

Inhaltsverzeichnis

Vorwort	1
Kurzfassung	2
Erklärung	2
1 Einleitung	3
1.1 Abgrenzung	4
1.2 Aufbau des Ratgebers	4
2 Softwareverteilung	5
2.1 Begriffsbestimmungen	5
2.2 Architekturen	8
2.3 Verteilungsstrategien	9
3 IT-Sicherheitsaspekte: Gefährdungslage und Maßnahmen	11
3.1 Begriffsbestimmungen	12
3.1.1 Theoretische und effektive Sicherheit	12
3.1.2 Ursachen von IT-Sicherheitsproblemen	12
3.1.3 Angriffstypen	13
3.1.4 Angreifertypen	14
3.1.5 Angriffsoberfläche	15
3.2 Sicherheitsaspekte bei der Administration	16
3.2.1 Administrationswerkzeuge	16
3.2.2 Administratoren	17
3.3 Protokollierung und Überwachung	21
3.4 Systemkonfiguration	25
3.5 Sicherheitsaspekte beim Outsourcing	26
3.6 Sicherheitsaspekte bei der Softwareverteilung	28
4 Softwareverteilung mittels Microsoft SCCM	30
4.1 Überblick über Microsoft SCCM	30
4.2 Einsatz von Microsoft SCCM über Domänengrenzen hinweg	31
4.2.1 Exkurs: Vertrauensbeziehungen zwischen Active-Directory-Domänen	32
4.2.2 Microsoft SCCM in Cross-Forest-Trust-Szenarien	34
4.3 Sicherheitsaspekte von Cross Forest Trust bei domänenübergreifendem SCCM	35
4.3.1 Zugriffsrechte von Administratoren auf mehrere Domänen	35
4.3.2 Zugriffsrechte auf alle freigegebenen Ressourcen innerhalb einer Domäne	36
4.3.3 Vertrauen in den Administrator des vertrauten Forest	36

5 Kriterienkatalog für sichere Softwareverteilung	38
5.1 Kriterien für die Administration	38
5.2 Kriterien für die Protokollierung und Überwachung	42
5.3 Kriterien für die Systemkonfiguration	43
5.4 Kriterien für das Outsourcing	45
5.5 Kriterien für die sichere Softwareverteilung	47
5.6 Kriterien bezüglich Microsoft SCCM, Active Directory und Cross Forest Trust	48
6 Fazit	56
Abkürzungen	57
Literaturverzeichnis	58