

# Auf einen Blick

1	Sichere Windows-Infrastrukturen .....	19
2	Angriffsmethoden .....	23
3	Angriffswerkzeuge .....	41
4	Authentifizierungsprotokolle .....	71
5	Ein Namenskonzept planen und umsetzen .....	97
6	Das Tier-Modell .....	125
7	Das Least-Privilege-Prinzip .....	163
8	Härten von Benutzer- und Dienstkonten .....	219
9	Just-in-Time- und Just-Enough-Administration .....	237
10	Planung und Konfiguration der Verwaltungssysteme (PAWs) .....	277
11	Härten der Arbeitsplatzcomputer .....	305
12	Härten der administrativen Systeme .....	369
13	Update-Management .....	403
14	Administrativer Forest .....	445
15	Härtung des Active Directory .....	493
16	Netzwerkzugänge absichern .....	517
17	PKI und Zertifizierungsstellen .....	609
18	Sicherer Betrieb .....	675
19	Auditing .....	701
20	Reporting und Erkennen von Angriffen .....	731

# Inhalt

Materialien zum Buch .....	15
Geleitwort des Fachgutachters .....	17

## **1 Sichere Windows-Infrastrukturen** 19

---

<b>1.1 Warum Sicherheitsmaßnahmen?</b> .....	19
<b>1.2 Wer hinterlässt wo Spuren?</b> .....	20
<b>1.3 Was sollten Sie von den Vorschlägen in diesem Buch umsetzen?</b> .....	20

## **2 Angriffsmethoden** 23

---

<b>2.1 Geänderte Angriffsziele oder »Identity is the new perimeter« und »Assume the breach«</b> .....	23
<b>2.2 Das AIC-Modell</b> .....	24
<b>2.3 Angriff und Verteidigung</b> .....	26
2.3.1 Phishing-Attacken .....	26
2.3.2 Ransomware .....	31
2.3.3 Kennwörter .....	33
2.3.4 Angriffe auf das Netzwerk .....	33
2.3.5 Pass the Hash und Pass the Ticket .....	36
2.3.6 Angriffe auf Cloud-Dienste .....	37
<b>2.4 Offline-Angriffe auf das Active Directory</b> .....	38
<b>2.5 Das Ausnutzen sonstiger Schwachstellen</b> .....	38

## **3 Angriffswerkzeuge** 41

---

<b>3.1 Testumgebung</b> .....	41
<b>3.2 Mimikatz</b> .....	43
3.2.1 Das Mimikatz-Modul »sekurlsa« .....	45
3.2.2 Mimikatz und Kerberos .....	49
3.2.3 Ein Golden Ticket mit Mimikatz erzeugen .....	51

3.2.4	Silver Ticket und Trust-Ticket .....	55
3.2.5	Crypto-Modul .....	56
<b>3.3</b>	<b>DSInternals</b> .....	58
<b>3.4</b>	<b>PowerSploit</b> .....	61
<b>3.5</b>	<b>BloodHound</b> .....	63
<b>3.6</b>	<b>Deathstar</b> .....	63
<b>3.7</b>	<b>Hashcat und Cain &amp; Abel</b> .....	63
<b>3.8</b>	<b>Erhöhen der Rechte ohne den Einsatz von Zusatzsoftware</b> .....	65
<b>3.9</b>	<b>Kali Linux</b> .....	68
<b>4</b>	<b>Authentifizierungsprotokolle</b> .....	71
<hr/>		
<b>4.1</b>	<b>Domänenauthentifizierungsprotokolle</b> .....	71
4.1.1	LanManager (LM) .....	72
4.1.2	NTLM .....	73
4.1.3	Kerberos .....	74
4.1.4	Service Principal Names (SPN) .....	82
4.1.5	Kerberos-Delegierung .....	85
4.1.6	Kerberos-Richtlinien .....	88
4.1.7	Kerberos und Vertrauensstellungen .....	89
4.1.8	Ansprüche (Claims) und Armoring .....	91
4.1.9	Sicherheitsrichtlinien .....	94
<b>4.2</b>	<b>Remotезugriffsprotokolle</b> .....	95
4.2.1	MS-CHAP .....	95
4.2.2	Password Authentication Protocol (PAP) .....	95
4.2.3	Extensible Authentication Protocol (EAP) .....	95
<b>4.3</b>	<b>Webzugriffsprotokolle</b> .....	96
<b>5</b>	<b>Ein Namenskonzept planen und umsetzen</b> .....	97
<hr/>		
<b>5.1</b>	<b>Planung</b> .....	97
5.1.1	Domännennamen .....	98
<b>5.2</b>	<b>Umsetzung</b> .....	99
5.2.1	Objekte des Active Directory .....	99
5.2.2	Hinzufügen von UPN-Suffixen und Aktualisieren der Benutzer .....	120

<b>6</b>	<b>Das Tier-Modell</b>	125
<b>6.1</b>	<b>Grundlagen eines Tier-Modells</b>	125
<b>6.2</b>	<b>Das Tier-Modell gemäß den Empfehlungen Microsofts</b>	128
<b>6.3</b>	<b>Erweitertes Tier-Modell</b>	131
6.3.1	Rollen- und Rechtematrix	133
6.3.2	Berechtigungen delegieren	136
6.3.3	Skripte für das Sammeln der Dienstkonten im AD	151
6.3.4	GPO für das Erzwingen der Anmeldebeschränkung an den Clients und Servern	152
6.3.5	Authentifizierungsrichtliniensilos und deren Richtlinien (Authentication Policies and Silos)	154
<b>7</b>	<b>Das Least-Privilege-Prinzip</b>	163
<b>7.1</b>	<b>Allgemeine Punkte zur Vorbereitung des Least-Privilege-Prinzips</b>	164
7.1.1	Notwendige Sicherheitsgruppen für die Umsetzung des Least-Privilege-Prinzips	164
<b>7.2</b>	<b>Werkzeuge für das Ermitteln der Zugriffsrechte</b>	168
7.2.1	ProcMon	168
7.2.2	Process Explorer	171
<b>7.3</b>	<b>Die Umsetzung des Least-Privilege-Prinzips</b>	176
7.3.1	Sicherung der lokalen Berechtigungen auf den Servern und Arbeitsplatzcomputern	176
7.3.2	Sichern von lokal privilegierten AD-Konten	177
7.3.3	Administrationskonten mit RID-500	177
7.3.4	Gruppenrichtlinien zum Einschränken der Berechtigungen auf Domänencontrollern, Servern und Clients	180
7.3.5	Administrative Kennungen im AD sichern	183
7.3.6	Eine Smartcard für die interaktive Anmeldung verwenden	189
7.3.7	SmartCard Authentication Mechanism Assurance	200
7.3.8	Dienstkonten für Anwendungen nutzen	202
7.3.9	Den Besitz aller OUs der Active Directory-Umgebung übernehmen	206
7.3.10	Delegation der Rechte für die Verwaltung der Organisationseinheiten an einem Standort	207
<b>7.4</b>	<b>Weitere Aspekte nach der Umsetzung</b>	211
7.4.1	Umgang und Aufbewahrung der Datensicherung	212
7.4.2	Ersetzen der verwendeten Dienstkonten durch MSAs bzw. gMSAs	212

<b>8</b>	<b>Härten von Benutzer- und Dienstkonten</b>	219
<hr/>		
8.1	Tipps für die Kennwörterstellung bei Benutzerkonten .....	219
8.2	Kennworteinstellungen in einer GPO für die normalen Benutzerkennungen .....	220
8.3	Kennworteinstellungsobjekte (PSO) für administrative Benutzerkonten .....	222
8.4	Kennworteinstellungsobjekte für Dienstkonten .....	223
8.5	<b>Multi-Faktor-Authentifizierung (MFA)</b> .....	225
8.5.1	Windows Hello .....	225
8.5.2	Windows Hello for Business .....	227
8.5.3	Azure MFA .....	227
8.6	GPO für Benutzerkonten .....	230
8.7	Berechtigungen der Dienstkonten .....	232
8.8	<b>Anmeldeberechtigungen der Dienstkonten</b> .....	233
8.8.1	Interaktive Anmeldeberechtigungen über GPOs .....	234
8.8.2	Notwendige Berechtigungen der Dienstkonten für die Nutzung geplanter Aufgaben .....	235
<b>9</b>	<b>Just-in-Time- und Just-Enough-Administration</b>	237
<hr/>		
9.1	<b>Just in Time Administration</b> .....	237
9.1.1	Voraussetzungen und Einrichtung .....	238
9.1.2	Just in Time Administration verwenden .....	243
9.1.3	Rechte zum Ändern der Mitglieder einer Gruppe delegieren .....	247
9.2	<b>Just Enough Administration (JEA)</b> .....	252
9.2.1	Voraussetzungen .....	252
9.2.2	Einsatzszenarien und Konfiguration .....	253
<b>10</b>	<b>Planung und Konfiguration der Verwaltungssysteme (PAWs)</b>	277
<hr/>		
10.1	<b>Wo sollten die Verwaltungssysteme (PAWs) eingesetzt werden?</b> .....	278
10.1.1	Tier-Level 0 (Domainadministration) .....	278
10.1.2	Tier-Level 1 (zugewiesene Rechte auf den DCs am Standort) .....	279

10.1.3	Tier-Level 2 (Serversysteme und Serveranwendungen) .....	279
10.1.4	Tier-Level 3 (Administration der normalen Arbeitsplatzcomputer) ...	280
<b>10.2</b>	<b>Dokumentation der ausgebrachten Verwaltungssysteme</b> .....	<b>281</b>
<b>10.3</b>	<b>Wie werden die Verwaltungssysteme bereitgestellt?</b> .....	<b>281</b>
<b>10.4</b>	<b>Zugriff auf die Verwaltungssysteme</b> .....	<b>282</b>
10.4.1	Restricted Adminmode (eingeschränkter Admin-Modus) .....	282
10.4.2	Windows Defender Remote Credential Guard .....	284
<b>10.5</b>	<b>Design der Verwaltungssysteme</b> .....	<b>286</b>
<b>10.6</b>	<b>Anbindung der Verwaltungssysteme</b> .....	<b>290</b>
<b>10.7</b>	<b>Bereitstellung von RemoteApps über eine Terminalserver-Farm im Tier-Level 0</b> .....	<b>293</b>
10.7.1	Bereitstellung einer RemoteApp in einer Terminalserver-Umgebung .....	293
<b>10.8</b>	<b>Zentralisierte Logs der Verwaltungssysteme</b> .....	<b>303</b>
<b>10.9</b>	<b>Empfehlung zu Verwendung von Verwaltungssystemen</b> .....	<b>303</b>
<b>11</b>	<b>Härten der Arbeitsplatzcomputer</b> .....	<b>305</b>
<b>11.1</b>	<b>Local Administrator Password Solution (LAPS)</b> .....	<b>305</b>
11.1.1	Das Schema im Active Directory um die benötigten Attribute erweitern .....	306
11.1.2	Empfohlene Einstellungen in der Gruppenrichtlinie für LAPS .....	308
11.1.3	Den Computerobjekten die notwendigen Rechte im Active Directory zuweisen .....	312
11.1.4	Einzelnen Kennungen oder Sicherheitsgruppen lesende Rechte auf die LAPS-Attribute zuweisen .....	312
11.1.5	Installation der LAPS CSE (Client Side Extension) .....	313
11.1.6	Ablauf und Funktionsweise der LAPS-CSE .....	314
11.1.7	Installation der LAPS-GUI auf einem Verwaltungsserver oder einer PAW .....	315
11.1.8	Verwaltung von LAPS mithilfe der PowerShell .....	316
11.1.9	Unsere Empfehlungen für den Einsatz von LAPS .....	316
<b>11.2</b>	<b>BitLocker</b> .....	<b>317</b>
11.2.1	Prüfung, ob ein TPM auf dem System vorhanden ist .....	318
11.2.2	TPM innerhalb einer virtuellen Maschine verfügbar machen .....	319
11.2.3	BitLocker-Konfiguration per GPO mit einem TPM im System .....	320
11.2.4	BitLocker für die Systempartition im Date Explorer aktivieren .....	322

11.2.5	BitLocker-Konfiguration per GPO ohne ein TPM im System .....	324
11.2.6	BitLocker auf Windows Servern verfügbar machen .....	324
11.2.7	Den BitLocker-Wiederherstellungsschlüssel aus dem Active Directory auslesen .....	325
11.2.8	BitLocker mit der PowerShell oder der Eingabeaufforderung verwalten .....	328
<b>11.3</b>	<b>Mitglieder in den lokalen administrativen Sicherheitsgruppen verwalten .....</b>	<b>329</b>
<b>11.4</b>	<b>Weitere Einstellungen: Startmenü und vorinstallierte Apps anpassen, OneDrive deinstallieren und Cortana deaktivieren .....</b>	<b>330</b>
11.4.1	Das Startmenü anpassen .....	330
11.4.2	Vorinstallierte Anwendungen entfernen .....	331
11.4.3	OneDrive deinstallieren .....	333
11.4.4	Cortana per GPO deaktivieren .....	334
11.4.5	Cortana per Registry deaktivieren .....	335
11.4.6	Edge über eine Gruppenrichtlinie konfigurieren .....	335
<b>11.5</b>	<b>Härtung durch Gruppenrichtlinien .....</b>	<b>338</b>
11.5.1	Gruppenrichtlinien aus dem Microsoft Security Compliance Toolkit .....	338
11.5.2	Unsere Empfehlungen für domänenweite Gruppenrichtlinien .....	340
11.5.3	Unsere Empfehlungen für Gruppenrichtlinien der Computerobjekte .....	350
11.5.4	Software Restriction Policies (Richtlinie für Softwareeinschränkungen) .....	354
11.5.5	AppLocker .....	355
<b>12</b>	<b>Härten der administrativen Systeme .....</b>	<b>369</b>
<b>12.1</b>	<b>Gruppenrichtlinieneinstellung für alle PAWs .....</b>	<b>369</b>
12.1.1	Die GPO »0-CBP-AdminClient-Administrative Vorlagen« .....	369
12.1.2	Die GPO »0-CBP-AdminClient-Benutzerrechte« .....	373
12.1.3	Die GPO »0-CBP-AdminClient-Sicherheitsoptionen« .....	374
<b>12.2</b>	<b>Administrative Berechtigungen auf den administrativen Systemen .....</b>	<b>375</b>
12.2.1	Verwalten der Sicherheitsgruppen .....	376
12.2.2	Lokale Sicherheitsrichtlinie .....	377
<b>12.3</b>	<b>Verwaltung der administrativen Systeme .....</b>	<b>377</b>
12.3.1	Das Clean-Source-Prinzip .....	378
<b>12.4</b>	<b>Firewall-Einstellungen .....</b>	<b>381</b>

<b>12.5 IPSec-Kommunikation</b> .....	383
12.5.1 IPSec-Kommunikation auf Basis eines Pre-shared Keys .....	384
12.5.2 IPSec-Kommunikation auf Basis eines Zertifikats, das von einer Unternehmens-CA ausgestellt wurde .....	392
12.5.3 Hinweise zur Verwendung einer IPSec-Verbindung zwischen Domänencontrollern .....	394
12.5.4 Erweitertes Auditing mithilfe von Auditpool.exe .....	395
<b>12.6 AppLocker-Einstellungen auf den administrativen Systemen</b> .....	396
<b>12.7 Windows Defender Credential Guard</b> .....	398

## **13 Update-Management** 403

---

<b>13.1 Installation der Updates auf Standalone-Clients oder in kleinen Unternehmen ohne Active Directory</b> .....	403
13.1.1 »Windows Update-Einstellungen« über die integrierte GUI .....	404
13.1.2 »Windows Update-Einstellungen« über eine Gruppenrichtlinie .....	405
<b>13.2 Updates mit dem WSUS-Server verwalten</b> .....	407
13.2.1 Installation der Rolle »WSUS-Server« .....	407
13.2.2 Konfiguration der Rolle »WSUS-Server« .....	410
13.2.3 Die WSUS-Datenbank mit dem SQL Server Management Studio optimieren .....	421
13.2.4 Aufbau einer WSUS-Struktur in einer großen Infrastruktur .....	424
13.2.5 WSUS-Server durch Nutzung von Zertifikaten absichern .....	426
13.2.6 Verwaltung des WSUS-Servers mit der PowerShell und wsusutil.exe .....	429
13.2.7 Troubleshooting .....	432
<b>13.3 Application Lifecycle Management</b> .....	437
13.3.1 Support-Phasen in Windows 7 .....	438
13.3.2 Support-Phasen in Windows 10 .....	441
13.3.3 Support-Phasen in Windows Server 2019 .....	442

## **14 Administrativer Forest** 445

---

<b>14.1 Was ist ein Admin-Forest?</b> .....	445
<b>14.2 Einrichten eines Admin-Forests</b> .....	448
14.2.1 DNS-Namensauflösung einrichten .....	449



14.2.2	Vertrauensstellung einrichten .....	456
14.2.3	Berechtigungen einrichten .....	472
<b>14.3</b>	<b>Privilege Access Management-Trust (PAM-Trust)</b> .....	<b>476</b>
14.3.1	ShadowPrincipals vorbereiten .....	477
14.3.2	Verwendung der ShadowPrincipals .....	483
<b>14.4</b>	<b>Verwaltung und Troubleshooting</b> .....	<b>487</b>
14.4.1	NRPT (Name Resolution Policy Table) .....	487
14.4.2	Break-Glass-Konten .....	489
14.4.3	Probleme mit der Authentifizierungsfirewall .....	489

## **15 Härtung des Active Directory** 493

---

<b>15.1</b>	<b>Schützenswerte Objekte</b> .....	<b>493</b>
15.1.1	Built-in-Gruppen .....	493
15.1.2	AdminCount .....	503
<b>15.2</b>	<b>Das Active Directory-Schema und die Rechte im Schema</b> .....	<b>509</b>
<b>15.3</b>	<b>Kerberos Reset (krbtgt) und Kerberoasting</b> .....	<b>511</b>
<b>15.4</b>	<b>Sinnvolles OU-Design für die AD-Umgebung</b> .....	<b>515</b>

## **16 Netzwerkzugänge absichern** 517

---

<b>16.1</b>	<b>VPN-Zugang</b> .....	<b>518</b>
16.1.1	VPN-Protokolle .....	539
16.1.2	Konfiguration des VPN-Servers .....	543
16.1.3	Konfiguration der Clientverbindungen .....	544
16.1.4	Troubleshooting .....	547
<b>16.2</b>	<b>DirectAccess einrichten</b> .....	<b>549</b>
16.2.1	Bereitstellen der Infrastruktur .....	551
16.2.2	Tunnelprotokolle für DirectAccess .....	554
<b>16.3</b>	<b>NAT einrichten</b> .....	<b>554</b>
<b>16.4</b>	<b>Netzwerkrichtlinienserver</b> .....	<b>558</b>
16.4.1	Einrichtung und Protokolle .....	561
16.4.2	RADIUS-Proxy-Server .....	568
16.4.3	Das Regelwerk für den Zugriff einrichten .....	570
16.4.4	Protokollierung und Überwachung .....	574

<b>16.5 Den Netzwerkzugriff absichern</b> .....	578
16.5.1 Konfiguration der Clients .....	578
16.5.2 Konfiguration der Switches .....	583
16.5.3 Konfiguration des NPS .....	587
16.5.4 Protokollierung und Troubleshooting .....	592
<b>16.6 Absichern des Zugriffs auf Netzwerkgeräte über das RADIUS-Protokoll</b> .....	595
16.6.1 RADIUS-Server für die Authentifizierung konfigurieren .....	596
16.6.2 Definition des RADIUS-Clients .....	599
16.6.3 Sicherheitsgruppen erstellen .....	603
<b>17 PKI und Zertifizierungsstellen</b> .....	609
<hr/>	
<b>17.1 Was ist eine PKI?</b> .....	609
17.1.1 Zertifikate .....	610
17.1.2 Verschlüsselung und Signatur .....	611
<b>17.2 Aufbau einer CA-Infrastruktur</b> .....	617
17.2.1 Installation der Rolle .....	625
17.2.2 Alleinstehende »Offline« Root-CA .....	630
17.2.3 Untergeordnete Zertifizierungsstelle als »Online«-Sub-CA .....	648
<b>17.3 Zertifikate verteilen und verwenden</b> .....	654
17.3.1 Verteilen von Zertifikaten an »Clients« .....	655
17.3.2 Remotedesktopdienste .....	657
17.3.3 Webserver .....	660
17.3.4 Clients .....	664
17.3.5 Codesignatur .....	665
<b>17.4 Überwachung und Troubleshooting der Zertifikatdienste</b> .....	669
<b>18 Sicherer Betrieb</b> .....	675
<hr/>	
<b>18.1 AD-Papierkorb</b> .....	675
<b>18.2 Umleiten der Standard-OUs für Computer und Benutzer</b> .....	681
<b>18.3 Mögliche Probleme beim Prestaging</b> .....	682
<b>18.4 Sichere Datensicherung</b> .....	683
18.4.1 Konfiguration des iSCSI-Targets .....	684
18.4.2 iSCSI-Laufwerk einbinden .....	687

18.4.3	Einrichten von BitLocker .....	689
18.4.4	Datensicherung einrichten .....	694
18.4.5	Zugriff auf die gesicherten Daten .....	696
<b>18.5</b>	<b>Disaster Recovery .....</b>	<b>697</b>

## **19 Auditing** 701

---

<b>19.1</b>	<b>Die Ereignisanzeige .....</b>	<b>701</b>
19.1.1	Eventlog und PowerShell .....	706
19.1.2	Eigene Quellen registrieren .....	707
19.1.3	Eventlog über das Windows Admin Center .....	708
<b>19.2</b>	<b>Logs zentral sammeln und archivieren .....</b>	<b>709</b>
19.2.1	Die Logs sichern .....	709
19.2.2	Eventlog-Forwarding .....	710
<b>19.3</b>	<b>Konfiguration der Überwachungsrichtlinien .....</b>	<b>717</b>
19.3.1	Löschen von Objekten .....	718
19.3.2	Manipulation von Gruppen .....	722
19.3.3	Konten sperren .....	723
<b>19.4</b>	<b>DNS-Logging .....</b>	<b>725</b>

## **20 Reporting und Erkennen von Angriffen** 731

---

<b>20.1</b>	<b>Azure ATP und ATA .....</b>	<b>731</b>
20.1.1	Azure Advanced Threat Protection (Azure ATP) .....	731
20.1.2	Advanced Threat Analytics (ATA) .....	733
<b>20.2</b>	<b>PowerShell-Reporting .....</b>	<b>736</b>
20.2.1	Den Status der Systeme prüfen .....	737
20.2.2	Die Einhaltung der Namenskonventionen prüfen .....	747
<b>20.3</b>	<b>Desired State Configuration .....</b>	<b>749</b>

Index .....	755
-------------	-----