Sicherheit bei APP-V, VDI, und Desktopvirtualisierung

Marc Grote
IT TRAINING GROTE
blog.it-training-grote.de
www.it-training-grote.de

\\ice:lingen
intelligent communities for europe

Inhalt

- Ueberblick ueber Virtualiserungstechnologien
- Microsoft Hyper-V (Security 101)
- Sicherheitsmassnahmen in Microsoft SCVMM
- Security Best Practices fuer Microsoft …
  - APP-V
  - Windows 7 XP Mode
  - MED-V
- Allgemeine Sicherheitsempfehlungen
  - Netzwerksicherheit (Zertifikate, IPSEC, SSL)
- Microsoft Security Compliance Manager

Referentenvorstellung

Ice 2008

Cebit 2010

Ueberblick ueber Virtualisierungstechnologien

- Desktop
  - Ein Windows Endgeraet wird in einer virtuellen Umgebung auf einem zentralen Server ausgefuehrt. Jedem Benutzer steht ein eigenes virtuelles Endgeraet zur Verfuegung
    - Windows XP Mode, MED-V, Microsoft PVD
- Application
  - Die Anwendung wird nicht zentral, aber lokal ausgefuehrt und nicht lokal installiert, sondern laeuft in einer isolierten Umgebung auf dem Endgeraet
    - Microsoft APP-V
- Server
  - Ein Server wird in einer virtuellen Serverumgebung betrieben und stellt (fast) alle Funktionen eines physikalischen Server zur Verfuegung
    - Microsoft Hyper-V, Microsoft Virtual Server

Ueberblick ueber Virtualisierungstechnologien

- Presentation
  - Anwendungen werden zentral auf einem Server ausgefuehrt, auf diese Endgeraete per Terminal Client Software zugreifen
    - Microsoft Remote Desktop Services
- Profile
  - Benutzerprofileinstellungen werden von den Benutzerdaten getrennt und ermoeglichen einen einheitlichen Zugriff auf Benutzerprofile von jedem Endgeraet

Sicherheit in virtuellen Umgebungen?

- Virtuelle Maschinen muessen nicht gehaertet werden, dass Hostsystem ist ja sicher?
- Wer patcht schon seine virtuellen Maschinen?
- Ich kuemmere mich nur um meine VM, das Host-System laeuft einfach so mit
- Wenn mein Host-System kompromittiert wird, betrifft das nicht meine virtuellen Maschinen!

Hyper-V Security (101)

- Windows Server 2008 / R2 Core!!
  - Reduziertes Attack Surface
  - Reduziertes Footprinting
  - Hoehere Systemverfuegbarkeit durch weniger Updates
- Aktuelle Patchstrategie
- Haerten des Hyper-V Hostsystems
  - Keine Installation zusaetzlicher Anwendungen
- Dedizierte Netzwerkkarte fuer Management und ggfs. iSCSI
- Anwendung des Windows Server 2008 Security Guide

Hyper-V Security (101)

- Verwendung von EFS nicht moeglich zur Absicherung von VM
- Firewall empfohlen – Host-FW und ISA/TMG
- Bitlocker nur auf dem Hyper-V Host
  - Funktioniert nicht mit Failover Clustering!
- Virenscanner
  - Ausschluss der VHD Datenverzeichnisse
  - VMMS.EXE (Mgmt) und VMWP.EXE (WorkerProcess) nicht scannen

Best Practice VM in Hyper-V

- Speicherort fuer VHD, VMC
- Speicherzuordnung zur VM (R2 SP1 nutzen)
- Limit Prozessornutzung
- VM Zugriff nur auf notwendigen Storage
- Zeitsynchronisation in VM (DC?)
- Speichern von VM mit gleichem Schutzbedarf auf der selben Host-Maschine
- Hyper-V Netzwerke
- Sicheres Loeschen von nicht mehr verwendeten VM
- Speichern von Snapshots (AVHD) an einem „sicheren“ Ort
- Firewallkonfiguration bei Server Core

Gast-Sicherheit

- RAM und CPU Monitoring
- VM Limits im Host System setzen
- Virenscanner
- Security Hardening (Hyper-V Sec. Guide)
- Patching
- DoS Angriffe auf VM mit Auswirkung auf Hyper-V Host und andere Gaeste beschraenken

Berechtigungen fuer Hyper-V VHD

Names	Permissions	Apply to
Administrators System	Full Control	This folder, subfolders, and files
Creator Owner	Full Control	Subfolders and files only
Interactive Service Batch	Create files/write data Create folders/append data Delete Delete subfolders and files Read attributes Read extended attributes Read permissions Write attributes Write extended attributes	This folder, subfolders, and files

Berechtigungs-Delegation

- Verwendung von AzMan (Authorization Manager)
- XML Store - C:\ProgramData\Microsoft\Windows\Hyper-V\InitialStore.xml
- Active Directory Store (Windows 2003 Functional Level)
- Ablauf
  - New Role Definiton
  - New Task Definition (Task zuordnen)
  - New Role Assignment
    - Assign Users and Groups
    - Gewuenschten Task hinzufuegen

SCVMM 2008 R2 Ueberblick

- P2V-Funktionen (Physical to Virtual)
- V2V-Funktionen (Virtual to Virtual), inklusive Vmware
- Zentrale Verwaltungskonsole fuer alle Microsoft Hyper-V Server und deren Gastsysteme
- Self Service Portal fuer das Provisioning virtueller Maschinen durch Nicht Administratoren
- Zentrale Library fuer die Ablage virtueller Maschinen und Templates

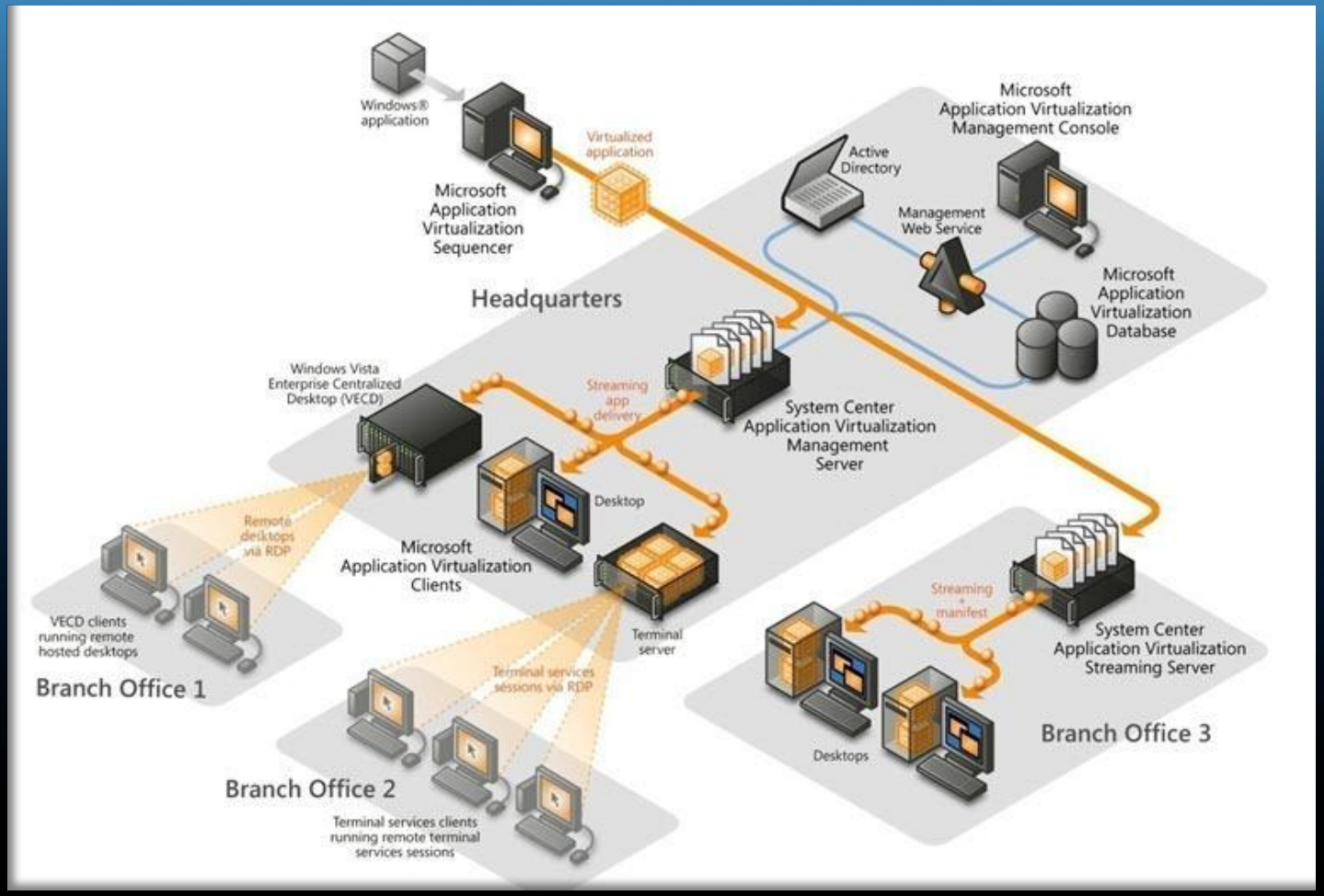
SCVMM 2008 R2 Rollen

- Administrator Profile
  - Vollstaendiger Zugriff auf alle Hosts, VM und Libraries
- Delegated Administrator Profile
  - Zugriff auf einen definierten Pool von Host Gruppen und Library Server
- Self-Service User Profile
  - Zugriff auf einen definierten Satz von VM ueber ein Webinterface

Microsoft APP-V

- Anwendungsvirtualisierung
- Ehemals Softgrid
- Zentrale Verwaltung von virtualisierten Anwendungen
- Anwendungen werden in einer „Sandbox“ auf dem Endgeraet ohne lokale Installation ausgefuehrt

Microsoft APP-V



Microsoft App-V

- APP-V Management Server
  - Paketinhalt streamen, Shortcut Publish.
- APP-V Streaming Server
  - Hostet APP-V Packages
- APP-V Data Store
  - SQL Datenbank mit den APP-V Informationen
- APP-V Management Service
  - Kommunikation mit APP-V Datastore
- APP-V Management Console
  - APP-V Administration
- APP-V Sequencer
  - Monitoring und Capturing der Installation von virtuellen Paketen
- APP-V Client
  - APP-V Desktop Client / APP-V Terminal Services Client

Security Best Practices fuer APP-V

- App-V 4.5 wurde nach folgenden Sicherheitsinitiativen programmiert:
  - Trustworthy Computing (TwC)
    - Sicherheit, Datenschutz und Zuverlaessigkeit von Software, Diensten und Produkten sowie Integritaet im geschaeftlichen Handeln
  - Secure Windows Initiative (SWI)
    - Designing, Erstellen und Testen von sicheren Produkten
  - Security Development Lifecycle (SDL)
    - Entwickeln sicherer Software welche wenig fehleranfaellig gegen boeswillige Angriffe ist

APP-V 4.5/6 Sicherheitsfunktionen

- Unterstuetzung fuer Streaming ueber das Internet
- Kerberos Authentication und Authorization
- “Secure by Default” Konfiguration im Rahmen der MS Trustworthy Computing Initiative
- Sicherer Zugriff auf Logdateien und Kontrolle ueber die Logdateigroesse
- Benutzerberechtigungen fuer den APP-V Desktop Client
- Dateisystem ACL koennen waehrend des Sequencing Prozess aufgezeichnet werden (Registry ACL nicht)

Security Best Practices fuer APP-V

- Hardening des Betriebssystem
  - Windows Server 2008 Security Guide
- Hardening des SQL Server
  - SQL Server Security Best Practice Guide
- Hardening der Netzwerkinfrastruktur
  - Sichere Kommunikationskanaele
  - Datenisolation
  - Zugriffskontrolle / -Steuerung auf Netzwerkebene
  - Firewall / IDS / IPS

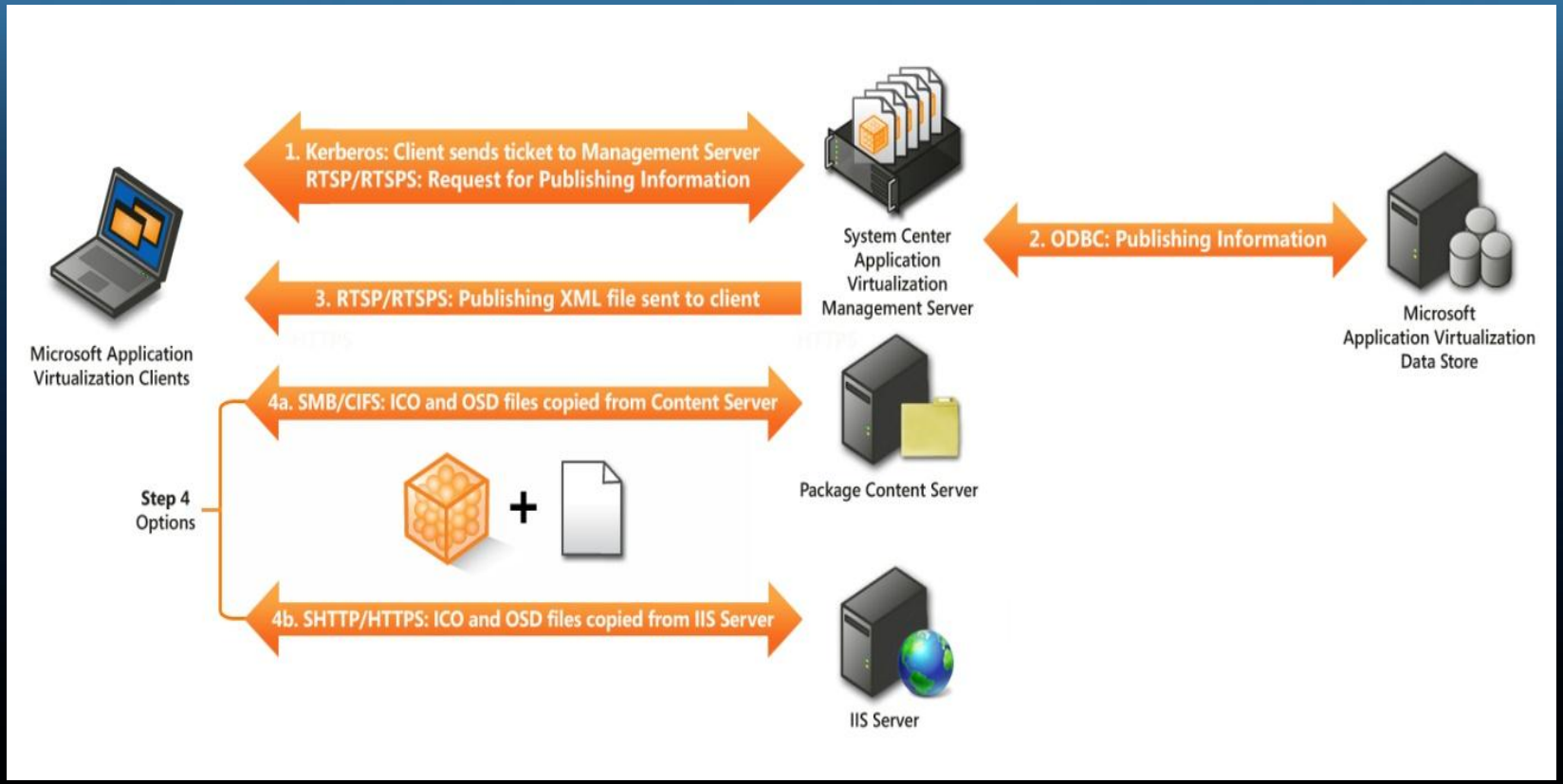
Security Best Practices fuer APP-V

- APP-V Kommunikation (Data Store)
  - Mgmt Server und Mgmt Service -> Port 1433 mit MS SQL Server
  - Abfrage Applikationen und Konfiguration + Schreiben
  - Mgmt Service -> Auth. als Administrator
  - Absicherung mit IPSEC empfehlenswert
  - Windows Server 2008 Security Guide
- APP-V Kommunikation (Content)
  - Mgmt Server –> Content Directory (Filesystem)
  - Bei Verwendung von Remote Storage –> IPSEC

Security Best Practices fuer APP-V

- Mgmt. Console -> Mgmt. Service
  - Erlaubt u. a. Aenderungen am DataStore
  - Verwendung von HTTPS
- APP-V Kommunikation (Client to Server)
  - APP-V Client zu APP-V Mgmt. Server
  - Kommunikation ueber User Credentials
  - XML File Transfer (enthaelt Pfad zur OSD-Datei)
  - No built in Security
  - Verwendung von RTSP/RTSPS (TLS – Server Auth. only) fuer Streaming
  - Content copy unter Verwendung von SMB/HTTP -> IPSEC fuer SMB oder HTTPS fuer HTTP verwenden

APP-V


1. Kerberos: Client sends ticket to Management Server
RTSP/RTSPS: Request for Publishing Information
2. ODBC: Publishing Information
3. RTSP/RTSPS: Publishing XML file sent to client
4a. SMB/CIFS: ICO and OSD files copied from Content Server
4b. SHTTP/HTTPS: ICO and OSD files copied from IIS Server
Step 4
Options
Microsoft Application Virtualization Clients
System Center Application Virtualization Management Server
Microsoft Application Virtualization Data Store
Package Content Server
IIS Server

Security Best Practices fuer APP-V

- Zertifikatanforderungen
  - Zertifikat muss gueltig sein
  - Korrekte EKU (Extended Key Usage) – ServerAuthentication (OID 1.3.6.1.5.5.7.3.1)
  - Namensuebereinstimmung des FQDN des Servers mit dem Common Name (CN) des Zertifikats
  - SAN in NLB Umgebungen notwendig
  - Client und Server muessen der ausstellenden CA vertrauen
  - Private Key des Zertfikats muss fuer Change Rechte des APP-V Service zugreifbar sein (R Permission fuer Priv Key)

Security Best Practices fuer APP-V

- APP-V Client Security
  - SFTLOG.TXT (Client Logfile) nur vom Admin aufrufbar
  - Authorization fuer Cached Applications beachten (liegt im Public Profile von Vista)
    - Pfad vor oder nach der Installation aenderbar
    - Ggfs. Applikationen im Offline Mode zu oeffnen
    - „Require AuthorizationIfCached“ Key
  - Verwendung von ADM-Templates (http://www.microsoft.com/downloads/details.aspx?FamilyID=67cdf9d2-7e8e-4d76-a552-fd82dbbff9bc&displaylang=en)
  - Registry – Nur Admin Zugriff
  - Virus Scanning -> Ausnahme SFTFS.FSD Datei (Packed Cache)

Security Best Practices fuer APP-V

- APP-V Server im „Internet“
  - RTSPS auf Mgmt Server erforderlich
  - HTTPS auf IIS erforderlich
  - APP-V Server hinter ISA/TMG (Empfohlen)
  - APP-V Server in der DMZ
    - Zusaetzliche Ports
    - SQL
    - SMB/CIFS (wenn Content Verzeichnis im LAN liegt)
    - Kerberos
    - DNS
    - LDAP
  - Kerberos Auth. von Client zu AD
    - Failback zu NTLM, wenn Ticket abgelaufen und kein AD Zugriff moeglich

Security Best Practices fuer den Windows 7 „XP Mode“

- Windows XP SP3 als Basis
- Moechte auch gepatched werden
- Behandeln Sie eine VM wie eine physikalische Maschine
  - Group Policy
  - NTFS / Registry ACL
  - Client Virus Scanner
  - MBSA etc.

Microsoft MED-V

- Bestandteil des MDOP (Mircosoft Desktop Optimization Pack)
- Bereitstellung, Verwaltung und Nutzung von Images virtueller PC
- Zentrale Loesung auf Basis von Virtual PC SP1 + QFE
- Zentrale Bereitstellung von Anwendungen im Virtual PC, welche nicht Windows 7 kompatibel sind
- Zentral verwalteter XP Mode fuer groessere Umgebungen

Security Best Practice fuer MED-V

- Verwendung von HTTPS im MED-V Server Configuration Manager
- Sparsame Verwendung von Management Permissions im MED-V Server Configuration Manager
- Virtuelle Maschinen moechten auch gepatched werden
- Behandeln Sie eine VM wie eine physikalische Maschine
  - Group Policy
  - NTFS / Registry ACL
  - Client Virus Scanner
  - MBSA etc.

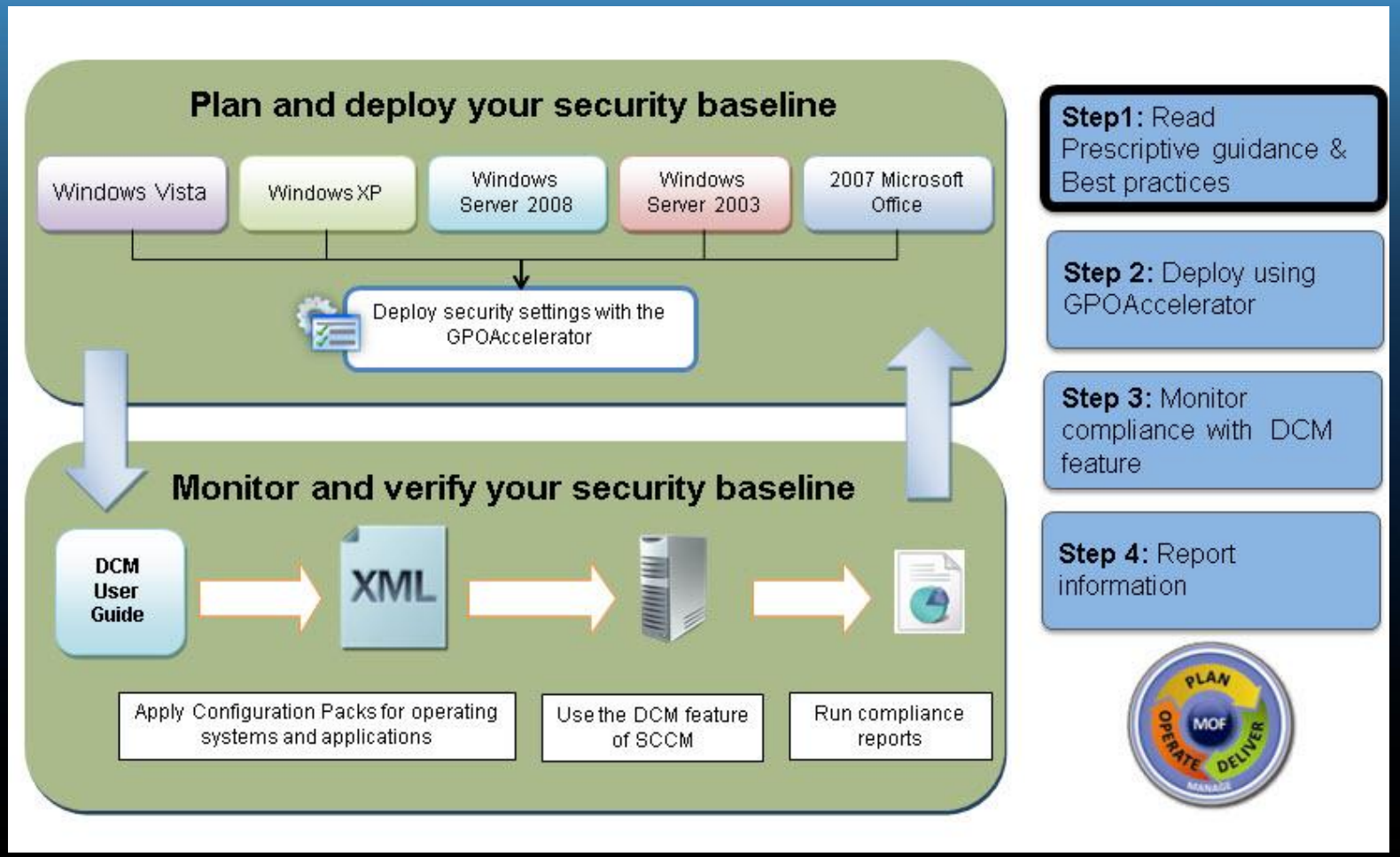
Allgemeine Sicherheitsempfehlungen

- Patch as Patch can (aber wann?)
- Verschluesselung verwenden
  - IPSEC
  - SSL
  - Verschluesselung der Anwendungssoftware nutzen
- Monitoring und zentrale Verwaltung
- Audit und Revision

MS Security Compliance Manager

- Nachfolger des SCMT (Security Compliance Management Toolkit)
- Zentrale Verwaltung von Security Baselines
- Planen, verteilen und verwalten von Sicherheitsrichtlinien fuer Windows Clients – Server und Applikationen
- Erstellt Baseline
  - Export in XLS, Group Policies, DCM Packs (SCCM)

MS Security Compliance Manager



Lust auf Links

- Microsoft Security Compliance Manager
  - http://technet.microsoft.com/en-us/library/cc677002.aspx
- MED-V
  - http://www.microsoft.com/windows/enterprise/products/mdop/med-v.aspx
- APP-V
  - http://www.microsoft.com/systemcenter/appv/default.mspx
- SCVMM 2008 R2
  - http://www.microsoft.com/systemcenter/en/us/virtual-machine-manager.aspx
- Windows 7 XP-Mode
  - http://blogs.technet.com/b/sieben/archive/2009/05/08/windows-xp-mode-mit-windows-7-download.aspx
- Hyper-V Security Guide
  - http://go.microsoft.com/fwlink/?LinkID=147397
- Hyper-V Attack Surface Reference
  - http://download.microsoft.com/download/8/2/9/829bee7b-821b-4c4c-8297-13762aa5c3e4/Windows%20Server%202008%20Hyper-V%20Attack%20Surface%20Reference.xlsx

Es gibt keine großen Entdeckungen und Fortschritte, solange es noch ein unglückliches Kind auf Erden gibt.

There ´s no such thing as a discovery or progress as long as we have bitterly unhappy children on earth.

Er zijn geen grote ontdekkingen en geen vooruitgang, zolang er op deze wereld nog één kind ongelukkig is.

(Albert Einstein)

Fragen?

Das Ende

Vielen Dank fuer Ihre Aufmerksamkeit