison Wesley 2010

[2] Zum Entfernen von administrativer Freigaben in Windows Server 2008, *http://support.microsoft.com/kb/954422/*

[3] Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren, *http://technet.microsoft.com/de-de/library/dd851895/*

[4] Windows Server 2008 R2 SP1 Security Guide, Security Compliance Manager, Microsoft 2011

[5] Description of security events in Windows 7 and in Windows Server 2008 R2, *http://support.microsoft.com/kb/977519/en-us*

[6] Vorabversion B 3.XX Windows Server 2008, *https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/download/download.html*

[7] Newsletter 17 / Juli 2007 "Mandatory Integrity Control", *http://www.ernw.de/content/e15/e28/index_ger.html*

[8] IT-Grundschutz-Kataloge12, *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html*

[9] Microsoft Security Compliance Manager, *http://technet.microsoft.com/library/cc677002.aspx*

[10] Active Directory Security: Sicherheitsbetrachtung des Privilegs "Trusted for delegation", *http://www.ernw.de/content/e15/e28/index_ger.html*

[11] „Enhanced Mitigation Experience Toolkit", *http://www.microsoft.com/en-us/download/details.aspx?id=29851*

13.2 Sicherheitsereignisse in Windows 7 und Windows Server 2008 R2

Siehe [5][44].

Auditkategorie: Anmeldeversuche

Subcategory: Credential Validation	
ID	Message
4774	An account was mapped for logon.
4775	An account could not be mapped for logon.
4776	The computer attempted to validate the credentials for an account.
4777	The domain controller failed to validate the credentials for an account.

Subcategory: Kerberos Authentication Service	
ID	Message
4768	A Kerberos authentication ticket (TGT) was requested.

[44] Siehe dazu „Beschreibung der Sicherheitsereignisse in Windows 7 und Windows Server 2008 R2" (DE) *http://support.microsoft.com/kb/977519/de*.

4771	Kerberos pre-authentication failed.
4772	A Kerberos authentication ticket request failed.

Subcategory: Kerberos Service Ticket Operations	
ID	Message
4769	A Kerberos service ticket was requested.
4770	A Kerberos service ticket was renewed.
4773	A Kerberos service ticket request failed.

Auditkategorie: Logon/Logoff

Subcategory: Logoff	
Collapse this tableExpand this table	
ID	Message
4634	An account was logged off.
4647	User initiated logoff.

Subcategory: Logon	
ID	Message
4624	An account was successfully logged on.
4625	An account failed to log on.
4648	A logon was attempted using explicit credentials.
4675	SIDs were filtered.

Subcategory: Other Logon/Logoff Events	
Collapse this tableExpand this table	
ID	Message
4649	A replay attack was detected.
4778	A session was reconnected to a Window Station.
4779	A session was disconnected from a Window Station.
4800	The workstation was locked.
4801	The workstation was unlocked.

4802	The screen saver was invoked.
4803	The screen saver was dismissed.
5378	The requested credentials delegation was disallowed by policy.
5632	A request was made to authenticate to a wireless network.
5633	A request was made to authenticate to a wired network.

Auditkategorie: Systemereignisse

Subcategory: Security State Change	
ID	Message
4608	Windows is starting up.
4616	The system time was changed.
4621	Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.

Subcategory: Security System Extension	
ID	Message
4610	An authentication package has been loaded by the Local Security Authority.
4611	A trusted logon process has been registered with the Local Security Authority.
4614	A notification package has been loaded by the Security Account Manager.
4622	A security package has been loaded by the Local Security Authority.
4697	A service was installed in the system.

Subcategory: System Integrity	
ID	Message
4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
4615	Invalid use of LPC port.
4618	A monitored security event pattern has occurred.
4816	RPC detected an integrity violation while decrypting an incoming message.
5038	Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
5056	A cryptographic self test was performed.
5057	A cryptographic primitive operation failed.
5060	Verification operation failed.
5061	Cryptographic operation.
5062	A kernel-mode cryptographic self test was performed.
6281	Code Integrity determined that the page hashes of an image file are not

	valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error

Auditkategorien Kontenverwaltung

Subcategory: User Account Management	
ID	Message
4720	A user account was created.
4722	A user account was enabled.
4723	An attempt was made to change an account's password.
4724	An attempt was made to reset an account's password.
4725	A user account was disabled.
4726	A user account was deleted.
4738	A user account was changed.
4740	A user account was locked out.
4765	SID History was added to an account.
4766	An attempt to add SID History to an account failed.
4767	A user account was unlocked.
4780	The ACL was set on accounts which are members of administrators groups.
4781	The name of an account was changed:
4794	An attempt was made to set the Directory Services Restore Mode.
5376	Credential Manager credentials were backed up.
5377	Credential Manager credentials were restored from a backup.