Absicherung von Microsoft Netzwerken mit Bordmitteln

Marc.Grote aka Jens Mander aka Marcimarc

Agenda

- PKI-Infrastrukturen
- Verschluesselung
- Active Directory Sicherheitsmodell
- Authentifizierungsverfahren
- Authentication Silos
- Privileged Access Management (PAM)
- LAPS (Local Administrator Password Solution)
- JEA (Just Enough Administration)
- Bitlocker und Bitlocker To Go
- Security Configuration Wizard (SCW)

Agenda

- Advanced Threat Analytics (ATA) – Windows Defender
- Microsoft Baseline Security Analyzer (MBSA)
- Shielded VM in Hyper-V Umgebungen
- Enhanced Mitigation Experience Toolkit (EMET)
- Virtual Secure Mode / Credential Guard
- Firewall Management
- Logging und Monitoring
- Organisatorische Massnahmen zur Erhoehung der Sicherheit in IT-Netzwerken

Wer bin ich?

- Marc Grote
- Seit 1989 hauptberuflich ITler / Seit 1995 Selbststaendig
- Microsoft MVP fuer Hyper-V 2014, seit 2015 MVP Cloud and Datacenter (MVP Forefront von 2004-2014)
- Microsoft MCT/MCSE Messaging/Security/Server/MCLC /MCITP*/MCTS*/MCSA*/MC*
  MCSE Private Cloud, Server Infrastructure, Exchange
  MCS Server Virtualization Hyper-V / System Center/ Azure
  MCITP Virtualization Administrator
- Buchautor und Autor fuer Fachzeitschriften
- Schwerpunkte:
  - Windows Server Clustering/Virtualisierung/PKI
  - System Center SCVMM/SCEP/DPM
  - Exchange Server seit Version 5.0
  - von *.Forefront reden wir nicht mehr ☹

PKI Infrastrukturen

- Certificate Authority
- Certificate Templates
- Certificates
- Registration Authority
- CRL & OCSP
- HSM
- CSP
- Role Separation
- CNG
- SCEP/NDES
- Key Recovery
- Trusted Root CA Certificates

Demo

Verschluesselung

- EFS
- Bitlocker
- SSL/TLS
- IPSEC/PPTP/SSL VPN
- S/MIME & PGP
- SMTPS
- LDAPS
- SMB/CIFS
- HTTPS
- Native Protokollverschluesselung

Active Directory Sicherheitsmodell

- Sichere Kennwoerter
- Dedizierte Admin Accounts
- Restricted Groups
- Managed Service Accounts
- Anmelderestrictionen
- Privileged User Accounts
- User Berechtigungen und -Rechte
- Group Policies
- Dokumentation
- User Account Control (UAC)

Active Directory Sicherheitsmodell

- DSRM Password
- Dedicated Admin Workstations
- Disable Guest – Rename Administrator
- Password Policy
- Protected Users
- Port und Service Minimierung
- Event Audit
- AD Sicherheitszonen
- Timesync
- DC Security
- RODC
- Trust (Selective Auth., SID-Filtering)

Demo

Authentifizierungsverfahren

- NTLM (enable only v2)
- Kerberos
- Digest
- oAuth
- Form Based Authentication (FBA)
- Client Certificate
- Zwei Faktor Authentifizierung (SMS/Token/PIN)
- Biometrie
- Windows Hello
- Passport
- Azure

Authentication Silos

- Legt Zugriff und Authentifizierung fuer restricted Accounts im Active Directory fest
- Authentication Policy definiert Kerberos Ticket Lifetime / Geraeterichtlinien (z. B. NTLM ablehnen) und Authentifizierungs-Anforderungen (Managed Service Account – Managed Group Service Accounts)
- Restricted Users Group
- Dynamic Access Control (DAC) ist Voraussetzung
- Erstellung im ADAC

Privileged Access Management (PAM)

- Mitgliedschaft in administrativen Gruppen auf Zeit
- Multi Faktor Authentifizierung integrierbar
- AD Forest mit Windows Server 2016 erforderlich
- AD Trust zum Produktions Forest erforderlich
- PAM kann separat aktiviert werden → Einstellung irreversibel
- SAM verwaltet Ablaufzeit von Gruppenzugehoerigkeiten → Token
- Kerberos TGT erhaelt Ablaufzeit der kuerzesten Gruppenmitgliedschaft
- Provisionierung mit MIM (Microsoft Identity Manager → ehemals FIM (Forefront Identity Manager)
- Administrative Gruppen werden im PAM AD Forest gespiegelt mit MIM → Shadow Security Principals)

Local Administrator Password Solution (LAPS)

- Aenderung von Administrator Kennwoertern auf lokalen Windows Clients
- Reaktion auf MS14-025
- Kennwoerter werden im AD gespeichert und auf dem Client aktualisiert
- Administration ueber GPO und GPO Client Side Extension
- Download kostenlos erhaeltlich

Just Enough Administration (JEA)

- Reduzierung der Anzahl Administratoren auf dem System
- Limitierung der Zugrissberechtigungen von Benutzern
- Download kostenlos erhaeltlich
- Windows Management Framework 5.0 notwendig
- Installation und Konfiguration via PowerShell
- Erweiterung der PowerShell um JEA-Extensions

Bitlocker & Bitlocker to Go

- Bitlocker bei mobilen Geraeten verwenden
- Bitlocker bei unsicheren Servern verwenden
- Bitlocker in virtuellen Maschinen verwenden
- Verschluesselung und Einstellungen per Group Policy steuern
- Alle Wechseldatentraeger schuetzen
- Bitlocker Network Unlock
- Bitlocker Recovery Key im Active Directory speichern

Demo

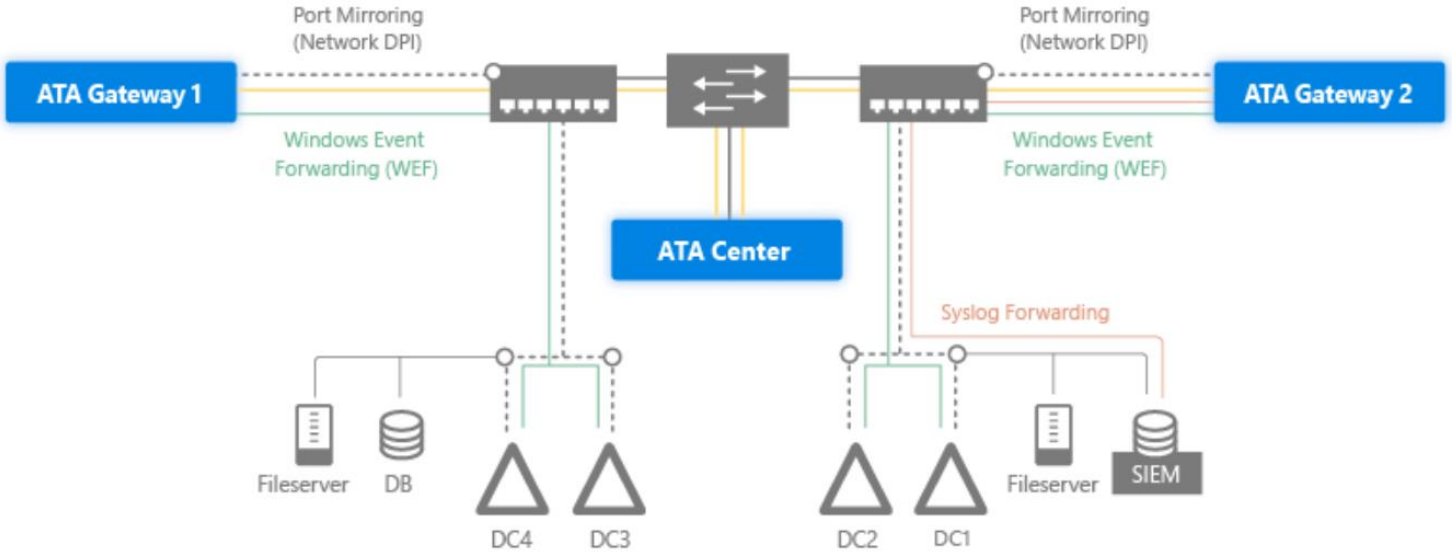
Security Configuration Wizard

- Rollenbasierte Sicherheit fuer Windows Systeme
- Referenzmaschine als Basis fuer Richtlinien
- Anwendung manuell per XML
- Konvertierung von SCW-Richtlinien per SCWCMD in Group Poliy Objects
- Teilweise verfuegbar fuer Microsoft Server Anwendungen

Demo

Advanced Threat Analytics (ATA)

- Analysen von Anomalien im Verhalten
- Erkennung von Angriffen
- Warnungen vor bekannten Sicherheitsrisiken



Quelle: https://technet.microsoft.com/en-us/library/dn707709.aspx

Demo

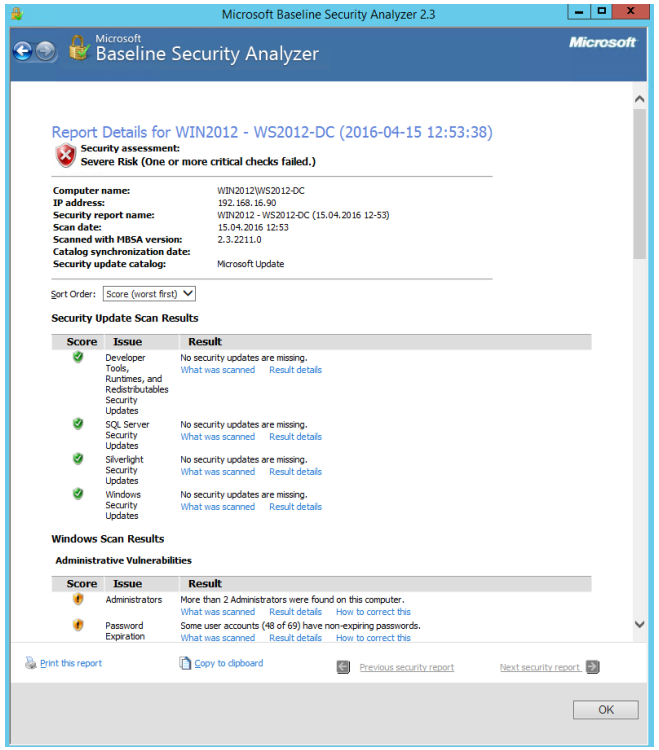
Enhanced Mitigation Experience Toolkit

- Verhinderung der Ausnutzung von Sicherheitsluecken in Anwendungen
- Certificate Pinning
- Certificate Trust Configuration
- Integration in Windows Sicherheitsfunktionen (DEP, SEHOP, ASR, MandatoryALSR)
- Bereitstellung per Group Policy / SCCM oder anderen Loesungen
- Download kostenlos erhaeltlich

Demo

Microsoft Baseline Security Analyzer

- Bestimmung des Sicherheitszustands von Windows Systemen und Microsoft Anwendungen
- Empfehlungen zur Behebung von gefundenen Problemen
- Ueberpruefung von einzelnen Systemen oder Netzwerk-Scans
- Integration mit WU/MU/WSUS/SCCM
- Download kostenlos erhaeltlich



Security Compliance Manager (SCM)

- Konfigurations Baselines fuer Windows Systeme und Anwendungen
- Aktuell fuer Windows 10 und Server 2016
- SCM erstellt Gruppenrichtlinienobjekte mit Baseline Konfigurationen
- SCM enthaelt Security Guides
- Download: https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx

Attack Surface Analyzer

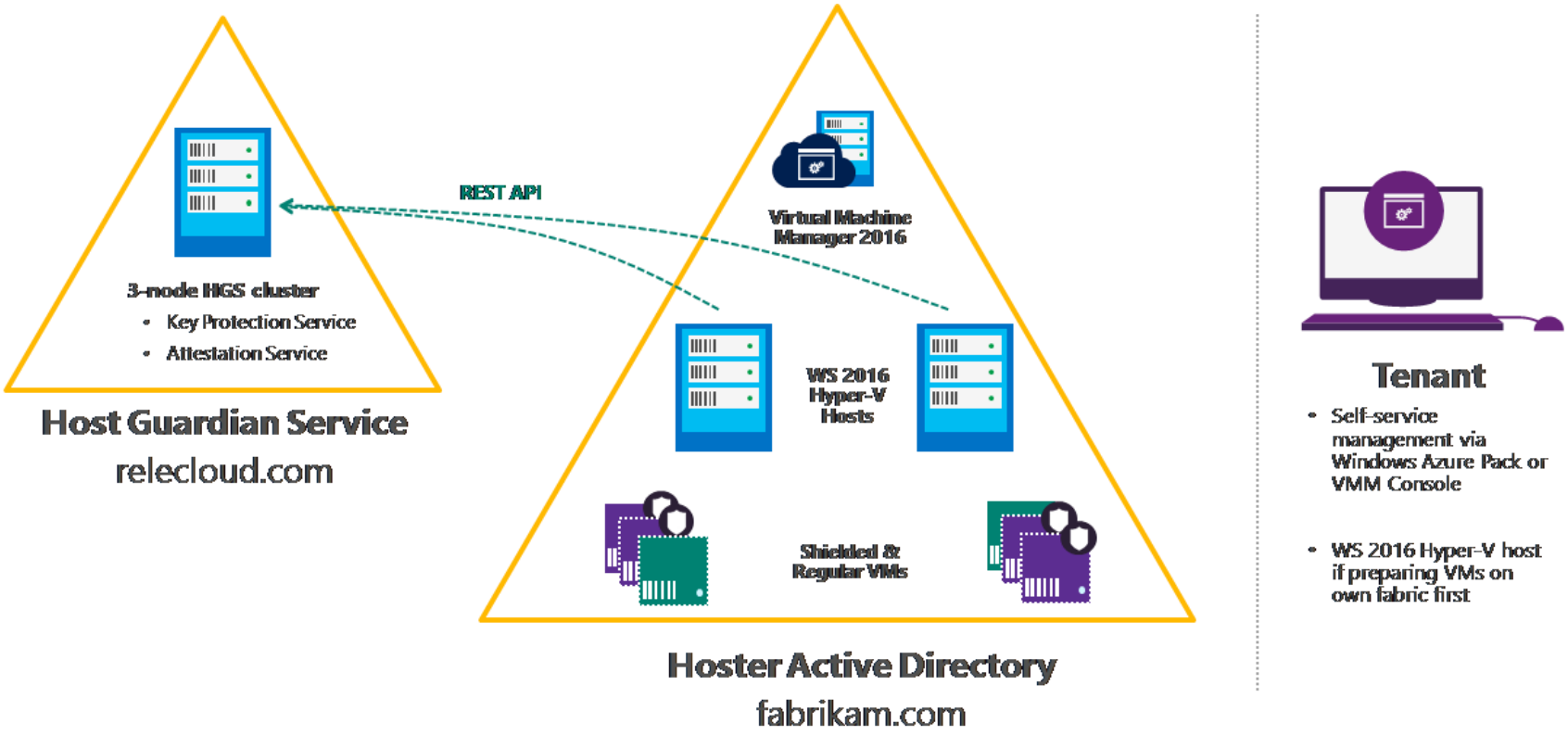
- Erstellt einen Snapshot eines Systems vor und nach der Installation von Anwendungen und vergleicht die Aenderungen auf Sicherheitsgefaehrdungen nach Microsoft Best Practices
- Download: https://www.microsoft.com/en-us/download/details.aspx?id=24487

Demo

Shielded VM in Hyper-V Umgebungen

- VSM – Virtual Secure Mode
- Shielded VM – Neue Schaltflaeche in Gen 2 VM
- Hyper-V Host muss TPM 2.0 und UEFI 2.3.1 verwenden, wenn kein dedizierter AD Forest verwendet warden soll
- Nutzung von Virtual TPM in VM
- Bitlocker Verschluesselung in VM (Live Mig Traffic)
- Ausfuehrung der VM nur auf Trusted Hosts
- Kein Zugriff durch nicht erlaubte Hyper-V / VMM Administratoren moeglich
- HGS (Host Guardian Service) verwendet dedizierten Active Directory Forest, wenn kein TPM 2.0 und UEFI 2.3.1 auf den Hyper-V Hosts verfuegbar ist
- HGS fuehrt Host-Validierung und Schluesselverteilung durch

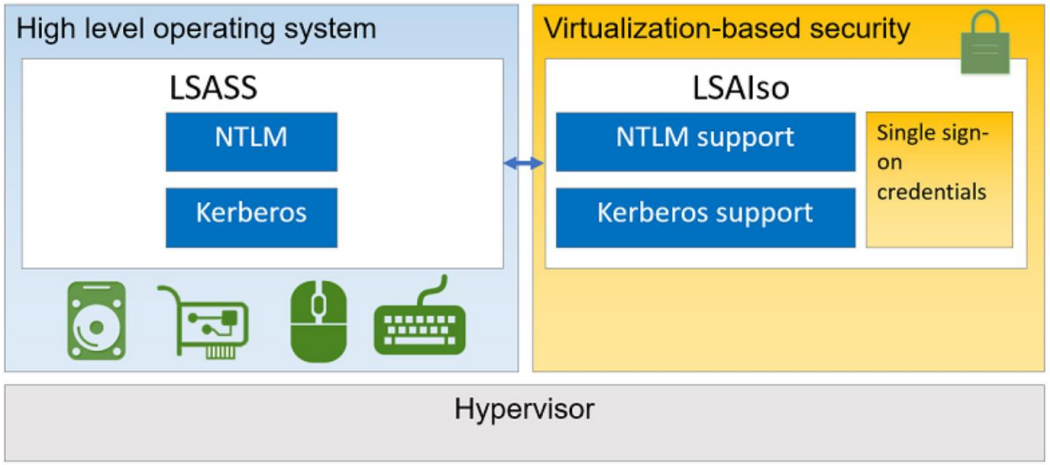
Shielded VM in Hyper-V Umgebungen



Source: TPM_version_Shielded VM and Guarded Fabric Deployment Guide for TP4.docx

Virtual Secure Mode / Credential Guard

- Schutz von Anmeldeinfomationen (LSA) mit Hilfe von Virtualisierung (VSM)
- Credential Guard kommuniziert ueber die LSA mit LSAIso
- Windows 10 Enterprise
- UEFI 2.3.1
- Secure Boot
- Intel VT-x oder AMD-V
- X64
- TPM 1.2 oder 2.0
- Aktivierung ueber GPO



Quelle: https://technet.microsoft.com/de-de/library/mt483740(v=vs.85).aspx

Firewall Management

- Enterprise Firewall
- Multi Layered Security
- Mehr Stufen DMZ Design
- Honeypot
- Reverse Proxy mit ALF
- Client Firewall (Windows oder Third Party)
- Intelligente Client Firewall (IPS, IDS, Malware, Behaviour Detection)
- Client Firewall Management mit Group Policy
- Auswertung von Firewall Logs

Logging und Monitoring

- Windows Event Logging
- Firewall / Proxy / Router Logs
- Special Log Files
- Baseline Security
- IDS/IPS Analyse Log Files
- Event Log Collection Services
- Archivierung von Logfiles
- Redundante (Read only) Log File Speicherung
- Third Party Monitoring Loesungen fuer Server, Anwendungen und Netzwerk

Organisatorische Massnahmen zur Erhoehung der Sicherheit in IT-Netzwerken

- Ausbildung der Anwender & Administratoren
- Arbeitsanweisungen & Verhaltensanleitungen
- Zutrittskontrolle & Zugangsschutz
- Audits
- Dokumentation
- Steuerung des Remotezugangs von Externen
- Sichere Entsorgung von Firmendaten
- Aendern von Standardkennwoerten / Zugaengen / Konfigurationen von Routern, Switchen, Druckern, Appliances und anderen Geraeten
- Kontrollierte Verbreitung von Firmeninformationen
- Sichere Aufbewahrung von Backups

Technische Sicherheitsfunktionen

- Zugangskontrolle / Zutrittskontrolle
- Ausgangskontrolle
- Pfoertner & Mentor
- Ausweise
- Sicherheitstueren / Sicherheitsschleusen
- Waagen im RZ
- Device Lock fuer mobile Geraete
- Sperren von Wechseldatentraegern
- Data Loss Prevention (DLP)
- Videoueberwachung
- WLAN / Port Security


Fragen?

Kontakt

- **Marc Grote**

- E-Mail: grotem@it-training-grote.de
- Web: http://www.it-training-grote.de
- Blog: http://blog.it-training-grote.de
- XING: https://www.xing.com/profile/Marc_Grote2
- Mobile: 0176/23380279