

Sichere Windows-Infrastrukturen

Das Handbuch für Administratoren

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhalt

Materialien zum Buch	17
Geleitwort des Fachgutachters	19

1 Sichere Windows-Infrastrukturen 21

1.1 Warum Sicherheitsmaßnahmen?	21
1.2 Wer hinterlässt wo Spuren?	22
1.3 Was sollten Sie von den Vorschlägen in diesem Buch umsetzen?	23

2 Angriffsmethoden 25

2.1 Geänderte Angriffsziele oder »Identity is the new perimeter« und »Assume the breach«	25
2.2 Das AIC-Modell	26
2.3 Angriff und Verteidigung	28
2.3.1 Phishing-Attacken	28
2.3.2 Ransomware	32
2.3.3 Kennwörter	34
2.3.4 Angriffe auf das Netzwerk	35
2.3.5 Pass the Hash und Pass the Ticket	37
2.3.6 Angriffe auf Cloud-Dienste	38
2.4 Offline-Angriffe auf das Active Directory	39
2.5 Das Ausnutzen sonstiger Schwachstellen	40

3 Angriffswerkzeuge 41

3.1 Testumgebung	41
3.2 Mimikatz	43
3.2.1 Das Mimikatz-Modul »sekurlsa«	45
3.2.2 Mimikatz und Kerberos	50
3.2.3 Ein Golden Ticket mit Mimikatz erzeugen	51

3.2.4	Silver Tickets und Trust-Tickets	56
3.2.5	Crypto-Modul	57
3.3	DSInternals	58
3.4	PowerSploit	62
3.5	BloodHound	64
3.6	Deathstar	64
3.7	Hashcat und Cain & Abel	64
3.8	Erhöhen der Rechte ohne den Einsatz von Zusatzsoftware	66
3.9	Kali Linux	69

4 Authentifizierungsprotokolle 71

4.1	Domänenauthentifizierungsprotokolle	71
4.1.1	LanManager (LM)	72
4.1.2	NTLM	73
4.1.3	Kerberos	74
4.1.4	Service Principal Names (SPN)	81
4.1.5	Kerberos-Delegierung	85
4.1.6	Kerberos-Richtlinien	87
4.1.7	Kerberos und Vertrauensstellungen	89
4.1.8	Ansprüche (Claims) und Armoring	91
4.1.9	Sicherheitsrichtlinien	93
4.2	Remotenzugriffsprotokolle	94
4.2.1	MS-CHAP	94
4.2.2	Password Authentication Protocol (PAP)	95
4.2.3	Extensible Authentication Protocol (EAP)	95
4.3	Webzugriffsprotokolle	95

5 Ein Namenskonzept planen und umsetzen 97

5.1	Planung	97
5.1.1	Domänennamen	98
5.2	Umsetzung	99
5.2.1	Objekte des Active Directory	99
5.2.2	Hinzufügen von UPN-Suffixen und Aktualisieren der Benutzer	120

6	Das Tier-Modell	125
6.1	Grundlagen eines Tier-Modells	125
6.2	Das Tier-Modell gemäß den Empfehlungen Microsofts	128
6.3	Erweitertes Tier-Modell	131
6.3.1	Rollen- und Rechtematrix	133
6.3.2	Berechtigungen delegieren	137
6.3.3	Ein Skript für das Sammeln der Dienstkonten im Active Directory	151
6.3.4	Ein Skript für das Sammeln der administrativen Konten nach Tier-Level im Active Directory	152
6.3.5	GPOs für das Erzwingen der Anmeldebeschränkung an den Clients und Servern	154
6.3.6	Authentifizierungsrichtliniensilos und deren Richtlinien (Authentication Policies and Silos)	156
6.3.7	Zentrale Services und administrative Berechtigungen mit Sicherheitsgruppen verwalten	163
7	Das Least-Privilege-Prinzip	165
7.1	Allgemeine Punkte zur Vorbereitung des Least-Privilege-Prinzips	166
7.1.1	Notwendige Sicherheitsgruppen für die Umsetzung des Least-Privilege-Prinzips	166
7.2	Werkzeuge für das Ermitteln der Zugriffsrechte	170
7.2.1	ProcMon	170
7.2.2	Process Explorer	173
7.3	Die Umsetzung des Least-Privilege-Prinzips	178
7.3.1	Sicherung der lokalen Berechtigungen auf den Servern und Arbeitsplatzcomputern	178
7.3.2	Sichern von lokal privilegierten AD-Konten	179
7.3.3	Administrationskonten mit RID-500	179
7.3.4	Gruppenrichtlinien zum Einschränken der Berechtigungen auf Domänencontrollern, Servern und Clients	182
7.3.5	Administrative Kennungen im AD sichern	185
7.3.6	Eine Smartcard für die interaktive Anmeldung verwenden	191
7.3.7	SmartCard Authentication Mechanism Assurance	202
7.3.8	Dienstkonten für Anwendungen nutzen	204
7.3.9	Den Besitz aller OUs der Active Directory-Umgebung übernehmen	208

7.3.10	Delegation der Rechte für die Verwaltung der Organisations- einheiten an einem Standort	209
7.4	Sicherheitsgruppen im Active Directory für die lokalen und Rollenadministratoren	213
7.4.1	Ein Gruppenrichtlinienobjekt für das automatische Zuweisen der administrativen Berechtigungen für alle Serverobjekte	217
7.5	Weitere Aspekte nach der Umsetzung	217
7.5.1	Umgang und Aufbewahrung der Datensicherung	218
7.5.2	Ersetzen der verwendeten Dienstknoten durch MSAs bzw. gMSAs ...	218

8 Härten von Benutzer- und Dienstknoten 225

8.1	Tipps für die Kennworterstellung bei Benutzerkonten	225
8.2	Kennworteinstellungen in einer GPO für die normalen Benutzerkennungen	226
8.3	Kennworteinstellungsobjekte (PSOs) für administrative Benutzerkonten	228
8.4	Kennworteinstellungsobjekte für Dienstknoten	229
8.5	Multi-Faktor-Authentifizierung (MFA)	231
8.5.1	Windows Hello	231
8.5.2	Windows Hello for Business	232
8.5.3	Azure MFA	233
8.6	GPO für Benutzerkonten	236
8.7	Berechtigungen der Dienstknoten	238
8.8	Anmeldeberechtigungen der Dienstknoten	239
8.8.1	Interaktive Anmeldeberechtigungen über GPOs	240
8.8.2	Notwendige Berechtigungen der Dienstknoten für die Nutzung geplanter Aufgaben	241

9 Just-in-Time- und Just-Enough-Administration 243

9.1	Just in Time Administration	243
9.1.1	Voraussetzungen und Einrichtung	244
9.1.2	Just in Time Administration verwenden	249
9.1.3	Rechte zum Ändern der Mitglieder einer Gruppe delegieren	253

9.2	Just Enough Administration (JEA)	259
9.2.1	Voraussetzungen	259
9.2.2	Einsatzszenarien und Konfiguration	260

10 Planung und Konfiguration der Verwaltungssysteme (PAWs) 285

10.1	Wo sollten die Verwaltungssysteme (PAWs) eingesetzt werden?	286
10.1.1	Tier-Level 0 (Domainadministration)	286
10.1.2	Tier-Level 1 (zugewiesene Rechte auf den DCs am Standort)	287
10.1.3	Tier-Level 2 (Serversysteme und Serveranwendungen)	287
10.1.4	Tier-Level 3 (Administration der normalen Arbeitsplatzcomputer) ...	288
10.2	Dokumentation der ausgebrachten Verwaltungssysteme	289
10.3	Wie werden die Verwaltungssysteme bereitgestellt?	289
10.4	Zugriff auf die Verwaltungssysteme	290
10.4.1	Restricted Adminmode (eingeschränkter Admin-Modus)	290
10.4.2	Windows Defender Remote Credential Guard	292
10.5	Design der Verwaltungssysteme	294
10.6	Anbindung der Verwaltungssysteme	298
10.7	Bereitstellung von RemoteApps über eine Terminalserver-Farm im Tier-Level 0	301
10.7.1	Bereitstellung einer RemoteApp in einer Terminalserver-Umgebung	301
10.8	Zentralisierte Logs der Verwaltungssysteme	310
10.9	Empfehlung zur Verwendung von Verwaltungssystemen	311

11 Härten der Arbeitsplatzcomputer 313

11.1	Local Administrator Password Solution (LAPS)	313
11.1.1	Schemaerweiterung im Active Directory um die benötigten Attribute	314
11.1.2	Empfohlene Einstellungen in der Gruppenrichtlinie für LAPS	317
11.1.3	Den Computerobjekten die notwendigen Rechte im Active Directory zuweisen	321

11.1.4	Einzelnen Kennungen oder Sicherheitsgruppen lesende Rechte auf die LAPS-Attribute zuweisen	321
11.1.5	Installation der LAPS CSE (Client Side Extension)	322
11.1.6	Ablauf und Funktionsweise der LAPS-CSE	323
11.1.7	Installation der LAPS-GUI auf einem Verwaltungsserver oder einer PAW	324
11.1.8	Verwaltung von LAPS mithilfe der PowerShell	325
11.1.9	Neues PowerShell Modul für LAPS	325
11.1.10	Zukünftige Verschlüsselung der LAPS-Kennwörter im Active Directory	326
11.1.11	Das Zurücksetzen des LAPS-Kennworts bei Neuinstallation und die Wiederherstellung eines Computersystems	326
11.1.12	LAPS-Passwörter exportieren	327
11.1.13	Unsere Empfehlungen für den Einsatz von LAPS	329
11.2	BitLocker	329
11.2.1	Prüfung, ob ein TPM auf dem System vorhanden ist	330
11.2.2	TPM innerhalb einer virtuellen Maschine verfügbar machen	332
11.2.3	BitLocker-Konfiguration per GPO mit einem TPM im System	332
11.2.4	BitLocker für die Systempartition im Dateexplorer aktivieren	334
11.2.5	BitLocker-Konfiguration per GPO ohne ein TPM im System	336
11.2.6	BitLocker auf Windows Servern verfügbar machen	336
11.2.7	Den BitLocker-Verschlüsselungsschutz anhalten	337
11.2.8	Den BitLocker-Wiederherstellungsschlüssel aus dem Active Directory auslesen	338
11.2.9	BitLocker mit der PowerShell oder der Eingabeaufforderung verwalten	342
11.3	Mitglieder in den lokalen administrativen Sicherheitsgruppen verwalten	343
11.4	Weitere Einstellungen: Startmenü und vorinstallierte Apps anpassen, OneDrive deinstallieren und Cortana deaktivieren	344
11.4.1	Das Startmenü anpassen	344
11.4.2	Vorinstallierte Anwendungen entfernen	345
11.4.3	OneDrive deinstallieren	347
11.4.4	Cortana per GPO deaktivieren	348
11.4.5	Cortana per Registry deaktivieren	349
11.4.6	Edge über eine Gruppenrichtlinie konfigurieren	349
11.5	Härtung durch Gruppenrichtlinien	352
11.5.1	Gruppenrichtlinien aus dem Microsoft Security Compliance Toolkit	352
11.5.2	Unsere Empfehlungen für domänenweite Gruppenrichtlinien	354

11.5.3	Unsere Empfehlungen für Gruppenrichtlinien der Computerobjekte	364
11.5.4	Software Restriction Policies (Richtlinie für Software-einschränkungen)	368
11.5.5	AppLocker	369

12 Härten der administrativen Systeme 383

12.1	Gruppenrichtlinieneinstellungen für alle PAWs	383
12.1.1	Die GPO »0-CBP-AdminClient-Administrative Vorlagen«	383
12.1.2	Die GPO »0-CBP-AdminClient-Benutzerrechte«	387
12.1.3	Die GPO »0-CBP-AdminClient-Sicherheitsoptionen«	388
12.2	Administrative Berechtigungen auf den administrativen Systemen	389
12.2.1	Verwalten der Sicherheitsgruppen	390
12.2.2	Lokale Sicherheitsrichtlinie	391
12.3	Verwaltung der administrativen Systeme	392
12.3.1	Das Clean-Source-Prinzip	392
12.4	Firewall-Einstellungen	395
12.5	IPSec-Kommunikation	397
12.5.1	IPSec-Kommunikation auf Basis eines Pre-shared Keys	398
12.5.2	IPSec-Kommunikation auf Basis eines Zertifikats, das von einer Unternehmens-CA ausgestellt wurde	406
12.5.3	Hinweise zur Verwendung einer IPSec-Verbindung zwischen Domänencontrollern	408
12.5.4	Erweitertes Auditing mithilfe von Auditpol.exe	409
12.6	AppLocker-Einstellungen auf den administrativen Systemen	410
12.7	Windows Defender Credential Guard	412

13 Update-Management 417

13.1	Installation der Updates auf Standalone-Clients oder in kleinen Unternehmen ohne Active Directory	417
13.1.1	»Windows Update-Einstellungen« über die integrierte GUI	418
13.1.2	»Windows Update-Einstellungen« über eine Gruppenrichtlinie	419
13.2	Updates mit dem WSUS-Server verwalten	421
13.2.1	Installation der Rolle »WSUS-Server«	421

13.2.2	Konfiguration der Rolle »WSUS-Server«	424
13.2.3	Die WSUS-Datenbank mit dem SQL Server Management Studio optimieren	435
13.2.4	Aufbau einer WSUS-Struktur in einer großen Infrastruktur	438
13.2.5	WSUS-Server durch Nutzung von Zertifikaten absichern	440
13.2.6	Verwaltung des WSUS-Servers mit der PowerShell und wsusutil.exe	443
13.2.7	Troubleshooting	446
13.3	Application Lifecycle Management	451
13.3.1	Support-Phasen in Windows 7	452
13.3.2	Support-Phasen in Windows 10 und Windows 11	455
13.3.3	Support-Phasen in Windows Server 2019 und Windows Server 2022	457
14	Der administrative Forest	459
14.1	Was ist ein Admin-Forest?	459
14.2	Einrichten eines Admin-Forests	462
14.2.1	DNS-Namensauflösung	463
14.2.2	Vertrauensstellung	470
14.2.3	Berechtigungen	486
14.3	Privilege Access Management-Trust (PAM-Trust)	489
14.3.1	ShadowPrincipals vorbereiten	490
14.3.2	Verwendung der ShadowPrincipals	497
14.4	Verwaltung und Troubleshooting	501
14.4.1	NRPT (Name Resolution Policy Table)	501
14.4.2	Break-Glass-Konten	503
14.4.3	Probleme mit der Authentifizierungsfirewall	503
15	Härtung des Active Directory	507
15.1	Schützenswerte Objekte	507
15.1.1	Built-in-Gruppen	507
15.1.2	AdminCount	516

15.2	Das Active Directory-Schema und die Rechte im Schema	522
15.3	Kerberos-Reset (krbtgt) und Kerberoasting	524
15.4	Sinnvolles OU-Design für die AD-Umgebung	528
16	Netzwerkzugänge absichern	531
16.1	VPN-Zugang	532
16.1.1	VPN-Protokolle	553
16.1.2	Konfiguration des VPN-Servers	557
16.1.3	Konfiguration der Clientverbindungen	558
16.1.4	Troubleshooting	561
16.2	DirectAccess einrichten	563
16.2.1	Bereitstellen der Infrastruktur	565
16.2.2	Tunnelprotokolle für DirectAccess	568
16.3	NAT einrichten	568
16.4	Der Netzwerkrichtlinienserver	572
16.4.1	Einrichtung und Protokolle	574
16.4.2	RADIUS-Proxy-Server	581
16.4.3	Das Regelwerk für den Zugriff einrichten	583
16.4.4	Protokollierung und Überwachung	587
16.5	Den Netzwerkzugriff absichern	591
16.5.1	Konfiguration der Clients	592
16.5.2	Konfiguration der Switches	596
16.5.3	Konfiguration des NPS	600
16.5.4	Protokollierung und Troubleshooting	606
16.5.5	Allgemeine Überlegungen zur Verwendung der Authentifizierungsmethoden	609
16.6	Absichern des Zugriffs auf Netzwerkgeräte über das RADIUS-Protokoll ...	610
16.6.1	RADIUS-Server für die Authentifizierung konfigurieren	611
16.6.2	Definition des RADIUS-Clients	613
16.6.3	Sicherheitsgruppen erstellen	617

17 PKI und Zertifizierungsstellen 625

17.1	Was ist eine PKI?	625
17.1.1	Zertifikate	626
17.1.2	Verschlüsselung und Signatur	627
17.2	Aufbau einer CA-Infrastruktur	633
17.2.1	Installation der Rolle	641
17.2.2	Alleinstehende »Offline«-Root-CA	646
17.2.3	Untergeordnete Zertifizierungsstelle als »Online«-Sub-CA	663
17.3	Zertifikate verteilen und verwenden	670
17.3.1	Verteilen von Zertifikaten an Clients	671
17.3.2	Remotedesktopdienste	672
17.3.3	Webserver	675
17.3.4	Clients	679
17.3.5	Codesignatur	679
17.4	Überwachung und Troubleshooting der Zertifikatdienste	684
17.5	Bevorstehende Änderungen und aktuelle Herausforderungen mit einer Microsoft-Zertifizierungsstelle	689
17.5.1	Besserer Schutz für Clientauthentifizierungszertifikate	689
17.5.2	Schutz vor PetitPotam	691

18 Sicherer Betrieb 693

18.1	AD-Papierkorb	693
18.2	Umleiten der Standard-OUs für Computer und Benutzer	699
18.3	Mögliche Probleme beim Prestaging	700
18.4	Sichere Datensicherung	701
18.4.1	Das iSCSI-Target konfigurieren	702
18.4.2	Das iSCSI-Laufwerk einbinden	704
18.4.3	BitLocker einrichten	707
18.4.4	Die Datensicherung einrichten	712
18.4.5	Zugriff auf die gesicherten Daten	713
18.5	Die Sicherheitsbezeichner (SIDs) dokumentieren	715

19 Auditing	717
19.1 Die Ereignisanzeige	717
19.1.1 Eventlog und PowerShell	722
19.1.2 Eigene Quellen registrieren	723
19.1.3 Das Eventlog über das Windows Admin Center nutzen	724
19.2 Logs zentral sammeln und archivieren	725
19.2.1 Die Logs sichern	725
19.2.2 Eventlog-Forwarding	726
19.3 Konfiguration der Überwachungsrichtlinien	735
19.3.1 Objekte löschen	735
19.3.2 Gruppen manipulieren	739
19.3.3 Konten sperren	740
19.4 DNS-Logging	744
20 Reporting und Erkennen von Angriffen	749
20.1 Azure ATP und ATA	749
20.1.1 Azure Advanced Threat Protection (Azure ATP)	749
20.1.2 Advanced Threat Analytics (ATA)	751
20.2 PowerShell-Reporting	754
20.2.1 Den Status der Systeme prüfen	755
20.2.2 Die Einhaltung der Namenskonventionen prüfen	765
20.3 Desired State Configuration	767
21 Disaster Recovery	773
21.1 Disaster Recovery planen	773
21.2 Forest Recovery	777
21.3 Die Gruppenrichtlinien-Infrastruktur wiederherstellen	778
21.4 Snapshots verwenden	780
21.5 Das DC-Computerpasswort ist »out-of-sync«	782

22 Praktische Implementierung der Sicherheitsmaßnahmen 785

22.1 Bestandsanalyse 785

22.2 Welche Maßnahmen sind für mich geeignet bzw. wie aufwendig ist die Umsetzung? 790

22.2.1 Rollen- und Rechtekonzept 790

22.2.2 Namenskonzept 791

22.2.3 Tier-Modell 791

22.2.4 PAW 793

22.2.5 DC-Härtung 794

22.2.6 Systemhärtung 794

22.2.7 Kennwortrichtlinie (Admins) 795

22.2.8 Kennwortrichtlinie (Dienstkonten) 795

22.2.9 Netzwerkverschlüsselung (IPSec) 796

22.2.10 802.1x 797

22.2.11 Least Privilege 797

22.2.12 Auditing 798

22.2.13 Eventlog-Forwarding 798

22.2.14 AD ACL Scanner (Compliance) 799

22.2.15 Compliance Reporting 799

22.2.16 Admin Forest 799

22.2.17 Clean Source 799

22.2.18 Datensicherung 800

22.3 Wie fange ich an? 800

Index 803

Materialien zum Buch

Auf der Webseite zu diesem Buch stehen folgende Materialien für Sie zum Download bereit:

- ▶ **Skriptbeispiele**
- ▶ **Detaillierte GPO-Vorlagen**

Viele der Skriptbeispiele sind ziemlich komplex. Wir haben bei der Darstellung im Buch auf gute Lesbarkeit geachtet und Umbrüche eingefügt. Auch bei den Vorschlägen für die Gruppenrichtlinien werden oft nur die relevanten Ausschnitte gezeigt oder ein Überblick gegeben. Wenn Sie die Skripte und GPOs im Detail studieren wollen und sie ausprobieren möchten, nutzen Sie am besten das Download-Material, das wir vorbereitet haben.

Gehen Sie dazu auf www.rheinwerk-verlag.de/5612. Klicken Sie auf den Reiter MATERIALIEN. Sie sehen die herunterladbaren Dateien samt einer Kurzbeschreibung des Dateiinhalts. Klicken Sie auf den Button HERUNTERLADEN, um den Download zu starten. Je nach Größe der Datei (und Ihrer Internetverbindung) kann es einige Zeit dauern, bis der Download abgeschlossen ist.