Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

RATGEBER FÜR EINE SICHERE ZENTRALE SOFTWAREVERTEILUNG

08/2017

FRAUNHOFER VERLAG

Fraunhofer SIT

Ratgeber für eine sichere zentrale Softwareverteilung

Michael Herfert, Thomas Kunz, Ruben Wolf

31. August 2017

Fraunhofer-Institut für
Sichere Informationstechnologie
Rheinstraße 75
64295 Darmstadt

FRAUNHOFER VERLAG

Der vorliegende Ratgeber wurde vom Fraunhofer-Institut für Sichere Informationstechnologie im Zeitraum von September 2016 bis Februar 2017 erstellt.

Die Erstellung wurde durch das Land Hessen, vertreten durch das Hessische Ministerium des Inneren und für Sport, gefördert.

HESSEN

Impressum

Kontaktadresse:
Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Telefon 06151 869-213
Telefax 06151 869-224
E-Mail info@sit.fraunhofer.de
URL www.sit.fraunhofer.de

Hrsg. Michael Waidner
Ratgeber für eine sichere zentrale Softwareverteilung
Michael Herfert, Thomas Kunz, Ruben Wolf
August 2017

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.
ISBN: 978-3-8396-1240-8

Druck und Weiterverarbeitung:
ESSER printsolutions GmbH, Bretten

Für den Druck des Buches wurde chlor- und säurefreies Papier verwendet.

Bildnachweis: Titelbild © md3d / Fotolia

Fraunhofer-Informationszentrum Raum und Bau IRB
Postfach 800469, 70504 Stuttgart
Nobelstraße 12, 70569 Stuttgart
Telefon 0711 970-2500
Telefax 0711 970-2508
E-Mail verlag@fraunhofer.de
URL http://verlag.fraunhofer.de

Inhaltsverzeichnis

Vorwort

Cybersicherheit@Hessen

©HMdIS

Kaum ein Thema war in der vergangenen Zeit in der öffentlichen Diskussion so präsent wie die unaufhaltsame Digitalisierung und ihre Folgen für Mensch und Gesellschaft. Doch mit der rasanten Entwicklung der Digitalisierung nimmt die Bedeutung von Sicherheitsaspekten zu.

Die Daten unserer Bürgerinnen und Bürger, unserer Unternehmen und nicht zuletzt die Daten und Infrastrukturen der Verwaltung müssen geschützt werden. Oftmals sind sie ganz handfester Erpressungs- und Betrugskriminalität ausgesetzt und Unternehmen sehen sich zudem mit digitaler Wirtschaftsspionage konfrontiert. Gerade für kritische Infrastrukturen ist IT-Sicherheit unverzichtbar und sie ist lebenswichtig für ein funktionierendes Gemeinwesen.

Zugleich werden das Internet und digitale Kommunikationsmittel zur Planung und Vorbereitung von Straftaten eingesetzt. Täter und potentielle Täter hinterlassen dabei digitale Spuren im Netz, so dass diese – entsprechende Kompetenzen und Systeme bei den Sicherheitsbehörden vorausgesetzt – bei der Strafverfolgung und bei der Prävention genutzt werden können.

Die enorm hohe Geschwindigkeit bei der Weiterentwicklung und Verbreitung digitaler Technologien erfordert innovative Sicherheitsmaßnahmen. Politik und Verwaltung müssen sich der Herausforderungen dieser digitalen Welt annehmen und den Wandel von der analogen zur digitalen Gesellschaft gestalten und steuern. Die Hessische Landesregierung verfolgt beim Thema Schutz in der virtuellen Welt mit der Agenda „Cybersicherheit@Hessen“ einen ganzheitlichen Ansatz. Eine Säule dabei ist die Förderung der Cybersicherheitsforschung durch das Hessische Ministerium des Innern und für Sport.

Der vorliegende „Ratgeber für eine sichere zentrale Softwareverteilung“ ist ein Studienergebnis dieser Forschungsförderung. Er zielt auf die Sensibilisierung von Administratoren in größeren Unternehmen und Organisationen für wichtige Sicherheitsaspekte bei der Softwareverteilung. Zudem kann er als Handreichung für Administratoren dienen, die sich über die zu berücksichtigenden Sicherheitsaspekte informieren möchten.

Sicherheit in vernetzen Systemen funktioniert nur, wenn alle Beteiligten für Sicherheit sorgen, wenn alle Bestandteile des Netzes sicher sind. Mit diesem Ratgeber wollen wir hierzu einen Beitrag leisten.

Peter Beuth
Hessischer Minister des Innern und für Sport

Kurzfassung

Vor allem in größeren Unternehmen und Organisationen gewinnt eine automatisierte Softwareverteilung zunehmend an Bedeutung. So müssen beispielsweise viele Endgeräte mit einer ähnlichen Software ausgestattet und kritische Sicherheitsupdates in möglichst kurzer Zeit auf vielen Endgeräten installiert werden. Aus Gründen der Konsolidierung und Standardisierung von IT-Diensten und den damit verbundenen Kosteneinsparungen und Effizienzsteigerungen wird die Softwareverteilung häufig als zentraler Dienst innerhalb eines Unternehmens oder einer Organisation angeboten.

Die zentrale Softwareverteilung berührt hierbei viele Aspekte der IT-Sicherheit. Neben naheliegenden Gefährdungen wie dem Einschleusen von Schadsoftware, müssen weitere Themenfelder wie beispielsweise Vertrauensbeziehungen zwischen Netzwerkdomänen, Umgang mit administrativen Berechtigungen und Erkennung von Sicherheitsvorfällen berücksichtigt werden.

Dieser Ratgeber richtet sich an Administratoren, die eine zentrale, netzwerkübergreifende Softwareverteilung in ihrem Unternehmen planen und sich über die zu berücksichtigenden Sicherheitsaspekte informieren möchten. Das zentrale Ziel des Ratgebers ist die Sensibilisierung von Administratoren für wichtige Sicherheitsaspekte bei der Softwareverteilung. Hierzu wird nach einer Einführung in das Thema sichere Softwareverteilung ein Katalog von Sicherheitskriterien bereitgestellt, der auf potentielle Gefährdungen hinweist und beispielhaft geeignete Sicherheitsmaßnahmen nennt.

Erklärung

Der vorliegende Ratgeber wurde vom Fraunhofer-Institut für Sichere Informationstechnologie im Zeitraum von September 2016 bis Februar 2017 erstellt. Die Erstellung wurde durch das Land Hessen, vertreten durch das Hessische Ministerium des Inneren und für Sport, gefördert.

Angaben zu den im Ratgeber genutzten Quellen finden sich im Literaturverzeichnis. Der Ratgeber wurde nach bestem Wissen und den zum Bearbeitungszeitraum vorliegenden Informationen allein und unabhängig vom Fraunhofer SIT erstellt.

1 Einleitung

In größeren Unternehmen und Organisationen besteht der Trend, IT-Dienstleistungen, wie die Systemverwaltung zu zentralisieren [34]. Die Gründe für die Zentralisierung sind vielfältig und betreffen u. a. Modernisierung und Standardisierung von Technologien, Konsolidierung von technischen und organisatorischen Prozessen und damit verbundenen Kosteneinsparungen. Für die Systemverwaltung bieten eine Reihe von Herstellern Produkte an, Beispiele hierfür sind *Microsoft System Center Configuration Manager* (SCCM), *Landesk Management Suite* (LDMS) und *IBM BigFix*. Neben Diensten wie Lizenzmanagement, Helpdesk oder Endgeräteverwaltung wird häufig auch die Softwareverteilung zentralisiert.

Die Softwareverteilung spielt in größeren Unternehmen und Organisationen mit vielen PC-Arbeitsplätzen eine wichtige Rolle. Es müssen in der Regel viele Endgeräte mit ähnlicher Softwareausstattung bestückt werden, außerdem müssen kritische Sicherheitsupdates in möglichst kurzer Zeit auf vielen Endgeräten installiert werden.

Hierbei werden viele Aspekte der IT-Sicherheit berührt. So muss beispielsweise verhindert werden, dass Schadsoftware eingeschleust wird, Angreifer unberechtigten Zugriff auf Informationen erhalten oder versteckte Hintertüren eingebaut werden. Wird Software über Netzwerkgrenzen hinweg verteilt, dann müssen Fragestellungen hinsichtlich des Vertrauens zwischen Netzen berücksichtigt werden. Hierbei erfordern Administratorenkonten eine besondere Betrachtung. Aufgrund ihrer weitreichenden Berechtigungen stellen sie einerseits ein attraktives Angriffsziel dar, können jedoch auch für vorsätzliche Handlungen ausgenutzt werden. Des Weiteren müssen Maßnahmen wie die beweissichere Protokollierung und Überwachung berücksichtigt werden, um Sicherheitsvorfälle einerseits forensisch analysieren und andererseits frühzeitig erkennen und verfolgen zu können. Schließlich kann es zur Erhaltung des gewünschten Sicherheitsniveaus sinnvoll sein, die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig zu prüfen.

Das Thema IT-Sicherheit bildet einen Schwerpunkt in diesem Ratgeber. Das zentrale Ziel des Ratgebers ist die Sensibilisierung von Administratoren für wichtige Sicherheitsaspekte bei der Softwareverteilung. Hierzu wird nach einer Einführung in das Thema sichere Softwareverteilung ein Katalog von Sicherheitskriterien bereitgestellt, der auf potentielle Gefährdungen hinweist und beispielhaft geeignete Sicherheitsmaßnahmen nennt. Dieser Ratgeber richtet sich an Administratoren, die eine zentrale, netzwerkübergreifende Softwareverteilung in ihrem Unternehmen planen und sich über die zu berücksichtigenden Sicherheitsaspekte informieren möchten.

1.1 Abgrenzung

Dieser Ratgeber fokussiert sich auf die Absicherung der Softwareverteilung. Allgemeine Sicherheitsaspekte für die Absicherung bzw. Härtung von IT-Systemen sind nicht Gegenstand der Betrachtung, müssen jedoch ebenfalls bei der Konzeption berücksichtigt werden.

Grundlage dieses Ratgebers sind Literaturrecherchen. Es wurden keine Produkte zur Softwareverteilung getestet. Die vorgeschlagenen Kriterien und geeigneten Maßnahmen betrachten Sicherheitsaspekte auf konzeptioneller Ebene, d. h. es werden in der Regel keine konkreten technischen Maßnahmen oder Konfigurationsbeispiele geliefert.

Einige der Sicherheitsaspekte werden am Beispiel der weitverbreiteten Systemverwaltungssoftware Microsoft SCCM erläutert. Die abgeleiteten Kriterien sind jedoch in der Regel allgemeingültig und unabhängig von SCCM anwendbar.

1.2 Aufbau des Ratgebers

Der Ratgeber beginnt in Kapitel 2 mit einer allgemeinen Einführung in das Thema Softwareverteilung. Es werden wichtige Begriffe zum Thema Softwareverteilung definiert sowie typische Topologien und Strategien für Softwareverteilung diskutiert.

Im Anschluss werden in Kapitel 3 wichtige Aspekte der IT-Sicherheit beleuchtet. Nach einer Einführung relevanter Begriffe werden insbesondere Sicherheitsaspekte bei der Administration von IT-Systemen, bei der Systemkonfiguration, bei der Softwareverteilung und dem Outsourcing betrachtet. Daneben beschäftigt sich dieses Kapitel auch mit der Protokollierung und Überwachung von IT-Systemen.

Kapitel 4 beschäftigt sich mit der Softwareverteilung mittels Microsoft SCCM. Ein Schwerpunkt hierbei bildet der Einsatz von Microsoft SCCM über mehrere Active Directories hinweg und dem Einrichten eines hierfür erforderlichen *Cross Forest Trust*. In diesem Zusammenhang werden wichtige Sicherheitsaspekte bezüglich des Einsatzes von Microsoft SCCM in Cross-Forest-Trust-Szenarien diskutiert.

Danach wird in Kapitel 5 ein Katalog von IT-Sicherheitskriterien definiert, die bei der Einführung und dem Betrieb eines Systems zur zentralen Softwareverteilung innerhalb eines Unternehmens oder einer Organisation eingehalten werden sollten. Zu jedem Kriterium werden Maßnahmen zur Umsetzung des jeweiligen Kriteriums genannt.

Der Ratgeber endet mit einem Fazit in Kapitel 6, welches die wesentlichen Ergebnisse des Ratgebers zusammenfasst.

2 Softwareverteilung

In größeren Unternehmen und Organisationen mit vielen PC-Arbeitsplätzen spielt das Thema Softwareverteilung eine wichtige Rolle. Es müssen in der Regel viele Endgeräte mit ähnlicher Softwareausstattung bestückt werden, außerdem müssen kritische Sicherheitsupdates in möglichst kurzer Zeit auf vielen Endgeräten installiert werden. Eine manuelle Softwareverteilung ist daher in vielen Fällen nicht praktikabel. In [13] werden zwei wesentliche Gründe für eine automatisierte Softwareverteilung genannt: Eine automatisierte Softwareverteilung kann zum einen die Kosten für die Verteilung der Software und Konfiguration der Endgeräte senken. Zum anderen kann sie die Produktivität erhöhen, da die Verfügbarkeit der Software auf den Endgeräten erhöht wird.

Gleichzeitig kann aber auch eine nicht korrekt konfigurierte Softwareverteilung erhebliche Risiken mit sich bringen. Gartner vermutet in [14], dass von allen Fehlern und Ausfällen bei IT-Systemen aufgrund von fehlerhaften Prozessen mehr als die Hälfte auf Fehler in den Prozessen zur Softwareverteilung und auf eine mangelnde Koordination zwischen Change-Management-Prozessen und Softwareverteilungsprozessen zurückzuführen sind. Aus diesem Grund ist eine sorgfältige Planung vor der Einführung einer automatisierten Softwareverteilung äußerst wichtig. Unter anderem sollten die Softwareverteilungsprozesse gut dokumentiert werden, es sollte auf Standards und etablierte Systeme zurückgegriffen werden und es sollte vermieden werden, mehrere verschiedene Systeme zur Softwareverteilung einzusetzen.

Dieses Kapitel gibt einen Überblick über das Thema der automatisierten Softwareverteilung. Es werden zunächst wichtige Begriffe zum Thema Softwareverteilung definiert. Im Anschluss werden typische Topologien von Softwareverteilungssytemen vorgestellt und es werden verschiedene Verteilungsstrategien diskutiert.

2.1 Begriffsbestimmungen

In diesem Abschnitt werden verschiedene Begriffe zum Thema Softwareverteilung definiert, welche für das Verständnis der nachfolgenden Kapitel dieses Ratgebers wichtig sind.

Softwareverteilung

Unter dem Begriff „Softwareverteilung“ (engl.: *software distribution*) wird im Rahmen dieses Ratgebers die automatische Lieferung und Installation von Software über das Netzwerk auf den Endgeräten der Mitarbeiter oder Servern eines Unternehmens oder einer Organisation verstanden [41]. Die Installation erfolgt in der Regel ohne weitere Nutzerinteraktion. In manchen Fällen (insbesondere in kleinen Unternehmen mit nur sehr wenigen Endgeräten) kann die Installation jedoch auch manuell durch einen dafür qualifizierten Mitarbeiter (z. B. Administrator) erfolgen.

In einigen Fällen wird in der englischsprachigen Literatur für die Softwareverteilung auch der Begriff *Software Deployment* genannt. Die Bedeutung dieses Begriffs ist jedoch nicht eindeutig. Im Kontext von Softwareentwicklung und Systemadministration (DevOps, siehe auch [15]) beschreibt der Begriff Deployment das kontinuierliche Ausliefern von Softwareversionen (engl.: *continuous delivery*) vom Hersteller an die Anwender der Software. Hingegen bezeichnet der Begriff *Deployment* im Kontext von Softwareverteilung den Teilprozess der Übertragung des Installationspakets auf die Endgeräte. Im Rahmen dieses Ratgebers wird daher auf die Verwendung des Begriffs *Software Deployment* verzichtet bzw. bei der referenzierten Literatur darauf hingewiesen, in welcher Weise der Begriff zu verstehen ist.

Die Softwareverteilung lässt sich in die folgenden Teilprozesse aufgliedern:

Orchestrieren. Im Rahmen der Orchestrierung wird die zu installierende Software in Abhängigkeit von den verwalteten Endgeräten und den dazugehörigen Endgerätekonfigurationen zusammengestellt.

Herunterladen. Die zu installierende Software wird entweder direkt vom Hersteller oder von lokalen Softwaredepots heruntergeladen.

Paketieren. Die zu installierende Software wird einschließlich der Installationsroutinen und der notwendigen Konfigurationen in Paketen zusammengestellt.

Testen. Die Installation der Installationspakete wird vor der Auslieferung getestet.

Verteilen. Die Softwarepakete werden auf die Endgeräte ausgeliefert.

Installieren. Die Softwarepakete werden auf den Endgeräten installiert. Hierzu zählt auch die Deinstallation obsoleter Software.

Durch eine Aneinanderreihung dieser Teilprozesse entsteht die sogenannte *Software Deployment Pipeline* [3].

In jedem der Teilprozesse findet eine Fehlerbehandlung statt, wodurch die Softwareverteilung jederzeit im Fehlerfall beendet werden. Hierbei wird ein Rollback durchgeführt, d. h. es können falls erforderlich beispielsweise unvollständige Softwarepakete gelöscht werden oder bereits installierte Software auf den Endgeräten wieder entfernt werden.

In dem vorliegenden Ratgeber werden nur automatisierte Softwareverteilungsprozesse betrachtet. Nur durch eine Automatisierung ist es möglich, die oben genannten Teilprozesse schnell und kosteneffizient auszuführen, und somit Software sehr schnell und effizient auf einer großen Zahl an Rechnern auszurollen [27]. Insbesondere können hierdurch auch Sicherheitsupdates und Patches zeitnah nach ihrer Veröffentlichung auf allen betroffenen Rechnern installiert werden, sodass neben Kosteneinsparungen auch die Sicherheit innerhalb des internen Netzwerks erhöht werden kann.

Systemverwaltung

In der Regel ist die Softwareverteilung Bestandteil einer Systemverwaltung (engl.: *systems management*), wie beispielsweise *Microsoft System Center Configuration Manager* (SCCM)[1], *Landesk Management Suite* (LDMS)[2] und *IBM BigFix*[3]. Eine Übersicht über verschiedene Systemverwaltungsprodukte ist zudem in [32] zu finden. Mit Hilfe der Systemverwaltung können neben der Softwareverteilung weitere Aufgaben erledigt werden (vgl. Abbildung 2.1):

Inventarisierung von Hardware und Software. Die Inventarisierung dient der Verwaltung, welche (lizenzpflichtige) Software auf welchen Endgeräten oder Servern installiert ist sowie der Ausstattung der Endgeräte und Server (z. B. Speicher, Prozessor).

Monitoring. Mithilfe des Monitorings kann überwacht werden, ob beispielsweise die Software auf den Endgeräten oder Servern aktuell ist oder ob die Lizenzen noch gültig sind.

Konfigurationsverwaltung. In der Praxis sind die Endgeräte und Server oftmals sehr heterogen bezüglich ihrer Hardware- und Softwarekonfiguration. D. h. die Rechner haben eine unterschiedliche Hardware-Basis, haben unterschiedliche Betriebssysteme oder Betriebssystemversionen und unterscheiden sich in der auf ihnen installierten Anwendungssoftware. Diese Konfigurationen können mithilfe der Systemverwaltung verwaltet werden.

Paketverwaltung. Die im Rahmen der Softwareverteilung erzeugten Installationspakete können verwaltet werden.

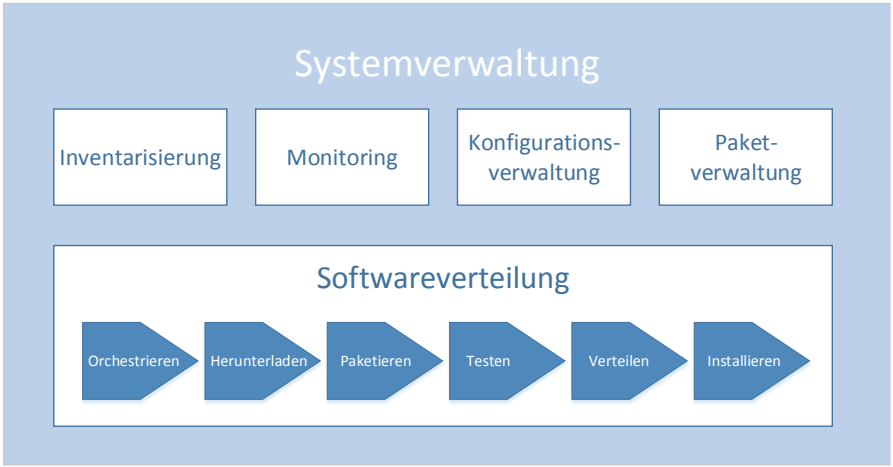

Abbildung 2.1: Systemverwaltung

[1] https://www.microsoft.com/de-de/server-cloud/products/system-center-configuration-manager/overview.aspx (besucht am 31.8.2017)

[2] http://www.landesk.com/de/products/management-suite/ (besucht am 31.8.2017)

[3] http://www-03.ibm.com/software/products/de/endpoint-manager-family (besucht am 31.8.2017)

2.2 Architekturen

Für eine automatisierte Softwareverteilung werden ein oder mehrere Softwareverteilungsserver benötigt, welche die in Abschnitt 2.1 genannten Aufgaben erledigen. Auf den Endgeräten ist für die Kommunikation mit dem Softwareverteilungsserver in der Regel eine dazugehörige Client-Anwendung installiert.

Prinzipiell lassen sich drei Topologien für die Softwareverteilung voneinander unterscheiden (vgl. Abbildung 2.2).

Zentrale Softwareverteilung. Bei der zentralen Softwareverteilung gibt es genau einen Softwareverteilungsserver, der alle Endgeräte bedient.

Dezentrale Softwareverteilung. Bei der dezentralen Softwareverteilung gibt es mehrere Softwareverteilungsserver, von denen die Endgeräte die Software beziehen. Bestimmte Softwarepakete sind hierbei nur von bestimmten Softwareverteilungsserver erhältlich.

Hierarchische Softwareverteilung. Bei der hierarchischen Softwareverteilung [16] gibt es einen zentralen Softwareverteilungsserver, welcher die Softwarepakete an mehrere untergeordnete Softwareverteilungsserver verteilt. Die untergeordneten Softwareverteilungsserver wiederum verteilen die Softwarepakete auf die Endgeräte. Bei dieser Topologie findet in der Regel eine Aufgabenteilung zwischen den Softwareverteilungsservern auf den einzelnen Ebenen der Hierarchie statt. In der Regel findet auf dem Server in der obersten Ebene der Hierarchie die Orchestrierung und Paketierung statt. Die Server auf den untersten Ebenen dienen dann nur noch der Verteilung der Softwarepakete auf die Endgeräte.

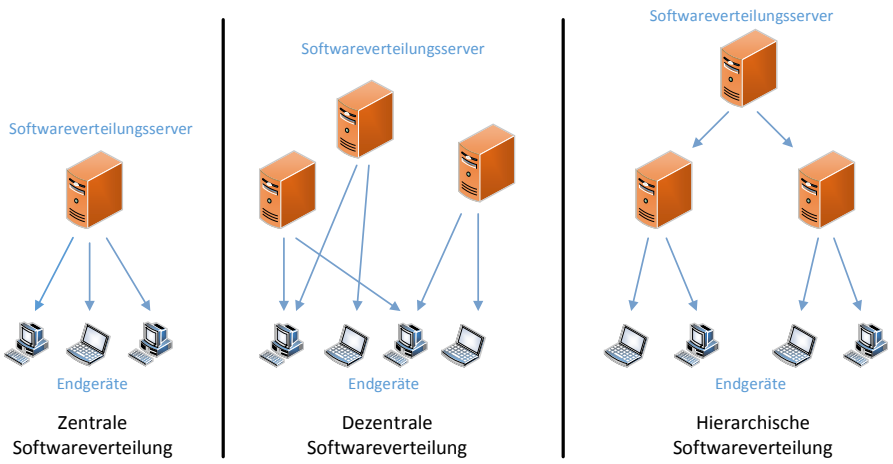

Abbildung 2.2: Softwareverteilungstopologien

Diese drei grundlegenden Topologien können beliebig miteinander kombiniert werden. Darüber hinaus ist auch eine Softwareverteilung über Netzwerkgrenzen hinweg möglich, d. h. Softwareverteilungsserver und Endgeräte können in unterschiedlichen Netzwerken angesiedelt sein.

Bei der Entscheidung für eine bestimmte Topologie sind auch Kostenaspekte zu berücksichtigen. So wird beispielsweise in einer Gartner-Studie zum Thema Optimierung

von IT-Kosten [34] empfohlen, prinzipiell IT-Dienste zu zentralisieren. Weiterhin wird dargelegt, dass sich Kosteneinsparungen durch die Konsolidierung der verwendeten Technologien sowie durch die Verwendung von Standardtechnologien ergeben können. Einsparpotentiale können sich laut dieser Studie auch durch die Verringerung der Komplexität des Anwendungsportfolios sowie durch die Vermeidung von Redundanzen bei den Anwendungen ergeben.

2.3 Verteilungsstrategien

In diesem Abschnitt werden verschiedene Strategien für die Softwareverteilung diskutiert. Hierbei spielt zum einen die Frage eine Rolle, ob der Softwareverteilungsserver die Software aktiv auf den Endgeräten installiert oder ob die Endgeräte sich die Software aktiv von einem Softwareverteilungsserver herunterladen (Push- vs. Pull-Verfahren). Zum anderen spielt auch die zeitliche Dimension bei der Softwareverteilung eine wichtige Rolle, d. h. kann zu jeder Zeit Software auf den Endgeräten installiert werden oder gibt es beispielsweise definierte Zeitfenster, innerhalb derer die Software auf die Endgeräte verteilt werden darf.

Push- vs. Pull-Verfahren

Typischerweise erfolgt die automatisierte Verteilung von Software entweder durch ein Push-Verfahren oder durch ein Pull-Verfahren [44]. Beim Push-Verfahren verteilt der Softwareverteilungsserver die Software aktiv an alle Endgeräte. Der Vorteil hierbei ist, dass der Administrator die Kontrolle darüber hat, zu welchem Zeitpunkt welche Software auf welchen Endgeräten installiert werden soll. Die Nachteile dieses Verfahrens sind jedoch, dass die Endgeräte jederzeit erreichbar sein müssen und dass der Softwareverteilungsserver Informationen über die einzelnen Endgeräte vorhalten muss (z. B. welche Software auf welchen Endgeräten installiert werden muss bzw. bereits vorhanden ist).

Beim Pull-Verfahren übernehmen die Endgeräte die Initiative. Eine spezielle Client-Anwendung, die auf dem Endgerät installiert ist, lädt die Software von dem Softwareverteilungsserver herunter und installiert die Software anschließend auf dem Endgerät. Die Endgeräte müssen bei dieser Variante nicht ständig erreichbar sein. Nachteilig ist, dass der Administrator keine Kontrolle darüber hat, zu welchen Zeiten Software auf bestimmten Endgeräten installiert wird. Das bedeutet, dass im schlimmsten Fall alle Endgeräte zum gleichen Zeitpunkt Software bei dem Softwareverteilungsserver anfordern.

Reihenfolge und Zeitplanung

Eine zeitliche Planung der Softwareverteilung kann sinnvoll sein, um einerseits eine Überlastung des Netzwerks zu vermeiden, andererseits aber insbesondere kritische Softwareupdates zeitnah auf den Endgeräten einzuspielen. Um eine Überlastung des internen Netzwerks und auch des Softwareverteilungsservers zu vermeiden, können unterschiedliche Zeitfenster für unterschiedliche Gruppen von Endgeräten (z. B. alle Endgeräte einer bestimmten Abteilung innerhalb der Organisation) definiert werden.

Software kann dann nur innerhalb des jeweils zugewiesenen Zeitfensters auf ein Endgerät verteilt werden. Hierbei sollten jedoch Ausnahmeregelungen definiert werden, die es ermöglichen, kritische Sicherheitsupdates zu jeder Zeit zu installieren.

Ein weiterer Aspekt bezüglich der zeitlichen Planung der Softwareverteilung beschäftigt sich mit der Frage, wie zeitnah nach der Veröffentlichung Software auf den Endgeräten installiert werden sollte. Hierbei ist abzuwägen zwischen der Dringlichkeit beispielsweise eines Softwareupdates, welches kritische Sicherheitslücken schließt, und andererseits dem Risiko, dass beispielsweise durch das Einspielen der neuen Software andere bereits installierte Software in ihrer Funktion beeinträchtigt wird, oder dass die Benutzer durch das Bereitstellen unausgereifter Software in ihrer Arbeit beeinträchtigt werden.

Software kann prinzipiell im laufenden Betrieb auf den Endgeräten eingespielt werden. Wenn jedoch abzusehen ist, dass es während des Installationsprozesses zu Beeinträchtigungen der Benutzer der Endgeräte kommen kann, weil während dieses Zeitraums bestimmte Software oder sogar das gesamte Endgerät nicht benutzt werden kann, sollte ein Wartungszeitfenster definiert und an die Benutzer kommuniziert werden. Innerhalb dieses Zeitfensters steht das Endgerät den Benutzern nicht oder nur eingeschränkt zur Verfügung und es kann die neue Software eingespielt werden. Eine generelle Empfehlung lässt sich hierfür jedoch nicht geben, da es sowohl von der zu installierenden Software als auch vom Endgerät (Betriebssystem etc.) abhängt, welche Methode am geeignetsten ist.

Gartner empfiehlt in der Studie „Principles and Practices of DevOps“ [27], Software sukzessive an einen immer größer werden Benutzerkreis auszuliefern. Das Ziel hierbei ist, Probleme und Fehler in der Software möglichst frühzeitig zu entdecken, dabei aber nur einen möglichst kleinen Benutzerkreis durch die fehlerhafte Software zu beeinträchtigen. Auch ein möglicherweise notwendiges Deinstallieren der Software und Zurücksetzen der Endgeräte in den ursprünglichen Zustand ist einfacher, wenn möglichst wenig Geräte betroffen sind. Diese Verteilungsstrategie ist jedoch eher im Rahmen des Softwareentwicklungsprozesses sinnvoll (DevOps), wenn kontinuierlich neue Versionen einer Software an die Anwender ausgeliefert werden.

3 IT-Sicherheitsaspekte: Gefährdungslage und Maßnahmen

Dieses Kapitel betrachtet IT-Sicherheitsaspekte, die hinsichtlich der Einführung einer Lösung zur zentralen netzwerkübergreifenden Softwareverteilung relevant sind. So müssen beispielsweise Fragen nach dem Schutz vor Schadsoftware oder unberechtigten Zugriffen auf Informationen berücksichtigt werden. Die Verteilung von Software über Netzwerkgrenzen hinweg betrifft Aspekte des Vertrauens zwischen Netzen. Administratorenkonten erfordern eine besondere Betrachtung. Aufgrund ihrer weitreichenden Berechtigungen stellen sie einerseits ein attraktives Angriffsziel dar, können jedoch auch für vorsätzliche Handlungen ausgenutzt werden. Die beweissichere Protokollierung und Überwachung kann notwendig sein, um Sicherheitsvorfälle forensisch analysieren, frühzeitig erkennen und verfolgen zu können. Schließlich kann es zur Erhaltung des gewünschten Sicherheitsniveaus sinnvoll sein, die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig zu prüfen.

Neben den in den nachfolgenden Abschnitten aufgeführten Aspekten gibt es jedoch zahlreiche weitere Gefährdungen und zugehörige Maßnahmen, die nicht in diesem Dokument enthalten sind. Dies gilt insbesondere für IT-Sicherheitsaspekte allgemeiner Natur, die unabhängig vom Thema Softwareverteilung berücksichtigt werden sollten. Beispiele hierfür sind:

- Gefährdungen durch ungeschützte Kommunikationsverbindungen (und zugehörige Maßnahmen wie den Einsatz eines verschlüsselten Kommunikationskanals sowie die Authentifizierung der kommunizierenden Komponenten).
- Gefährdungen durch die unentdeckte Manipulation von Daten (und zugehörige Maßnahmen wie beispielsweise den Einsatz digitaler Signaturen).
- Gefährdungen durch schwache Passwörter (und zugehörige Maßnahmen wie Empfehlungen zu Eigenschaften sicherer Passwörter).
- Gefährdungen durch technisches Versagen im Sinne von defekter Hardware, Nichtverfügbarkeit von Komponenten etc. (und zugehörige Maßnahmen zur Steigerung der Ausfallsicherheit)
- Gefährdungen durch unzureichende Einschränkung der Berechtigungen von Benutzern und Systemkomponenten (und zugehörige Maßnahmen hinsichtlich der Verbesserung des Berechtigungsmanagements).

Die Tatsache, dass solche IT-Sicherheitsaspekte in diesem Dokument nicht aufgeführt werden, darf hierbei nicht als Entschuldigung dienen, diese nicht zur berücksichtigen. Es wird im Gegenteil angenommen, dass Sicherheitsaspekte allgemeiner Natur ohnehin bereits berücksichtigt werden. In diesem Zusammenhang wird beispielsweise die Berücksichtigung des BSI-Grundschutz [9] empfohlen, der im Rahmen seiner Bausteine zahlreiche Gefährdungen auflistet und zugehörige Maßnahmen vorschlägt. Für weiterführende Informationen wird auf die umfangreiche Literatur zum Thema IT-Sicherheit verwiesen.

Es wird darauf hingewiesen, dass es zur Absicherung eines Systems unerlässlich ist, die verschiedenen Sicherheitsaspekte ganzheitlich zu betrachten und einzeln aufeinander abzustimmen. Die nachfolgende Darstellung erhebt keinen Anspruch auf Vollständigkeit, in konkreten Anwendungsfällen kann die Berücksichtigung weiterer IT-Sicherheitsaspekte notwendig sein.

3.1 Begriffsbestimmungen

3.1.1 Theoretische und effektive Sicherheit

Bei der Bewertung der Sicherheit einer Komponente oder eines Systems muss unterschieden werden zwischen der theoretischen Sicherheit, charakterisiert durch den Grad der Sicherheit einer Komponente, der theoretisch technisch erreichbar ist, und der effektiven Sicherheit – auch praktische oder tatsächliche Sicherheit genannt – als Grad der Sicherheit, der in realistischen und praktisch relevanten Anwendungsszenarien tatsächlich erreicht wird [17, 19, 20, 45].

Dourish und Redmiles [20] gehen davon aus, dass der effektive Sicherheitsgrad fast immer unterhalb des theoretischen Sicherheitsgrads liegt. Als Gründe für die Diskrepanz zwischen beiden Sicherheitslevels nennen sie schlechtes Design von Sicherheitslösungen, Fehler bei der Implementierung kryptografischer Primitiven, unsicheres Protokolldesign und unzureichende Unterstützung durch das jeweilige Betriebssystem. Gerade auch die Interaktion verschiedener Systemkomponenten (Anwendungen, Infrastrukturkomponenten, Protokolle) habe Einfluss auf die effektive Sicherheit. Zusätzlich habe die Struktur und das Verhalten von internen Komponenten auch signifikanten Einfluss auf die Interaktion des Benutzers mit dem System. Dourish und Redmiles sprechen hierbei vom Ende-zu-Ende-Phänomen, bei dem die effektive Sicherheit einer komplexen Anwendung potentiell von jeder involvierten Komponente, wie beispielsweise Einzelanwendung, Infrastrukturkomponente, Protokoll, Netzwerkdienst, und deren Abhängigkeiten abhängt.

Da die effektive Sicherheit eines Systems also immer auch von der tatsächlichen Realisierung (u. a. charakterisiert durch die Implementierung, die Konfiguration, dem Zusammenspiel der Teilkomponenten in der Praxis und menschlichen Interaktionen) abhängt, ist eine Sicherheitsanalyse, welche auf der Analyse von Konzepten und Spezifikationen aufbaut, hinsichtlich Aussagen über die effektive Sicherheit eines Systems stets unvollständig.

In Abschnitt 3.4 werden einige Beispiele für fehlerhafte Konfigurationen genannt, die Ursache dafür sein können, dass die effektive Sicherheit eines Systems niedriger ist als die theoretische Sicherheit.

3.1.2 Ursachen von IT-Sicherheitsproblemen

IT-Sicherheitsprobleme treten dann ein, wenn Gefährdungen verschiedener Art eintreten bzw. ausgenutzt werden. Gefährdungen in der IT-Sicherheit sind in der Regel auf eine oder mehrere der folgenden Ursachen aus den folgenden Kategorien (nach Grundschutz [9]) zurückzuführen:

1. Elementare Gefährdungen
2. Höhere Gewalt
3. Organisatorische Mängel
4. Menschliche Fehlhandlungen
5. Technisches Versagen
6. Vorsätzliche Handlungen

Im Rahmen dieses Ratgebers werden insbesondere die letzteren vier Kategorien betrachtet.

3.1.3 Angriffstypen

Es gibt verschiedene Merkmale zur Kategorisierung von Angriffen. Wichtige Kategorien sind beispielsweise die Unterscheidung zwischen passiven und aktiven Angriffen, sowie die Unterscheidung zwischen zielgerichteten und nicht-zielgerichteten Angriffen.

Passive und aktive Angriffe

Passive Angriffe betreffen das Mithören und Ausspähen von Informationen ohne aktive Beeinflussung der Kommunikation oder Veränderung von Informationen. Hierzu zählen beispielsweise das Mithören von ausgetauschten E-Mails, von Netzwerkkommunikation oder von Telefonaten. Passive Angriffe sind in der Regel schwer zu erkennen.

Aktive Angriffe hingegen umfassen alle Angriffe, bei denen der Angreifer aktiv Schwachstellen in Systemen ausnutzt, gezielt Daten verändert oder Systeme manipuliert. Aktive Angriffe sind in der Regel gefährlicher, können einen höheren Schaden verursachen, sind aber häufig einfacher erkennbar als passive Angriffe.

Zielgerichtete und nicht-zielgerichtete Angriffe

Die Unterscheidung von Angriffen hinsichtlich ihrer Zielgerichtetheit erscheint zunächst paradox, da man davon ausgehen kann, dass ein Angreifer mit jeglichem Angriff ein Ziel verfolgt. Aus technischer Sicht ist jedoch interessant zu unterscheiden, ob das Angriffsziel stark fokussiert ist oder nicht. Als Analogie kann man sich unter einem zielgerichteten Angriff ein Schuss aus einem Präzisionsgewehr vorstellen, während ein nicht-zielgerichteter Angriff eher mit dem Schuss aus einem Schrotgewehr vergleichbar ist.

Zielgerichtete Angriffe erfordern in der Regel mehr Detailinformationen über das Angriffsziel, während nicht-zielgerichtete Angriffe in der Regel darauf abzielen, dass unter der Menge möglicher Angriffsziele eine ausreichend große Menge enthalten ist, die angreifbar ist.

3.1.4 Angreifertypen

Angreifer unterscheiden sich von normalen Benutzern derart, dass ihr Handeln grundsätzlich vorsätzlich und ggf. auch böswillig ist. Angreifer können aus eigener Motivation handeln oder im Auftrag von Dritten. Ziele von Angreifern sind beispielsweise der unberechtigte Zugriff auf Informationen, das Auslösen von temporären oder dauerhaften Funktionsstörungen an technischen oder informationstechnischen Anlagen (wie beispielsweise Denial-of-Service-Angriffe) oder Erpressungen. Hierzu nutzen Angreifer Schwachstellen oder Hintertüren in Systemen aus, bauen neue Hintertüren ein, schleusen Schadsoftware wie Trojaner oder Würmer ein und versuchen in der Regel dabei, unerkannt zu bleiben und ihre Spuren zu verwischen.

Interne und externe Angreifer

Angreifer werden typischerweise in interne und externe Angreifer unterschieden (vgl. beispielsweise [22, 43]). Diese Unterscheidung ist jedoch ungenau, da die Attribute intern und extern sich je nach verwendeter Begriffsdefinition einerseits auf den „Ort" oder die „Schnittstelle" des Angreifers beziehen, der den Angriff ausführt, d. h. ob der Angriff von außen (wie beispielsweise über das Internet-Portal eines Unternehmens) kommt oder nicht. Andererseits können sich die Attribute intern und extern auch auf die Verbindung des Angreifers zum Angriffsziel oder dessen Eigentümer beziehen, d. h. ob der Angreifer ein Insider (d. h. beispielsweise Mitarbeiter eines Unternehmens) ist oder nicht.

Hinzu kommt, dass in Zeiten von Cloud-Computing, internet-basierten Anwendungen und Outsourcing die Begriffe intern und extern sowohl hinsichtlich der Lokation als auch der Zugehörigkeit zusätzlich schwieriger zu fassen sind. Wird beispielsweise das Systemmanagement eines Unternehmens ausgelagert und durch einen Dienstleister durchgeführt, dann sind die Mitarbeiter des Dienstleisters aus Sicht des Unternehmens einerseits Externe, da sie nicht zum Unternehmen gehören, andererseits aufgrund von Verträgen nicht ganz so extern wie Personen, die weder im Unternehmen noch beim Dienstleister angestellt sind. Andererseits können Mitarbeiter des Dienstleisters auch als Interne verstanden werden, da sie aufgrund ihres Vertrags und Auftrags weitreichende Berechtigungen und Informationen im Unternehmen besitzen und somit bei Betrachtung von außen dem Unternehmen logisch zugerechnet werden können.

Umgekehrt kann ein Angriff eines Mitarbeiters, der über Insider-Informationen verfügt und eine Schwachstelle im Internet-Portal des Unternehmens ausnutzt, als Angriff von extern verstanden werden, weil der Angriff von außerhalb des Unternehmensnetzwerkes erfolgt ist.

Im Rahmen dieses Ratgebers werden die Begriffe intern und extern hinsichtlich der logischen Zugehörigkeit der Person (hier des Angreifers) zum Betrachtungsgegenstand (hier des Angriffsziels) interpretiert. Externe nach dieser Festlegung sind beispielsweise Personen ohne Verbindungen zum Betrachtungsgegenstand. Zu den Internen zählen u. a. Mitarbeiter (und auch ehemalige Mitarbeiter) des Betrachtungsgegenstands, sowie dessen Praktikanten, externe Mitarbeiter, Dienstleister und Kooperationspartner. Je nach Szenario können auch (aus Sicht eines Dienstleisters) die Kunden des Betrachtungsgegenstands als Interne betrachtet werden.

Legitime Benutzer und interne Angreifer

Häufig ist es nicht einfach, Angreifer zu identifizieren. Yurcik et al. beschreiben in [48], dass insbesondere interne Angreifer schwer zu erkennen sein können. Als legitime Benutzer müssen sie einerseits als grundsätzlich vertrauenswürdig eingestuft werden (im Gegensatz zu externen Benutzern), andererseits sollte ungewöhnliches Verhalten mit Hilfe von Verifikations- und Monitoring-Werkzeugen erkannt werden. Yurcik et al. unterscheiden hierbei zwei Arten von internen Benutzern: interne Angreifer und nachlässige Benutzer. Letztere fallen wie interne Angreifer durch ihr ungewöhnliches Verhalten auf. Dieses Verhalten ist jedoch im Gegensatz zu internen Angreifern nicht durch böswilliges, sondern durch unbeabsichtigtes Fehlverhalten begründet. Auch der Grundschutz [9] unterscheidet hierbei zwischen vorsätzlichen Handlungen und menschlichen Fehlhandlungen. Häufig ist es schwierig, mit Hilfe von technischen Werkzeugen interne Angreifer von nachlässigen Benutzern zu unterscheiden.

3.1.5 Angriffsoberfläche

Unter der Angriffsoberfläche (engl.: *attack surface*) eines Systems versteht man typischerweise die Summe aller Angriffsvektoren (insbesondere Dienste, Protokolle, Schnittstellen, Datenkanäle, Applikationen, Kommandos, Daten), die ausgenutzt werden können, um ein System anzugreifen (vgl. [40], [47]). Nach OWASP [40] hilft die Analyse der Angriffsoberfläche dabei, die Funktionen und Teilsysteme zu identifizieren, welche (ggf. aufgrund einer Veränderung des Systems) auf Schwachstellen hin untersucht werden sollten. OWASP [40] weist darauf hin, dass Änderungen an Systemkomponenten direkten Einfluss auf die Angriffsoberfläche haben können und eine erneute Analyse nach sich ziehen sollten. Als wichtige Beispiele nennt OWASP:

- Änderungen am Session Management
- Änderungen an der Authentifizierung
- Änderungen an der Zugriffskontrolle (insbesondere das Hinzufügen oder Ändern von Rollendefinitionen, das Hinzufügen von Admin-Benutzern oder Admin-Funktionen mit weitreichenden Privilegien)
- Änderungen an den Ver- und Entschlüsselungskomponenten und der Verwaltung von Geheimnissen
- Änderungen an der Überprüfung von Daten
- Änderungen an der technischen Architektur
- Änderungen an den Vertrauensbeziehungen von Komponenten

Die Analyse der Angriffsoberfläche laut OWASP fokussiert sich auf den Schutz eines Systems vor externen Angriffen. Angriffe von internen Angreifern und Angriffe auf Benutzer oder Administratoren eines Systems (beispielsweise mittels Malware- oder Social-Engineering-Angriffen) werden häufig nicht betrachtet. Ein Trennlinie zwischen intern und extern lässt sich jedoch in heutigen Systemen nicht immer ziehen, beispielsweise wenn externe Dienstleistungen verwendet werden, Benutzer über interne und externe Schnittstellen Zugriffe erhalten oder die Administration auch von außerhalb

des Systems möglich ist. In anderen Modellen zur Angriffsoberfläche findet diese Trennung nicht explizit statt. Das BSI verzichtet im Grundschutzkatalog weitgehend auf die Verwendung des Begriffs Angriffsoberfläche. Er wird nur einmal in der Maßnahme zur Löschung ungenutzter Konten verwendet [9: M 2.317].

3.2 Sicherheitsaspekte bei der Administration

Für die Analyse der Sicherheit eines Systems ist es wichtig, dessen Administration zu untersuchen. Die Administration eines Systems umfasst beispielsweise die Verwaltung von Benutzerkonten, die Verwaltung von Zugriffsrechten, die Installation und Deinstallation von Software und die Anpassung der Konfigurationen aller Komponenten des Systems. Hierbei sollten sowohl die technischen Werkzeuge zur Administration als auch die mit der Administration betrauten Personen, die Administratoren, genauer betrachtet werden.

3.2.1 Administrationswerkzeuge

Administrationswerkzeuge sollten fehlerfrei und erwartungsgemäß arbeiten. Insbesondere sollten sie keine unbeabsichtigten Sicherheitsprobleme einführen. Weiterhin muss kontrolliert werden, dass nur berechtigte Personen die Administrationswerkzeuge verwenden. Diese Kontrolle kann entweder außerhalb oder innerhalb des Administrationswerkzeugs erfolgen.

Viele Systemkomponenten bringen bereits ihre eigenen Administrationswerkzeuge mit, diese sind in der Regel vom Hersteller getestet und auf die Benutzung mit der jeweiligen Systemkomponente abgestimmt. Es ist hierbei zu beachten, verfügbare Updates der Administrationswerkzeuge zeitnah einzuspielen, um beispielsweise Programmfehler zu beheben.

Zusätzlich werden häufig eigene Administrationswerkzeuge entwickelt und eingesetzt. Gründe hierfür sind beispielsweise, dass für bestehende Komponenten (engl.: *legacy systems*) keine geeigneten Werkzeuge existieren, dass administrative Aufgaben aus mehreren Teilaufgaben bestehen, die in Stapelverarbeitungsweise durchgeführt werden sollen, oder dass wiederkehrende Eingaben und Ausführungsschritte in anderen Administrationswerkzeugen automatisiert werden sollen. Die Erfahrung zeigt, dass gerade selbst entwickelte Administrationswerkzeuge in der Regel weniger gut getestet und weniger häufig gewartet werden. Daher ist die Gefahr von unerwünschten Effekten bei der Administration größer. Beispielsweise kann eine unzureichende Prüfung von Eingabeparametern sowohl bei fehlerhaften Eingaben eines Administrators als auch bei einem vorsätzlich handelnden Administrator großen Schaden anrichten. Umgehen Eigenentwicklungen typische Sicherheitsmechanismen wie die Authentifizierung des Administrators bei einer Systemkomponente, weil beispielsweise Passwörter fest im Programmcode eines Skripts gespeichert sind, können auch Unberechtigte die Werkzeuge anwenden.

Um negative Implikationen von Administrationswerkzeugen auf die Sicherheit eines Systems zu vermeiden, sollen folgende Maßnahmen ergriffen werden:

- Administrationswerkzeuge, die vom Hersteller der jeweiligen Systemkomponente bereitgestellt wurden, sollten bevorzugt eingesetzt werden.
- Eine regelmäßige Prüfung auf verfügbare Updates der o. g. Administrationswerkzeuge und zeitnahe Installation der Updates sollte durchgeführt werden.
- Auf den Einsatz von selbst entwickelten Administrationswerkzeugen sollte verzichtet werden, sofern dies möglich ist und Alternativen des Herstellers vorliegen.
- Selbst entwickelte Administrationswerkzeugen sollten besonders sorgfältig getestet werden, insbesondere hinsichtlich Fehlbedienung, Prüfung ungeeigneter Eingabedaten und Fehlerbehandlung.
- Selbst entwickelte Administrationswerkzeuge dürfen etablierte Sicherheitsmechanismen nicht außer Kraft setzen (beispielsweise indem notwendige Anmeldeinformationen wie Passwörter fest im Programmcode kodiert werden).

3.2.2 Administratoren

Administratoren sind für die Administration eines Systems verantwortlich. Sie nutzen hierzu Administrationswerkzeuge und führen administrative Aufgaben durch. Administratoren sind privilegierte Benutzer. Sie verfügen im Vergleich zu normalen Benutzern des Systems über weiterführende Berechtigungen. Sie können beispielsweise Systeme starten und stoppen, Software installieren und deinstallieren oder Konfigurationen von Software und Systemen ändern und so beispielsweise auch Sicherheitseinstellungen in Systemen verändern.

Berechtigungen von Administratoren können grundsätzlich über die folgenden drei Einstellungen im Berechtigungsmanagement angepasst werden:

1. durch direkte Zuweisung von administrativen Berechtigungen an den Account des Administrators.
2. durch Zuweisung von administrativen Rollen bzw. Gruppen, welche über die administrativen Berechtigungen verfügen, an den Account des Administrators.
3. durch Ausstellung eines oder mehrerer Administrator-Accounts, denen entweder direkt oder über Rollen bzw. Gruppen administrative Berechtigungen zugewiesen wurden. Um diese Berechtigungen nutzen zu können, muss sich der Administrator mit dem zugehörigen Administrator-Account anmelden.

Die effektiven Berechtigungen eines Administrators – das heißt die Summe aller Berechtigungen, die ein Administrator besitzt – ergibt sich aus allen Berechtigungen, die sich aus den drei o. g. Einstellungen ableiten lassen. Häufig werden bei Verwendung eines rollenbasierten Berechtigungsmodells [1] die Rollen hierarchisch gegliedert und Berechtigungen von Rollen an darunterliegende Rollen weitervererbt. In diesem Fall müssen auch alle rekursiv geerbten Rollenberechtigungen bei Ermittlung der effektiven Berechtigungen berücksichtigt werden.

In der Regeln findet aus Sicherheitsgründen eine Trennung zwischen dem normalen Benutzer-Account eines Administrators und seinem/n höher privilegierten

Administrator-Account/s statt. Der Administrator führt dann alle gewöhnlichen Tätigkeiten mit seinem normalen Benutzer-Account statt und wechselt für administrative Aufgaben zu einem Administrator-Account.

Da Administratoren als privilegierte Benutzer über weitreichende Rechte verfügen, sind sie bei der Betrachtung der Sicherheit eines Systems von großer Bedeutung. Hierbei sind insbesondere die folgenden drei Sicherheitsaspekte von zentraler Bedeutung:

1. Wie bei jeder menschlichen Handlung können auch bei der Administrationsarbeit Fehler entstehen. Diese können aufgrund der vielfältigen Berechtigungen von Administratoren im System weitreichende Folgen haben und im Vergleich zu normalen Benutzern größeren Schaden anrichten.
2. Aufgrund ihrer weiterführenden Berechtigungen sind Administratoren attraktive Sicherheitsziele für Angreifer.
3. Administratoren können aufgrund ihrer Berechtigungen auch vorsätzlich (und ggf. im Auftrag eines Angreifers) die Sicherheit eines Systems schädigen oder beispielsweise vertrauliche Daten unberechtigt ausspähen.

In den folgenden Abschnitten werden diese drei Aspekte genauer betrachtet.

Faktor Mensch bei der Administration

Menschliche Fehler oder Fehlhandlungen bei der Administration können verschiedene Ursachen haben. Hierbei ist das Thema Komplexität von großer Bedeutung. Administratoren haben unterschiedliche administrative Aufgaben zu erledigen und sind häufig für viele verschiedene Systeme oder Netzwerke zuständig. Jede dieser Komponenten verfügt über eigene Administrationswerkzeuge. Administrationswerkzeuge sind hinsichtlich der Aufgabenangemessenheit und Benutzbarkeit ihrer Administrationsschnittstellen sehr unterschiedlich. Eine Firemon-Studie [10] ergab, dass allein für den Aspekt der Firewall-Konfiguration 72% der befragten Administratoren zwei oder mehr unterschiedliche Firewall-Systeme (mit verschiedenen Administrationswerkzeugen und unterschiedlicher Firewall-Regel-Syntax) innerhalb eines Unternehmens parallel verwalten müssen.

Yurcik et al. beschreiben in [48] die große Bandbreite an Administrationsaufgaben in komprimierter Form am Beispiel eines typischen Tagesablaufs eines Sicherheitsadministrators. Als besondere Faktoren für Stress von Administratoren bei ihrer Tätigkeit nennen sie u. a. die Aufgabe, sich kontinuierlich über neue Schwachstellen und Angriffsmöglichkeiten zu informieren und entsprechende Maßnahmen zu ergreifen, die häufige Installation von Sicherheitsupdates und die zeitnahe Reaktion auf Anfragen von Benutzern. Botta et al. [5] haben Sicherheitsadministratoren mittels Fragebögen und Interviews befragt und die Vielfältigkeit von Aufgaben, Fertigkeiten und Werkzeugen von Administratoren analysiert. Hier kann es bei Sicherheitsadministratoren aufgrund der Komplexität von Administrationsaufgaben und schlecht gestalteter Administrationswerkzeugen zu Fehlbedienung und Gefährdungen in den administrierten Systemen kommen. Chiasson et al. diskutieren in [11] ebenfalls diese Problematik und definieren zehn Gestaltungsprinzipien für Sicherheitsmanagement-Systeme. Die negativen Rückwirkungen mangelnder Gebrauchstauglichkeit von Werkzeugen für

IT-Sicherheitsmanagement und ID-Management diskutieren auch Dhamija und Dusseault [18] sowie Hawkey et al. [28]. Hawkey et al. [28] und Botta et al. [4] haben die relevanten Aspekte, die zur Komplexität der administrativen Arbeit von Sicherheitsadministratoren führen, zusammengefasst. Sie unterscheiden hierbei mehr als zehn unterschiedliche Einflussfaktoren, die sie in die drei Gruppen „Menschlich", „Organisatorisch" und „Technisch" gliedern.

Im Vergleich zu normalen Benutzern haben gerade Administratoren aufgrund ihrer umfangreichen technischen Kenntnisse und häufig auch aufgrund ihrer Freiheitsgrade hinsichtlich der technischen Ausgestaltung ihrer Aufgabenerledigung unterschiedliche Vorlieben bezüglich der verwendeten Administrationswerkzeuge. Manche Administratoren bevorzugen das textbasierte Arbeiten auf der Konsole, während andere grafische Administrationswerkzeuge bevorzugen. Botta et al. [6] haben die unterschiedlichen Vorlieben hinsichtlich Administrationswerkzeugen genauer untersucht. Dabei kamen sie zu dem Ergebnis, dass der Arbeitsbereich der befragten Administratoren charakterisiert ist durch ihre Verantwortlichkeiten, Aufgaben, ihre Ziele und ihre Fertigkeiten – insbesondere Analysefertigkeiten, Mustererkennung und Fertigkeiten der kreativen Problemlösung (engl. *bricolage*).

Um menschliche Fehler bei der Administration zu reduzieren, sollten Administrationswerkzeuge den Administrator unterstützen, dem Administrator einen guten Überblick über den Gegenstand der Administration geben, die Plausibilität von Eingaben und Konfigurationsanpassungen prüfen, den Administrator vor Problemen warnen und die Komplexität der administrativen Tätigkeit reduzieren. Wenn möglich, sollten mehrschrittige Administrationsaufgaben automatisiert werden, um Inkonsistenzen zwischen den Schritten zu verhindern. Weiterhin sollten administrative Berechtigungen in mehrere Administrator-Accounts aufgeteilt werden, so dass kein Super-Administrator-Account existiert, der über sämtliche Berechtigungen in einem System verfügt. Hierdurch kann erreicht werden, dass Implikationen administrativer Fehler reduziert werden können.

Administratoren als Angriffsziele

Administratoren besitzen im Vergleich zu normalen Computernutzern weitergehende Rechte bezüglich Zugriffsmöglichkeiten auf Systeme und auf gespeicherte Informationen. Daher stellen sie aus Sicht von Angreifern attraktive Angriffsziele dar. Wenngleich Administratoren in der Regeln sensibilisiert sind hinsichtlich dieser Gefährdung und Gegenmaßnahmen kennen und postulieren, so zeigen sich im Alltag dennoch Handlungsweisen und Praktiken, die dem entgegenstehen. Ion et al. [29] haben das Verhalten von normalen Computernutzern und Administratoren hinsichtlich sicherheitsrelevanter Praktiken verglichen und kamen hierbei zu interessanten Ergebnissen. Insbesondere stellten Sie Unterschiede zwischen den von Administratoren erteilten Ratschlägen zur Erhöhung der Sicherheit und tatsächlichen Verhaltensweisen von Administratoren im Vergleich zu normalen Nutzern fest. So wurde beispielsweise festgestellt, dass Administratoren häufiger Passwörter in Webseiten eingaben, die sie als E-Mail-Link erhielten, häufiger E-Mails von unbekannten Empfängern öffneten und auf Links unbekannter Sender klickten.

Wiebusch et al. diskutieren in [46] die Fragestellung, ob es für die Fernwartung aus IT-Sicherheitssicht vorteilhafter ist, lokale Administrationskonten oder Active-Directory-

Konten mit administrativen Berechtigungen auf dem zu administrierenden Zielsystem zu verwenden. Die Entscheidung darüber hängt hierbei maßgeblich vom Anwendungsbereich, der Anzahl von Zielsystemen und der Anzahl von Administratoren ab. So lassen sich Administrationskonten sehr viel einfacher mittels Active Directory verwalten. Sie hinterlassen jedoch auch Spuren auf den verwalteten Zielsystemen, die von Angreifern ausgenutzt werden könnten. Andererseits erhöhen lokale Administrationskonten die Komplexität hinsichtlich der Verwaltung und Benutzbarkeit, beschränken Zugriffe jedoch ausschließlich auf das Zielsystem. Wiebusch et al. geben hierzu einige Entscheidungshilfen und Konfigurationsempfehlungen für die Praxis.

Malchar weist auf Gefahren hin, die bei der Verwaltung von administrativen Berechtigungen entstehen können [33]: „Eine weitere zentrale Schwachstelle in Unternehmen sind Dienst-Accounts und administrative Zugänge mit weitreichenden Berechtigungen. Aufgrund der Masse an existierenden, historisch gewachsenen Accounts ist deren Wartung und Verwaltung jedoch oft schwierig“

Die folgenden Maßnahmen sind Beispiele dafür, wie man den Aufwand von Angreifern beim Angriff auf Administratoren erhöhen kann:

- Unsichere Praktiken wie oben genannt vermeiden. Beispielweise sollte man keine Daten in Formulare eingeben, welche über einen E-Mail-Link verteilt wurden. Generell sollte man keine Links in E-Mails unbekannter Herkunft anklicken (vgl. [29])
- Administrative Berechtigungen auf ein Minimum beschränken, d. h. Umsetzung des Least-Privilege-Prinzips (vgl. [46], auch Need-To-Know-Prinzip genannt, [9: M2.8, M2.220]).
- Whitelisting-Regeln: Administrative Berechtigungen sollten explizit formulieren, was erlaubt ist. Alles andere ist verboten.
- Plausibilitätsprüfungen bei Durchführung von administrativen Tätigkeiten (z. B. Prüfung der Eingabe- und Ausgabedaten, Prüfung welcher Administrator eine Aufgabe durchführt und Prüfung des Zeitpunkts der Durchführung)
- Verschiedene Zugangsdaten (wie Passwörter) für unterschiedliche Zwecke verwenden [12, 30]
- Reduktion der Verwendung von hoch privilegierten AD-Konten [46] und Fragmentierung administrativer Berechtigungen in verschiedene Accounts
- Einsatz von Werkzeugen zur Gewaltenteilung[1], wie beispielsweise das Mehr-Augen-Prinzip bei wichtigen Administrationsaufgaben und die Trennung administrativer Verantwortungsbereiche
- Protokollierung und Überwachung administrativer Tätigkeiten (vgl. Abschnitt 3.3).

[1] Der Begriff Gewaltenteilung wird im Rahmen dieser Studie im Kontext des Berechtigungsmanagements verwendet und betrifft die Teilung von Zugriffsberechtigungen von Administratoren. Der Begriff ist nicht im Sinne der Teilung staatlicher Gewalten zu verstehen.

Vorsätzliche Handlungen von Administratoren

Administratoren können Ziel eines Angriffs werden, jedoch auch aus eigenem Antrieb und mittels vorsätzlicher Handlungen die von ihnen verwalteten Systeme angreifen und schwächen. Zu den vorsätzlichen Handlungen zählen beispielsweise die Ausnutzung der weiterführenden Berechtigungen

- für den unberechtigten Zugriff auf vertrauliche Informationen (Ausspähen von Informationen),
- für die Installation von Trojanern oder das Abschalten bzw. die Deinstallation von Sicherheitssoftware,
- für die absichtliche Falschkonfiguration von Systemen, so dass Sicherheitsrisiken oder konkrete Schwachstellen entstehen (z. B. die unberechtigte Freischaltung von IP-Adressen und Ports in der Firewall),
- für die Ausweitung der administrativen Berechtigungen (engl. *privilege escalation*) durch die unberechtigte Vergabe von Berechtigungen.

Hierbei sind zwei Arten von Angriffen hervorzuheben, welche in der Regel schwieriger zu erkennen sind:

1. *Mehrstufige Angriffe:* Angriffe dieser Art erfolgen in mehreren Schritten, wobei einzelne Schritte voneinander abhängen können und die Reihenfolge der Schritte relevant sein kann. Einzelne Schritte schaffen dabei die Voraussetzung für nachfolgende Schritte. So gelingt es dem Angreifer, sich sukzessive weiter zum Ziel seines Angriffs vorzuarbeiten.

   Diese Angriffe sind natürlich nicht nur auf Administratoren beschränkt, sondern werden auch von externen Angreifern angewendet. Bei mehrstufigen Angriffen durch Administratoren können jedoch die beim Angriff hinterlassenen Spuren schrittweise beseitigt werden.

2. *Angriffe durch kooperatives Fehlverhalten:* Diese Art von Angriff ist ein Spezialfall eines mehrstufigen Angriffs, bei dem die verschiedenen Schritte von unterschiedlichen kooperierenden Angreifern durchgeführt werden. Da jeder Administrator jeweils nur einen kleinen Teil des Angriffs durchführt und dabei möglicherweise nur seine zugewiesenen Berechtigungen ausnutzt, sind solche Angriffe für technische Sicherungssysteme schwer zu erkennen.

Die im vorherigen Abschnitt genannten Beispiele für Maßnahmen finden auch Anwendung zum Schutz vor vorsätzlich handelnden Administratoren. Hierbei ist jedoch zu berücksichtigen, dass ein Administrator als handelnder Akteur über viel umfangreicheres Detailwissen über die verwendeten Systeme und Netzwerke verfügt als ein externer Angreifer und so leichter unentdeckt bleiben kann.

3.3 Protokollierung und Überwachung

Zur Beurteilung der Sicherheit eines Systems im laufenden Betrieb ist es wichtig, den aktuellen Zustand des Systems und seiner einzelnen Systemkomponenten zu ermitteln. Hierzu zählt beispielsweise die Überprüfung,

- ob alle Systemkomponenten wie gewünscht funktionieren,
- ob und welche Fehler aufgetreten sind,
- ob versucht wurde, auf Systemkomponenten unberechtigterweise Zugriff zu erhalten,
- ob die etablierten Sicherheitsmaßnahmen (wie Firewalls oder Sicherheitsgateways) funktionieren und
- ob die Konfigurationen der Systemkomponenten (wie Portfreigaben in der Firewall oder Zugriffsrechte von Mitarbeitern und Administratoren im Berechtigungsmanagement) verändert wurden.

Neben der bloßen Beurteilung der Sicherheit kann eine Organisation auch verpflichtet sein, die Wirksamkeit der umgesetzten Sicherheitsmaßnahmen regelmäßig zu überprüfen. Auch der IT-Grundschutz listet hierzu einige Gefährdungen auf, die durch unzureichende Kontrollen von Sicherheitsmaßnahmen entstehen und schlägt Gegenmaßnahmen vor (vgl. [9: G 2.4, G 2.131, M 2.64, M 2.65]). Die Durchführung von Wirksamkeitsprüfungen in der Praxis wurde beispielsweise in der aktuellen Sicherheitsstudie [31] von <kes> und Microsoft ermittelt. Es wurde u. a. untersucht, welcher Anteil der Befragten angab, dass ihr Unternehmen die Einhaltung vorgesehener Sicherheitsmaßnahmen prüft. Hierbei gaben 84% der Befragten an, dass solche Prüfungen stattfinden, jedoch finden diese Prüfungen mit einem Anteil von 53% überwiegend anlassbezogen statt. Die Studie fand weiterhin heraus, dass regelmäßige Prüfungen nur bei 34% der großen Unternehmen stattfinden. Bei 13% der großen Unternehmen wird die Einhaltung von Sicherheitsmaßnahmen gar nicht geprüft. Regelmäßige Wirksamkeitstests sind auch im neuen europäischen Datenschutzgesetz, der Datenschutzgrundverordnung, verankert (vgl. [23: Art. 32 Abs. 1 Lit. d]), welches das bestehende Bundesdatenschutzgesetz am 28. Mai 2018 ablösen wird.

Zur Beurteilung der Systemsicherheit und zur Wirksamkeitsprüfung werden i. d. R. zwei unterschiedliche Maßnahmen eingeführt: die Protokollierung aller sicherheitskritischen Aktionen und die kontinuierliche Überwachung (engl. *monitoring*) des Systems und seiner Komponenten. Eine scharfe Trennung der beiden Begriffe Protokollierung und Überwachung ist hierbei nicht immer möglich. Häufig werden die Sicherheitsmaßnahmen Protokollierung und Überwachung komplementär genutzt. Tabelle 3.1 listet Eigenschaften auf, die den Begriffen Protokollierung und Überwachung in der praktischen Verwendung zugeschrieben werden.

Tabelle 3.1: Eigenschaften von Protokollierung und Überwachung

Protokollierung	Überwachung
Reaktiv: durch ein Ereignis initiiert	Proaktiv: kontinuierliche oder regelmäßig stattfindende Überprüfungen
Passiv: Mitschreiben von Ereignissen, i. d. R. kein Auslösen von Aktionen	Aktiv: Überprüfung des Systemzustands mittels Regeln, die beschreiben, welche Eigenschaften immer erfüllt sein müssen, bzw. niemals eintreten dürfen. Auslösen einer Aktion bei Regelverletzung (beispielsweise Benachrichtigung des verantwortlichen Mitarbeiters, Erzeugung eines Sicherheitsvorfalls oder Protokollierung des Sicherheitsvorfalls)
Retrospektiv: Geeignet für forensische Analysen (z. B. die nachträgliche Aufklärung eines Sicherheitsvorfalls mittels digitaler Forensik) und für statistische Zwecke (z. B. Anzahl der fehlerhaften Authentifizierungsversuche beim VPN-Server im letzten Monat)	Prospektiv: Geeignet zur regelmäßigen Überprüfung der Wirksamkeit von Sicherheitsmaßnahmen (z. B. ob die Firewall wie gewünscht läuft)

Betrachtungsgegenstand

Die Protokollierung und Überwachung kann verschiedenste Aspekte oder Eigenschaften eines Systems während des Betriebs berücksichtigen, beispielsweise

- Authentifizierungsversuche und Ressourcenzugriffen von Benutzern und Administratoren
- Installation, Deinstallation und Aktualisierung von Softwarekomponenten auf den Endgeräten der Benutzer
- Installation, Deinstallation und Aktualisierung von Softwarekomponenten auf Infrastrukturkomponenten (wie Firewalls, Sicherheitsgateways oder Domain Controller)
- Sicherstellung der Einhaltung von Sicherheitsmaßnahmen, wie beispielsweise
  - Prüfung der Funktion und Verfügbarkeit von Komponenten
  - Prüfung von Konfigurationen in Infrastrukturkomponenten
  - Änderungen im Identitätsmanagement und Berechtigungsmanagement (inkl. Rollen-/Gruppenzugehörigkeiten) von Benutzern und Administratoren (insbesondere auch die Abgrenzung von administrativen Verantwortlichkeiten und Gewaltenteilungsmaßnahmen)

Protokollierung und Überwachung in verteilten Umgebungen

Die Verwendung von Protokollierung und Überwachung in verteilten Umgebungen und in Outsourcing-Szenarien bedarf besonderer Sorgfalt, Schendel [42] beschreibt hierzu in seinem Artikel wichtige Problembereiche wie die Manipulationssicherheit, chronologischer Nachweis (engl. *chain of custody*), Log-Zyklen, Erzeugung und Auswertung von Systemzuständen (engl. *snapshots*).

Für die Verwendung in verteilten Umgebungen existieren spezielle Protokollierungswerkzeuge. Diese erlauben es, die Eigenschaften der beteiligten Systemkomponenten mittels Sensoren und Skripten zu ermitteln und diese Informationen zur Auswertung an die zentrale Auswertungslogik zu übertragen.

Abhängigkeiten zum Change Management

Wird bei der Überwachung ein Sicherheitsvorfall ausgelöst, dann muss in der Regel manuell geprüft werden, ob die Verletzung der geprüften Systemeigenschaft tatsächlich erfolgt ist, oder ob ein falscher Alarm ausgelöst wurde, beispielsweise eine Konfigurationsänderung ohne Anpassung der zugehörigen Überwachungsregel. Sofern ein Change-Management-Werkzeug eingesetzt wird, in welchem auch wichtige Änderungen der Systemkonfiguration protokolliert werden, kann leichter festgestellt werden, ob ein falscher Alarm vorliegt oder nicht.

Verfügbarkeit und Manipulationssicherheit

Wird eine Protokollierungs- oder Überwachungskomponente eingesetzt, um den Systemzustand zu ermitteln, Sicherheitsvorfälle zu entdecken oder die Wirksamkeit von Sicherheitsmaßnahmen zu prüfen, dann ist darauf zu achten, dass diese Komponenten hochverfügbar sind und Ausfälle umgehend entdeckt werden. Außerdem müssen sie vor Missbrauch und Manipulation geschützt werden, so dass es einem Angreifer nicht möglich ist, die Komponenten zu umgehen bzw. Daten nachträglich zu manipulieren. Weiterhin muss die Verantwortlichkeit für die Protokollierungs- und Überwachungskomponente geklärt werden (vgl. auch [2]).

Datenschutz, Privatsphäre und Leistungskontrolle

Der Einsatz von Protokollierung und Überwachung muss stets im Einklang mit existierenden Bestimmungen erfolgen, wie beispielsweise dem Schutz der Privatsphäre, dem persönlichen Datenschutz, den Persönlichkeitsrechten der Mitarbeiter und dem Recht auf informationelle Selbstbestimmung. Weiterhin dürfen derartige Maßnahmen nicht zur Leistungsmessung herangezogen werden.

Maßnahmen wie die Protokollierung und Überwachung aber auch Gewaltenteilungsinstrumente bei Administratoren erhöhen einerseits den Druck auf Administratoren, können jedoch auch dazu beitragen, Administratoren zu entlasten, da mittels dieser Werkzeuge Verdachtsmomente vorsätzlicher Handlungen ausgeschlossen werden können.

3.4 Systemkonfiguration

Die Funktionsweise von Systemkomponenten ist in der Regel von deren Konfiguration abhängig. Eine fehlerhafte Konfiguration kann dazu führen, dass Systeme nicht ordnungsgemäß oder erwartungsgemäß funktionieren. Insbesondere können fehlerhafte Konfigurationen zu Schwachstellen in Systemen führen. Besonders kritisch sind hierbei Konfigurationen von Komponenten, welche die Sicherheit eines Systems sicherstellen bzw. verbessern sollen.

Konfigurationen kommen an vielen unterschiedlichen Stellen vor, beispielsweise beim

- Identitätsmanagement (für normale Benutzer und Administratoren),
- Berechtigungsmanagement (für normale Benutzer und Administratoren),
- Management von Domänen,
- Management von Firewalls,
- Management von Sicherheitsgateways und
- Management der Softwareverteilungskomponente.

Die meisten Konfigurationen ändern sich über die Zeit und unterliegen damit einer Dynamik. In der Regel hat sich die aktuelle Konfiguration sukzessive aus vorherigen Versionen entwickelt. Leider ist hierbei oft der Trend zu erkennen, dass Konfigurationen lediglich ergänzt werden, statt als Ganzes betrachtet und ggf. neu strukturiert oder vereinfacht zu werden. Das Unternehmen Firemon befragte im Rahmen der Europäischen Sicherheitsmesse Infosecurity Europe 2016 insgesamt 300 Sicherheitsexperten zu ihren Firewall-Regeln [10]. 65% der Befragten gaben an, dass sie mit Schwierigkeiten rechnen müssten, falls der Zustand ihrer Firewall-Konfiguration bekannt würde, 50% der Befragten rechnete sogar mit „lebenslangem Stubenarrest“. Die gleiche Studie zeigte auch, dass 32% der Befragten mehr als die Hälfte der Firewall-Regeln von ihren Vorgängern übernommen haben und dass es 25% der Befragten vermeiden, bestehende Firewall-Regeln zu deaktivieren. In einer weiteren Studie [25] gaben die Befragten an, dass die Optimierung des Firewall-Regelwerks die größte Herausforderung beim Einsatz von Firewalls ist. Auch der BSI-Leitfaden Informationssicherheit [8] beschreibt am Beispiel von Firewall-Regeln die Gefahr, dass sich Konfigurationen allmählich aufblähen und unübersichtlicher werden. Der Leitfaden empfiehlt, für Firewalls regelmäßig zu prüfen, ob die bestehenden Filterregeln noch konsistent sind, ob sie vereinfacht werden können und ob sie noch hinreichend restriktiv sind.

Diese Empfehlungen lassen sich auch auf andere Konfigurationen verallgemeinern, insbesondere für solche Konfigurationen, bei denen sich die Gesamtkonfiguration aus einer Menge von einzelnen Konfigurationsregeln ergibt. Hier einige Beispiele:

- Beim Berechtigungsmanagement gibt es in der Praxis beispielsweise die Tendenz, dass Benutzer im Laufe der Zeit sukzessive neue Berechtigungen erhalten, sofern neue Aufgabenbereiche hinzukommen, jedoch umgekehrt nur sehr selten geprüft wird, ob vorhandene Berechtigungen überhaupt noch benötigt werden.

- Gleiches gilt nicht nur für normale Benutzer, sondern auch für Administratoren. In der Praxis besitzen Administratoren häufig mehr Berechtigungen als für ihren Verantwortungsbereich (inkl. Vertretungsregelungen) notwendig sind. Gleichermaßen gibt es administrative Verantwortungsbereiche, denen mehr Administratoren zugewiesen sind, um den normalen Betrieb und Vertretungssituationen zu meistern.
- Auch hinsichtlich des Zugriffs von Benutzern auf Netzwerkressourcen besteht die Gefahr, dass zu viele Freigaben bzw. zu viele Berechtigungen von Benutzern auf Freigaben bestehen.
- Weitere Beispiele für fehlerhafte Konfigurationen und deren Ursachen werden auch in den Abschnitten 3.2.1 und 3.2.2 beschrieben.

Oft werden Konfigurationsänderungen dann durchgeführt, wenn in dringenden Situationen technische Probleme oder Probleme beim Zugriff auf Ressourcen bestehen. Aufgrund der Dringlichkeit werden dann temporäre Ausnahmen konfiguriert, die aber nach Lösung der Probleme nicht wieder entfernt werden.

Fehlerhafte Konfigurationen können die effektive Sicherheit eines Systems (siehe Abschnitt 3.1.1) negativ beeinflussen, insbesondere dann, wenn eine Konfiguration redundante Regeln enthält. Wird beispielsweise der Zugriff auf eine Systemressource durch mehrere Konfigurationsregeln erlaubt, dann genügt es nicht, eine der Regeln zu entfernen, um den Zugriff zu verhindern, da der Zugriff weiterhin über eine der übrigen Konfigurationsregeln möglich sein kann.

Zur Vermeidung solcher Probleme sollten u. a. die o. g. Empfehlungen des BSI berücksichtigt werden. Zusätzlich sollten Anpassungen der Konfiguration und deren zugehörigen Gründe dokumentiert werden, beispielsweise durch Einsatz eines Werkzeugs für das Veränderungsmanagement (engl. *change management*). Eine solche Dokumentation erlaubt es einerseits, die aktuelle Konfiguration zu einem späteren Zeitpunkt besser zu verstehen, und anderseits, temporäre Änderungen der Konfiguration leichter zu entfernen.

3.5 Sicherheitsaspekte beim Outsourcing

Findet ein Teil der Datenverarbeitung außerhalb der eigenen Organisation oder des eigenen Unternehmens statt, sind weitere Sicherheitsaspekte zu berücksichtigen. Hierbei gibt es ganz unterschiedliche Arten ausgelagerter Datenverarbeitung, beispielsweise die Speicherung von Geschäftsdaten in ausgelagerten Rechenzentren, ausgelagerte Dienste wie die E-Mail-Kommunikation oder Unternehmenskalender, ausgelagertes Systemmanagement und ausgelagerte Sicherheitsdienste.

Die Auslagerung der Datenverarbeitung ist ein anhaltender Trend, aus unterschiedlichen Gründen, aber unabhängig der Größe des Unternehmens. Der BSI-Grundschutz 2016 [9] hat inzwischen dem Thema einen eigenen Baustein B 1.11 (Outsourcing) gewidmet und empfiehlt verschiedene Maßnahmen zur Absicherung von Outsourcing-Szenarien, wie z. B. die Maßnahmen M 2.90 (Überprüfung der Lieferung), M 4.65 (Test neuer Hard- und Software) und M 2.226 (Regelungen für den Einsatz von Fremdpersonal). Der Grundschutz verweist in Baustein B 1.11 an mehreren Stellen auf ein

weiteres Dokument „IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“ [7], eine themenspezifische Ergänzung des Grundschutzkatalogs. Darin heißt es, dass eine „Auslagerung von Tätigkeiten oder Aufgaben [. . .] nur dann für eine IT-Grundschutz-Zertifizierung relevant [ist], wenn die folgenden Bedingungen alle erfüllt sind: Die Bindung an den Dienstleister erfolgt auf längere Zeit und durch die Dienstleistung kann die IT-Sicherheit des Auftraggebers beeinflusst werden und im Rahmen der Dienstleistung erbringt der Dienstleister auch regelmäßig nennenswerte IT-Sicherheitsmanagement-Tätigkeiten“ [7].

Outsourcing-Szenarien sind durch die beiden Rollen des Auftraggebers und des Dienstleisters charakterisiert. Der Auftraggeber gibt mit der Beauftragung eines Dienstleisters einen Teil seines Einflussbereichs und seiner Kontrolle über die zu verarbeiteten Daten an den Dienstleister, in der Regel ein externes Unternehmen, ab. Hierbei sind die eigenen Geschäftsprozesse häufig sehr eng mit den Dienstleistungen des externen Dienstleisters verknüpft. Dennoch ist die Anbindung weniger direkt als bei unternehmensinterner Verarbeitung. Daher sind bei der Auswahl des Dienstleisters einerseits das Vertrauen des Auftraggebers in den Dienstleister, wie auch Kontroll- und Überwachungsmöglichkeiten des Auftraggebers beim Dienstleister zu berücksichtigen.

Vergrößerung der Angriffsoberfläche

Häufig werden vom Dienstleister wichtige Unternehmensinformationen verarbeitet. Daher sind Sicherheitsziele wie die Vertraulichkeit, die Integrität und die Verfügbarkeit der Informationen bei der Entscheidung für Outsourcing und bei der Wahl eines Outsourcing-Dienstleisters zu berücksichtigen.

Werden die Daten extern verarbeitet, müssen diese aus technischer Sicht i. d. R. über Netzwerke zwischen Auftraggeber und Dienstleister übertragen werden. Hierbei ist die Sicherheit der Kommunikationsverbindungen zu berücksichtigen und ggf. zusätzliche technische Sicherheitsmaßnahmen, wie der Einsatz authentischer und verschlüsselter Kommunikationsverbindungen (z. B. mittels HTTPS oder VPN), einzuführen. Durch die externe Datenverarbeitung werden häufig zusätzliche Kommunikationsschnittstellen und -protokolle eingesetzt (z. B. das REST-Protokoll), dies impliziert Konfigurationsanpassungen. So müssen i. d. R. Firewall-Regeln, Benutzer- oder Dienstkonten und Berechtigungen angepasst werden. Die damit einhergehenden Gefahren wurden im vorherigen Abschnitt beschrieben.

Beim Outsourcing wird die Dienstleistung nicht durch die eigenen Mitarbeiter erbracht, sondern durch fremde Benutzer, die Mitarbeiter des Dienstleisters. Hierdurch vergrößert sich die Anzahl der Benutzer, welche direkt oder indirekt Zugriff auf die Daten haben können, und welche versehentlich oder vorsätzlich Daten verändern oder abhören können.

Weitere Sicherheitsprobleme können entstehen, da die entfernte Verarbeitung über Netzwerke unter Umständen fehleranfälliger ist, längere Laufzeiten hat und aktuelle Informationen nicht ausgetauscht werden können.

Outsourcing und Zentralisierung

Die Gründe für die Entscheidung, Outsourcing einzuführen, sind vielfältig. In größeren Organisationen und Unternehmen kommt es häufig vor, dass in den verschiedenen Organisationsteilen genutzte Systeme und Dienste in Hinblick auf eine Homogenisierung und Zentralisierung ausgelagert und zukünftig durch einen Dienstleister erbracht werden. Aus Sicht der einzelnen Organisationsteile werden diese Dienste dann zentral erbracht, während aus Dienstleistersicht die unterschiedlichen Organisationsteile ggf. als eigenständige Auftraggeber separat verwaltet werden müssen. Neben unterschiedlichen Systemkonfigurationen können sich auch die organisatorischen Abläufe der einzelnen Organisationsteile unterscheiden.

Die Zentralisierung bisheriger Dienste kann sich einerseits vorteilhaft auf die Sicherheit eines Systems auswirken, da Dinge nun einheitlich und gleichförmig gestaltet oder konfiguriert sind. Auf der anderen Seite birgt Zentralisierung aber auch die Gefahr, dass im Falle von Problemen, Fehlern oder Ausfällen viele beteiligte Systeme und Organisationsteile betroffen sind. Diese Nachteile können jedoch teilweise durch Maßnahmen zur Erhöhung der Ausfallsicherheit ausgeglichen werden.

Mandantenfähigkeit der eingesetzten Systeme

In der Regel erbringt ein Outsourcing-Dienstleister die Dienstleistungen nicht ausschließlich für einen einzigen Kunden, sondern für eine Vielzahl von Kunden. Aus Sicherheitssicht müssen hierbei verschiedene technische und organisatorische Aspekte berücksichtigt werden, die unter dem Stichwort Mandantenfähigkeit zusammengefasst werden. So müssen einerseits die für die verschiedenen Kunden genutzten Systeme und Netze des Dienstleisters gegenseitig abgeschottet werden, damit verhindert wird, dass Kunden Informationen über andere Kunden oder unberechtigt Zugriff auf deren Prozesse oder Systeme erhalten können. Dies gilt sowohl für physische als auch virtualisierte Systeme. Gleichzeitig müssen aber auch organisatorische Regelungen eingeführt werden, hinsichtlich der Zuständigkeiten von Mitarbeitern des Dienstleisters für verschiedene Kunden, um Interessenskonflikte beim Dienstleister zu vermeiden.

3.6 Sicherheitsaspekte bei der Softwareverteilung

Nach der Einführung der Grundlagen von Softwareverteilung im Abschnitt 2 werden nachfolgend einige wichtige Aspekte sicherer Softwareverteilung beschrieben.

Administrative Gewaltenteilung

Der Prozess der Softwareverteilung besteht aus mehreren Teilprozessen wie das Orchestrieren, Herunterladen, Paketieren, Testen, Verteilen und dem eigentlichen Installieren auf den Endgeräten. Um Anwendungsfehler von Administratoren und vorsätzliches Fehlverhalten (wie beispielsweise das Einschleusen von Schadsoftware) zu verhindern bzw. zu reduzieren, sollten die verschiedenen Teilprozesse durch unterschiedliche Personen administriert werden. D. h. ein Administrator, der ein Softwarepaket packt, darf

beispielsweise nicht dafür zuständig sein, dieses Softwarepaket zu testen oder zu verteilen. Die administrative Gewaltenteilung ist auch bei der Softwareverteilung ein wirksames Mittel, administrative Fehler, Administratoren als Angriffsziele und vorsätzlich handelnde Administratoren zu erkennen (vgl. Abschnitt 3.2.2), jedoch nur bedingt bei kooperierenden, vorsätzlich handelnden Administratoren.

Absicherung der Software Deployment Pipeline

Bass et al. [3] nennen die Aneinanderreihung der verschiedenen Teilprozesse der Softwareverteilung die sogenannte *Software Deployment Pipeline*. Innerhalb dieser Software Deployment Pipeline können Fehler und Angriffsversuche in jedem Teilprozess auftreten. Des Weiteren können Angreifer versuchen, die Aneinanderreihung der Teilprozesse zu verändern, indem sie versuchen, Teilprozesse zu überspringen oder die Reihenfolge der Teilprozesse verändern. Daher muss nach Bass et al. die Softwareverteilungskomponente sicherstellen, dass sowohl die einzelnen Teilprozesse als auch die Verbindung der einzelnen Teilprozesse abgesichert ist und die Software Deployment Pipeline vollständig durchlaufen wird. Um dies zu erreichen, schlagen sie einerseits vor, sichere Kommunikationskanäle (beispielsweise SSL, TLS) zwischen Komponenten, sowie HMACs oder digitale Signaturen einzusetzen, mit denen z. B. die Authentizität und Integrität der kommunizierenden Teilprozesse und der ausgetauschten Installationspakete abgesichert werden kann. Weiterhin plädieren sie für den Einsatz von Checksummen, gegenseitige Authentifizierung der beteiligten Dienstkonten, Anwendung des Least-Privilege-Prinzips für Berechtigungen und administrative Gewaltenteilung hinsichtlich der verschiedenen beteiligten Komponenten.

Softwareupdates in komplexen Systemen

Softwareupdates dienen neben der Installation neuer Funktionen oder der Verbesserung der Leistungsfähigkeit von Programmen auch dazu, Programmfehler zu beheben. Dumitras et al. diskutieren in [21] die Problematik von administrationsdomänenübergreifenden Softwareupdates. Sie weisen auf die besondere Problematik hin, wenn ein Softwareupdate verschiedene Systeme (wie beispielsweise Server-Komponenten und verschiedenen Endgeräte) einschließt. Hierbei kann die Situation entstehen, dass diese verschiedenen Systeme häufig in unterschiedliche administrative Verantwortlichkeiten fallen und daher Softwareupdates gut koordiniert werden müssen, damit die Funktionalität und Verfügbarkeit der Software auch nach dem Update erhalten bleibt. Sie kommen zu dem Schluss, dass in solchen Fällen das Risiko abgewogen werden muss, ob es gefährlicher ist, die Installation eines Softwareupdates zu verzögern und mehr Zeit für die Tests des Softwareupdates im Zusammenspiel mit den zugehörigen Updates weiterer Komponenten zu verbringen oder die Softwareupdates möglichst schnell auszurollen und ggf. Sicherheitslücken schnell zu schließen, dafür aber Gefahr zu laufen, dass inkompatible Softwareteile die Funktionalität der Anwendung beeinträchtigen. Dumitras et al. schlagen hierzu in [21] ein Modell vor, um diese beiden Risiken gegeneinander abzuwägen.

4 Softwareverteilung mittels Microsoft SCCM

Dieses Kapitel gibt einen Überblick über *Microsoft System Center Configuration Manager 2012* (SCCM 2012) und die innerhalb einer SCCM-Infrastruktur benötigten Komponenten. Im Anschluss werden typische Sicherheitsaspekte beim Einsatz von Microsoft SCCM diskutiert. Der Fokus der Betrachtungen in diesem Kapitel liegt auf der Softwareverteilung mittels Microsoft SCCM über Domänengrenzen hinweg. Alle Aussagen in diesem Kapitel beziehen sich auf Microsoft SCCM 2012.

4.1 Überblick über Microsoft SCCM

Bei *Microsoft System Center Configuration Manager 2012* (SCCM) handelt es sich um eine Lösung zur Systemverwaltung (vgl. Abschnitt 2.1). Eine der Kernaufgaben von SCCM ist die Verteilung und Installation von Softwarepaketen auf den Endgeräten. Eine typische SCCM-Infrastruktur besteht aus einer Hierarchie von Systemservern (*Sites*), an deren Spitze die *Central Administration Site* (CAS) steht [24, 39]. Abbildung 4.1 zeigt eine solche SCCM-Hierarchie.

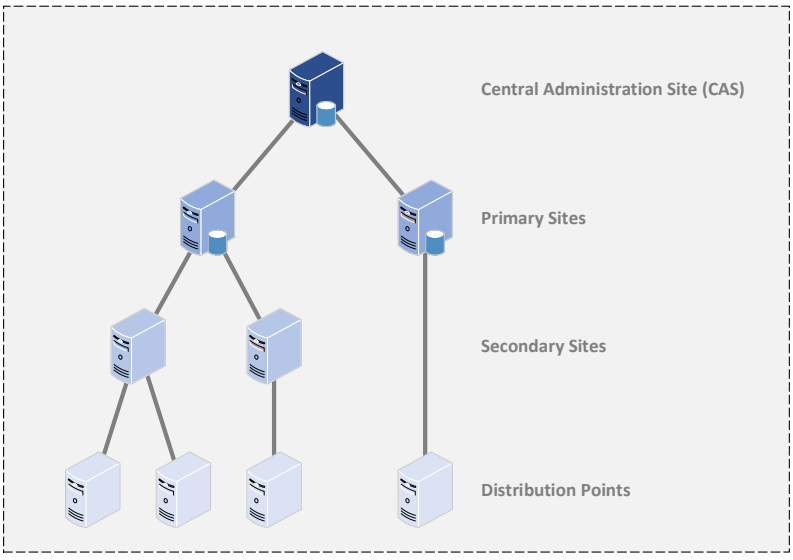

Abbildung 4.1: SCCM Hierarchie

Central Administration Site. Die CAS stellt die zentrale Verwaltungs- und Reporting-Komponente von SCCM 2012 dar. Die CAS ist zwingend erforderlich, wenn mehr als eine Primary Site betrieben werden sollen.

Primary Site. Die Primary Sites verwalten die ihnen zugewiesenen Endgeräte (bis zu 100.000 Stück).

Secondary Site. Secondary Sites erweitern eine Primary Site und können daher nur unterhalb einer Primary Site betrieben werden. Secondary Sites können in Szenarien eingesetzt werden, in denen nur eine langsame Netzwerkverbindung zwischen den Endgeräten und der Primary Site besteht. Die Verwaltung der Endgeräte erfolgt jedoch nach wie vor in der Primary Site.

Distribution Point. Die Distribution Points stellen die zu verteilende Software (Softwarepakete, Softwareupdates, Betriebssystem-Images usw.) für die ihnen zugewiesenen Endgeräte bereit. Diese Software wird über die Primary Sites bzw. Secondary Sites an die Distribution Points verteilt. Alternativ kann ein Distribution Point die Softwarepakete auch über einen Pull-Mechanismus von einem anderen Distribution Point beziehen [24].

Daneben gibt es noch weitere (optionale) Komponenten, auf die in diesem Ratgeber jedoch nicht weiter eingegangen wird, da sie für die weiteren Betrachtungen nicht relevant sind.

Auf den Endgeräten muss ein spezieller SCCM-Client (Configuration Manager Client) vorhanden sein. Im Rahmen der Softwareverteilung lädt der Configuration Manager Client die Softwarepakete von dem Distribution Point herunter und installiert sie auf dem Endgerät. Das bedeutet, die Softwareverteilung mittels Microsoft SCCM erfolgt über ein Pull-Verfahren (vgl. Abschnitt 2.3).

Die Kommunikation zwischen den SCCM-Komponenten erfolgt bidirektional. Softwarepakete werden ausgehend von der CAS in der SCCM-Hierarchie nach unten über Primary Sites und Secondary Sites bis zu den Distribution Points geleitet (*Content Replication*). Die SCCM-Clients auf den Endgeräten senden in regelmäßigen Abständen Inventarinformationen und Statusmeldungen an ihre jeweilige Primary Site oder Secondary Site. Von dort werden diese Daten in der Hierarchie nach oben bis zur CAS geleitet, wo sie zentral verwaltet werden. Es ist offensichtlich, dass sich der überwiegende Teil des Netzwerkverkehrs innerhalb der SCCM-Hierarchie von oben nach unten bewegt (verursacht durch die übertragenen Softwarepakete).

4.2 Einsatz von Microsoft SCCM über Domänengrenzen hinweg

Microsoft SCCM kann in Szenarien eingesetzt werden, in denen die einzelnen SCCM-Komponenten in unterschiedlichen Netzen betrieben werden, die wiederum in unterschiedlichen Active-Directory-Domänen angesiedelt sind („domänenübergreifendes SCCM"). Dies ist insbesondere auch in Domänen möglich, zwischen denen prinzipiell keine Vertrauensbeziehungen bestehen.

Bevor auf solche Szenarien näher eingegangen wird, werden zunächst im Rahmen eines Exkurses die Vertrauensbeziehungen zwischen Active-Directory-Domänen vorgestellt.

4.2.1 Exkurs: Vertrauensbeziehungen zwischen Active-Directory-Domänen

Active Directory ist ein Verzeichnisdienst von Microsoft, mit dessen Hilfe Domänen (d. h. Namensräume) verwaltet werden. Unternehmen oder Organisationen können mehrere Active-Directory-Domänen betreiben. Sind diese Domänen in einer hierarchischen Struktur unter einer so genannten Root-Domäne angeordnet, dann bilden diese Domänen einen *Domain Tree* oder kurz *Tree* (vgl. auch Abbildung 4.2) [38]. In einem solchen Tree sind auch die Namen der einzelnen Domänen hierarchisch unterhalb des Namens der Root-Domäne angeordnet, sie bilden einen Namensraum.

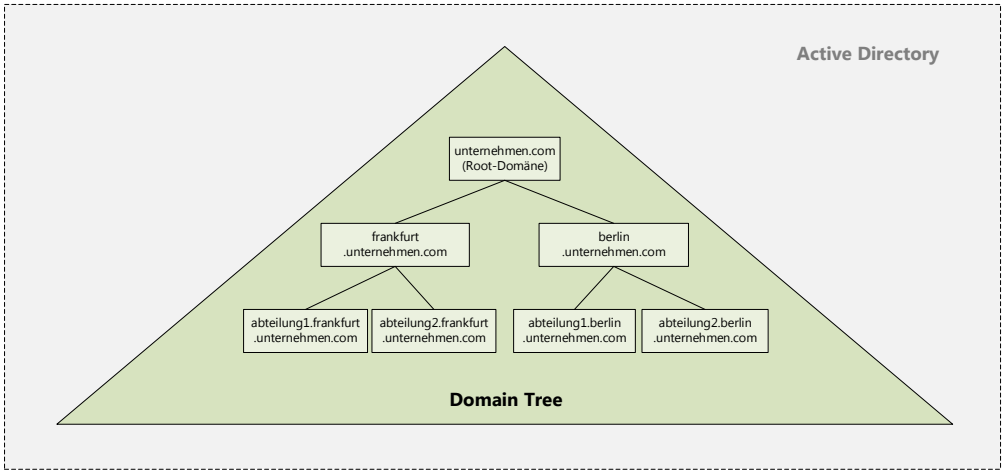

Abbildung 4.2: Active Directory Domänenbaum

Werden innerhalb eines Verzeichnisdienstes (Active-Directory-Instanz) mehrere Trees und somit mehrere unabhängige Namensräume verwaltet, entsteht ein *Forest* [38]. Ein Forest ist also eine Menge an Trees innerhalb einer Active-Directory-Instanz[1]. Abbildung 4.3 zeigt einen Forest bestehend aus zwei Trees. Hierbei ist zu beachten, dass in einem solchen Forest die als erstes erzeugte Domäne eine besondere Rolle einnimmt (*Forest-Root-Domäne*). Die Administratoren dieser Forest-Root-Domäne besitzen weitreichende Berechtigungen im gesamten Forest (vgl. hierzu auch IT-Grundschutzkataloge, Maßnahme M 3.64 [9]).

Innerhalb eines Forest bestehen bidirektionale transitive Vertrauensbeziehungen zwischen den Domänen der einzelnen Trees [35]. Solche Vertrauensbeziehungen innerhalb eines Forest werden *Intraforest Trust* genannt. Wird eine neue Domäne erzeugt, besteht automatisch eine bidirektionale transitive Vertrauensbeziehung zu der ihr übergeordneten Domäne („Elterndomäne"). „Bidirektional" bedeutet, die beiden Domänen vertrauen sich gegenseitig. „Transitiv" bedeutet: Vertraut die Domäne *A* der Domäne *B* und vertraut die Domäne *B* der Domäne *C*, so besteht auch eine Vertrauensbeziehung zwischen Domäne *A* und Domäne *C*. Zudem bestehen immer bidirektionale transitive Vertrauensbeziehungen zwischen den Root-Domänen eines Forest. In dem in Abbildung 4.3 dargestellten Beispiel ist dies die Vertrauensbeziehung zwischen den Domänen *A1* und *B1*. Auf diese Weise besteht zwischen allen Domänen innerhalb eines Forests eine Vertrauensbeziehung. Dieser so genannte Vertrauenspfad zwischen zwei

[1] Eine Active-Directory-Instanz entspricht somit genau einem Forest.

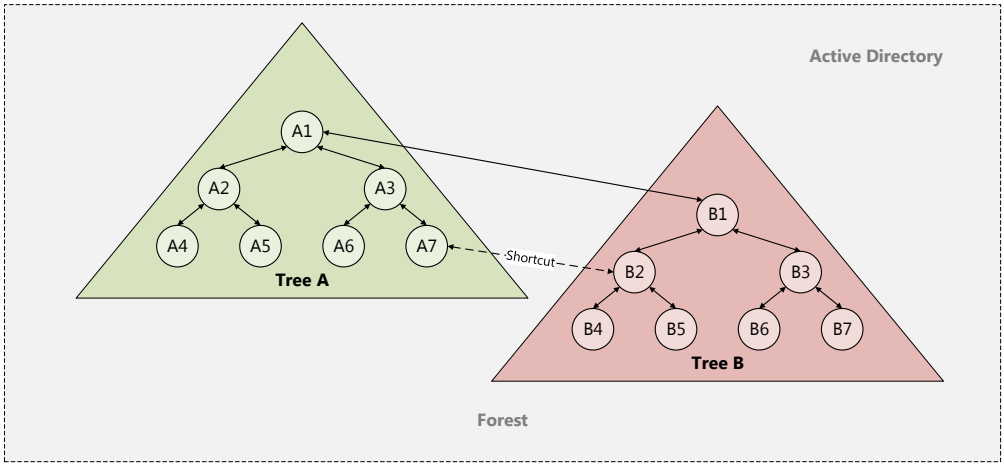

Abbildung 4.3: Active Directory Forest

Domänen kann somit über mehrere Domänen hinweg verlaufen. Der Vertrauenspfad zwischen den Domänen *A4* und *B3* in Abbildung 4.3 verläuft demnach über die Domänen *A2*, *A1* und *B1*. Da die Vertrauenspfade in komplexen Domänenstrukturen sehr lang werden können, ist es möglich, direkte Vertrauensbeziehungen zwischen zwei Domänen eines Forests zu etablieren (sogenannte *Shortcuts*). In Abbildung 4.3 besteht beispielsweise ein solcher Shortcut zwischen den Domänen *A7* und *B2*. Hierbei verläuft der Vertrauenspfad nicht über die übergeordneten Domänen hinweg, sondern direkt zwischen den beiden Domänen.

Große Unternehmen oder Organisationen betreiben häufig mehrere Active-Directory-Instanzen. Auf diese Weise entstehen mehrere Domänen-Forests. Zwischen Domänen aus unterschiedlichen Forests bestehen prinzipiell keine Vertrauensbeziehungen, sodass Zugriffe über Forest-Grenzen hinweg zunächst nicht möglich sind. Häufig ist es jedoch in solchen Unternehmen oder Organisationen erforderlich, dass Benutzer oder Geräte aus einer Domäne des Forests *A* Zugriff auf Ressourcen aus einer Domäne des Forests *B* benötigen. Um solche Zugriffe zu ermöglichen, müssen die Benutzer oder Geräte der Domäne aus Forest *A* auch in der Domäne aus Forest *B* authentifiziert und autorisiert werden können. Zu diesem Zweck muss explizit eine Vertrauensbeziehung zwischen den beteiligten Forests hergestellt werden, in Zusammenhang mit Microsoft Active Directory wird dies *Forest Trust* oder *Interforest Trust* genannt (siehe auch [36]). Ein Forest Trust ist immer eine transitive Vertrauensbeziehung zwischen zwei Forest-Root-Domänen. Besteht zudem eine gegenseitige (bidirektionale) Vertrauensbeziehung zwischen den beiden Forests, d. h. die Root-Domäne aus Forest *A* vertraut der Root-Domäne aus Forest *B* und andersherum, dann wird diese Vertrauensbeziehung *Cross Forest Trust* genannt.

Abbildung 4.4 zeigt exemplarisch einen Forest Trust zwischen zwei Active Directories. Hier wurde eine Vertrauensbeziehung von der Forest-Root-Domäne *A1* aus dem vertrauenden Forest (Active Directory *AD-1*) zu der Forest-Root-Domäne *C1* aus dem vertrauten Forest (Active Directory *AD-2*) etabliert. Das bedeutet, dass Benutzer oder Geräte aus einer Domäne des Active Directory *AD-2* in Active Directory *AD-1* authentifiziert werden können und es können für diese Benutzer oder Geräte Berechtigungen für den Zugriff auf Ressourcen innerhalb von Domänen in Active Directory *AD-1* erstellt

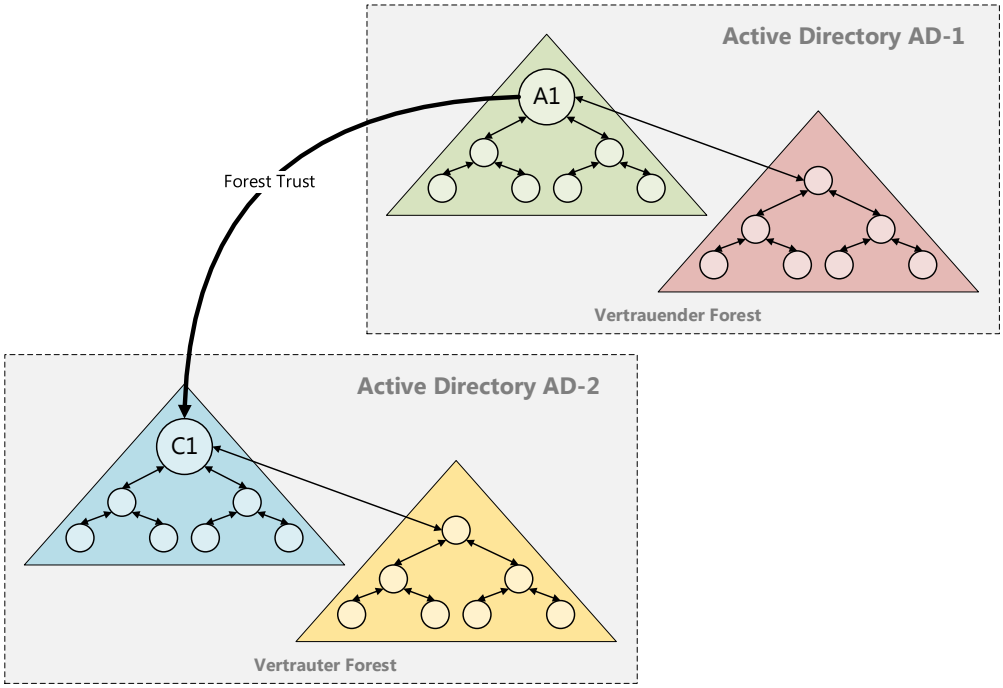

Abbildung 4.4: Active Directory Forest Trust

werden. Da es sich in dem Beispiel um keinen Cross Forest Trust handelt, besteht nur eine Vertrauensbeziehung von *AD-1* zu *AD-2*, aber nicht andersherum, Benutzer aus einer Domäne in Active Directory *AD-1* können weiterhin nicht in Active Directory *AD-2* authentifiziert werden.

4.2.2 Microsoft SCCM in Cross-Forest-Trust-Szenarien

In SCCM-Infrastrukturen greifen die einzelnen SCCM-Komponenten wechselseitig aufeinander zu. Wird SCCM 2012 in einem Szenario betrieben, in dem die SCCM-Komponenten in unterschiedlichen Domänen angesiedelt sind, welche sich zudem in unterschiedlichen Active Directory Forests befinden, muss für den Betrieb von SCCM 2012 ein Cross Forest Trust zwischen den beteiligten Active Directorys eingerichtet werden.

In dem in Abbildung 4.5 dargestellten Szenario besteht eine Kommunikationsbeziehung zwischen der CAS und der Primary Site, zwischen der Primary Site und der Secondary Site sowie zwischen der Secondary Site und dem Distribution Point. Die Kommunikation zwischen Primary Site und Secondary Site erfolgt hierbei über Domänengrenzen zwischen zwei Forests hinweg. Im Detail bedeutet dies, dass zum einen ein Dienstkonto der Primary Site und ein Datenbankkonto (beide Domäne *A*) schreibenden Zugriff auf die Secondary Site und deren Datenbank (Domäne *B*) benötigen. Zum anderen benötigen ein Dienstkonto der Secondary Site und ein Datenbankkonto (beide Domäne *B*) schreibenden Zugriff auf die Primary Site und deren Datenbank (Domäne *A*). Die Kommunikation ist somit wechselseitig, d. h. sie erfolgt in beide Richtungen. Aus diesem

Grund muss hierfür ein Cross Forest Trust zwischen den beiden Active Directorys eingerichtet werden. Über eine entsprechende Firewall-Konfiguration muss in diesem Fall dafür gesorgt werden, dass ausschließlich eine Kommunikation zwischen Primary Site und Secondary Site über Domänengrenzen hinweg möglich ist.

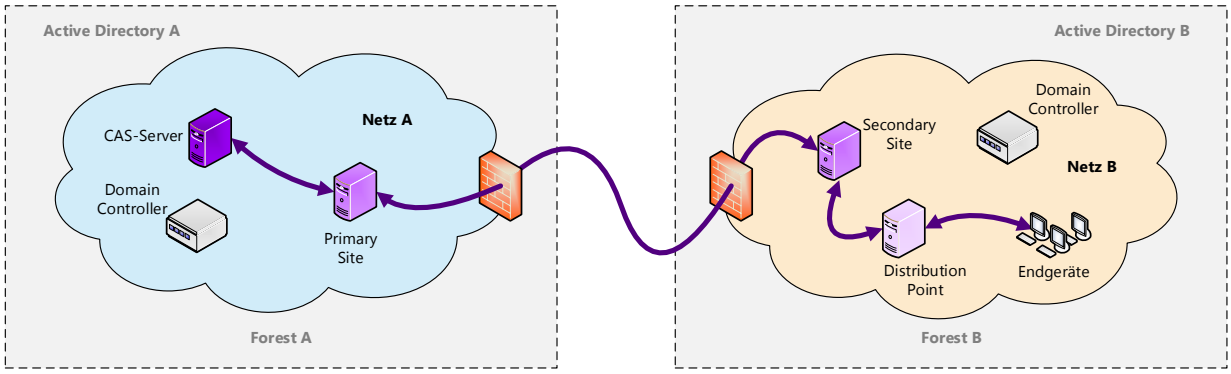

Abbildung 4.5: SCCM Cross Forest Trust

4.3 Sicherheitsaspekte von Cross Forest Trust bei domänenübergreifendem SCCM

Prinzipiell stellt ein Active Directory Forest eine Sicherheitsgrenze (engl.: *security boundary*) dar und definiert den maximalen Zugriffsbereich für Administratoren. Das bedeutet, dass kein Administrator von außerhalb eines Forests Rechte auf Ressourcen innerhalb des Forests besitzt. Daran ändert sich auch durch das Einrichten eines Forest-Trusts nichts: Durch das Etablieren einer Forest-Trust-Beziehung zwischen zwei Forests werden nicht automatisch die Berechtigungen der Administratoren der vertrauten Forest-Root-Domäne auf den vertrauenden Forest übertragen, sondern diese Berechtigungen müssen nach dem Einrichten des Forest Trust explizit erzeugt werden, sofern sie gewünscht sind. Des Weiteren impliziert das Einrichten eines Forest Trust zunächst nicht, dass dadurch Zugriffsberechtigungen auf Ressourcen des vertrauenden Forests für Benutzer oder Geräte des vertrauten Forest entstehen. Der Forest Trust ermöglicht es lediglich, solche Zugriffsberechtigungen zu definieren.

Trotzdem existieren Sicherheitsrisiken, die beim Einsatz von SCCM 2012 insbesondere in Cross-Forest-Trust-Szenarien eintreten können. Diese Sicherheitsrisiken werden im Folgenden diskutiert. Die betrachteten Sicherheitsrisiken beziehen sich ausschließlich auf Vertrauensstellungen zwischen sich vertrauenden Forests (*Interforest Trust*). Sicherheitsrisiken innerhalb eines Forests (*Intraforest Trust*) werden nicht betrachtet.

4.3.1 Zugriffsrechte von Administratoren auf mehrere Domänen

Ein böswilliger Administrator der vertrauten Domäne kann versuchen, die SID[2] eines Benutzers mit weitreichenden Zugriffsrechten auf Ressourcen der vertrauenden Do-

[2] Die SID (*Security Identifier*) bezeichnet in Microsoft Windows-Umgebungen eine interne Repräsentation eines Benutzers. Die SIDs werden insbesondere in *Access Control Lists* mit den Berechtigungen des Benutzers verknüpft.

mäne auszuspähen. Diese SID kann der böswillige Administrator dem „SID-History"-Attribut eines Benutzerkontos aus der vertrauten Domäne hinzufügen, welches unter seiner Kontrolle steht. Auf diese Weise erhält der böswillige Administrator aus der vertrauten Domäne Zugriff auf Ressourcen innerhalb der vertrauenden Domäne (Rechteausweitung, engl.: *elevation of privilege*). Das „SID-History"-Attribut wird normalerweise bei der Migration von Benutzerkonten von einer Domäne in eine andere verwendet, um Zugriffsberechtigungen auf Ressourcen in der alten Domäne zu erhalten.

Diese Art von Angriffen kann durch die so genannte *SID-Filterung* verhindert werden. Hierbei wird die Authentifizierung von Benutzern aus vertrauten Domänen an der vertrauenden Domäne verhindert, wenn die Anmeldedaten des Benutzers SIDs aus der vertrauenden Domäne enthalten. Diese Maßnahme wird auch in der IT-Grundschutzmaßnahme M 4.314 [9] empfohlen. Microsoft nennt die SID-Filterung eine der zwei wichtigsten Schutzmaßnahmen für die Absicherung mittels Cross Forest Trust verbundener Domänen und stellt in [37] weiterführende Informationen bereit.

4.3.2 Zugriffsrechte auf alle freigegebenen Ressourcen innerhalb einer Domäne

Eine weitere Angriffsmöglichkeit kann dadurch entstehen, dass ein erfolgreich authentifizierter Benutzer aus der vertrauten Domäne prinzipiell Standardzugriffsberechtigungen auf alle freigegebenen Ressourcen innerhalb der vertrauenden Domäne erhält. Hierdurch entsteht eine größere Angriffsfläche für böswillige Benutzer.

Diese Angriffsmöglichkeit kann durch eine selektive Authentifizierung verhindert werden. Hierbei muss der Administrator eines Systems innerhalb der vertrauenden Domäne Benutzern aus der vertrauten Domäne explizit das Recht erteilen, auf das System innerhalb der vertrauenden Domäne zugreifen zu dürfen (*Whitelisting*). Zu beachten ist allerdings, dass durch das Einführen der selektiven Authentifizierung auch zusätzlicher administrativer Aufwand eingeführt wird.

Microsoft beschreibt in dem Artikel „Security Considerations for Trusts" [37] ausführlich, welche Angriffe sich mittels selektiver Authentifizierung abwehren lassen.

4.3.3 Vertrauen in den Administrator des vertrauten Forest

Durch das Etablieren eines Forest Trust erhält ein Administrator aus einer vertrauten Domäne *B* keinerlei Rechte in der vertrauenden Domäne *A*. Aber der Administrator aus Domäne *B* hat einen maßgeblichen Einfluss darauf, welche Benutzer aus Domäne *B* auf Ressourcen in Domäne *A* zugreifen dürfen. Angenommen, der Administrator der vertrauenden Domäne *A* richtet Zugriffsrechte auf Ressourcen in Domäne *A* für eine Gruppe aus Domäne *B* ein. Ein Administrator aus der vertrauten Domäne *B* kann nun nach Belieben Benutzer aus Domäne *B* dieser Gruppe hinzufügen und bestimmt dadurch, welche Benutzer Zugriffsrechte auf Ressourcen in Domäne *A* erhalten. Der Administrator aus Domäne *A* hat darauf nur wenig Einfluss. Er kann lediglich der kompletten Gruppe die Zugriffsrechte wieder entziehen oder er kann mittels selektiver Authentifizierung einzelnen Benutzern dieser Gruppe die Zugangsberechtigung für Domäne *A* gewähren oder wieder entziehen.

In diesem Zusammenhang sind auch die standardmäßig vorhandenen Windows-Gruppen „Everyone“ und „Authenticated Users“ zu beachten. Diese Gruppen werden häufig verwendet, um allen Benutzern innerhalb einer Domäne *A* Zugriffsrechte auf bestimmte Ressourcen einzurichten. Die Menge der Benutzer in dieser Gruppe ändert sich schlagartig, wenn die Domäne einer anderen Domäne *B* vertraut, denn dadurch erhalten auch alle Benutzer aus der Domäne *B* Zugriff auf diese Ressourcen. Handelt es sich zudem um eine transitive Vertrauensbeziehung, so wird der Zugriff auf alle Benutzer aus allen Domänen, denen Domäne *B* vertraut, ausgeweitet. Ein Entziehen der Zugriffsrechte für die gesamte Gruppe ist in diesem Fall problematisch, da dadurch auch alle Benutzer der Domäne *A* ihre Zugriffsrechte verlieren würden.

Wie in [26] erläutert wird, impliziert daher eine Vertrauensbeziehung zwischen zwei Domänen *A* und *B* auch, dass der Administrator der vertrauenden Domäne *A* dem Administrator der vertrauten Domäne *B* vertraut. Er muss ihm einerseits dahingehend vertrauen, dass es sich nicht um einen böswilligen Administrator handelt, der versucht, sich unberechtigte Zugriffsrechte in Domäne *A* zu verschaffen. Er muss andererseits aber auch darauf vertrauen, dass der Administrator aus Domäne *B* sein Handwerk versteht und keine (unbeabsichtigten) Fehler bei seinen Administrationstätigkeiten in Domäne *B* begeht. Denn wird aufgrund solcher Fehler die Domäne *B* kompromittiert und einem Angreifer gelingt es beispielsweise, ein Benutzerkonto aus Domäne *B* zu übernehmen, dann sind dadurch nicht nur Ressourcen aus Domäne B bedroht, sondern möglicherweise auch Ressourcen aus Domäne A, für die dieses Benutzerkonto Zugriffsrechte besitzt. D. h. gelingt es dem Administrator aus Domäne *B* nicht, seine Systeme aus Domäne *B* entsprechend abzusichern, adäquate Sicherheitsrichtlinien zu etablieren oder die Systeme kontinuierlich zu überwachen (*Monitoring*), dann sind Ressourcen aus der vertrauenden Domäne *A*, auf die Benutzer aus Domäne *B* zugreifen dürfen, genauso gefährdet, wie Ressourcen aus Domäne *B*.

5 Kriterienkatalog für sichere Softwareverteilung

Dieses Kapitel definiert einen Katalog von IT-Sicherheitskriterien, die bei der Einführung und dem Betrieb eines Werkzeugs zur zentralen Softwareverteilung innerhalb eines Unternehmens oder einer Organisation eingehalten werden sollten. Die einzelnen Kriterien sind thematisch in Kriteriengruppen zusammengefasst.

Die in diesem Kriterienkatalog enthalten IT-Sicherheitskriterien sind unabhängig vom BSI-Grundschutzkatalog [9]. Gleichwohl listet der Grundschutzkatalog in seinen Bausteinen zahlreiche Gefährdungen und zugehörige Maßnahmen, die auch für die sichere Softwareverteilung relevant sind. Geeignete Maßnahmen des Grundschutzkatalogs sollten daher komplementär berücksichtigt werden.

Alle Kriterien besitzen einen Bezeichner. Dieser Bezeichner setzt sich zusammen aus dem Prefix „K" für Kriterium, der Gruppennummer und der Position des Kriteriums innerhalb der Gruppe. So bezeichnet beispielsweise „K5.1.2" das zweite Kriterium im Abschnitt „5.1 Kriterien für die Administration".

Die untenstehenden Kriterien beinhalten i. d. R. Vorschläge für geeignete typische Maßnahmen, die zur Erfüllung des Kriteriums beitragen. Jedoch sind die konkreten Anwendungsfälle sehr heterogen. Daher stellen diese Vorschläge lediglich Beispiele dar, die Aufzählung ist nicht abschließend. Weiterhin müssen nicht notwendigerweise alle aufgeführten Maßnahmen erfüllt werden, bzw. kann im konkreten Anwendungsfall sogar keine der vorgeschlagenen Maßnahmen relevant sein.

5.1 Kriterien für die Administration

Die in diesem Abschnitt aufgeführten Kriterien umfassen die Aspekte Administration und administrative Verantwortungsbereiche.

K 5.1.1 – *Einführung von administrativen Verantwortungsbereichen*
In einem Unternehmen oder einer Organisation sollen die administrativen Verantwortlichkeiten für die Systemkomponenten (z. B. Firewalls, Sicherheitsgateways oder Domain Controller) getrennt sein, d. h. sie sollten von unterschiedlichen Administratoren verantwortet werden. Hierfür sollten unterschiedliche administrative Verantwortungsbereiche definiert werden.

Geeignete Maßnahmen:

- Einführung und Dokumentation administrativer Verantwortungsbereiche
- Zuordnung von Administratoren zu administrativen Verantwortungsbereichen gemäß Grundsatz zur Trennung administrativer Verantwortungsbereiche

K 5.1.2 – *Least-Privilege-Prinzip in der Administration*
Die Administration sollte nach dem Least-Privilege-Prinzip erfolgen, das bedeutet, jeder Administrator bekommt nur so wenig Rechte wie möglich.

Geeignete Maßnahmen:

- Identifikation und Dokumentation der minimalen notwendigen Rechte für alle administrativen Aufgaben
- Zuordnung der notwendigen Rechte an Administratoren gemäß dem Least-Privilege-Prinzip

K 5.1.3 – *Protokollierung administrativer Tätigkeiten*
Alle administrativen Tätigkeiten sollten protokolliert werden. Besonders wichtig sind hierbei Änderungen von Benutzerberechtigungen (beispielsweise Änderungen an Gruppenmitgliedschaften oder Rechteänderungen an Benutzerkonten).

Geeignete Maßnahmen:

- Protokollierung aller administrativen Tätigkeiten
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Protokollierung

K 5.1.4 – *Keine eigenmächtige Vergrößerung administrativer Verantwortlichkeiten*
Es sollte verhindert werden, dass Administratoren den eigenen administrativen Verantwortungsbereich eigenmächtig vergrößern können.

Geeignete Maßnahmen:

- In administrativen Verantwortungsbereichen sollten die Vergabe bzw. die Änderung von administrativen Zugriffsrechten nur durch ausgewählte Administratoren (sogenannte „Admin-Administratoren") durchgeführt werden können.
- Diese Admin-Administratoren dürfen die eigenen administrativen Zugriffsrechte nicht verändern. Dies muss durch einen anderen Admin-Administrator oder einen übergeordneten Administrator erfolgen.
- Die administrativen Verantwortungsbereiche der Admin-Administratoren sollten disjunkt sein, um den Missbrauch von administrativen Berechtigungen zu erschweren.

K 5.1.5 – *Einsetzen von Instrumenten zur Gewaltenteilung*
Für besonders kritische administrative Tätigkeiten (wie beispielsweise die Tätigkeiten der Admin-Administratoren) und Änderungen administrativer Verantwortungsbereiche sollten Instrumente zur Gewaltenteilung eingesetzt werden. Hierfür eignen sich beispielsweise Instrumente wie das Vier-Augen-Prinzip oder mehrstufige Freigaben.

Geeignete Maßnahmen:

- Identifikation besonders kritischer administrativer Tätigkeiten

- Einführung und Dokumentation von Instrumenten zur administrativen Gewaltenteilung für kritische administrative Tätigkeiten

K 5.1.6 – *Protokollierung der Änderungen an administrativen Verantwortlichkeiten*
Alle Änderungen an administrativen Verantwortlichkeiten durch Admin-Administratoren (beispielsweise Änderungen an Gruppenmitgliedschaften oder Rechteänderungen an Administratorkonten) müssen protokolliert werden.

Geeignete Maßnahmen:

- Protokollierung aller administrativen Tätigkeiten der Admin-Administratoren
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Protokollierung

K 5.1.7 – *Dokumentation der Änderungen an administrativen Verantwortlichkeiten*
Alle Änderungen an administrativen Verantwortlichkeiten durch Admin-Administratoren inkl. der Gründe für die Änderungen und erteilte Freigaben sollten dokumentiert werden. Sofern ein Werkzeug für das Änderungsmanagement eingesetzt wird, sollte es hierzu genutzt werden.

Geeignete Maßnahmen:

- Dokumentation aller Änderungen an administrativen Verantwortlichkeiten
- Zusätzlich: Einführung eines Werkzeugs für das Änderungsmanagement

K 5.1.8 – *Regelmäßige Überprüfung der administrativen Verantwortungsbereiche*
Wirksamkeitsprüfung der Kriterien K 5.1.1, K 5.1.2, K 5.1.4 und K 5.1.5: Es sollte in regelmäßigen Abständen überprüft werden, dass die Administration nach dem Least-Privilege-Prinzip, sowie die eingeführten Konzepte für administrative Verantwortungsbereiche und Gewaltenteilung eingehalten bzw. nicht umgangen werden können. Beispielsweise sollte es einem Administrator nicht möglich sein, mithilfe mehrerer Gruppenzugehörigkeiten oder Accounts diese Konzepte auszuhebeln und so mehr Berechtigungen als notwendig zu erhalten.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung, dass Administratoren nur die für ihre administrativen Aufgaben notwendigen Rechte besitzen (sei es durch den Besitz eines Accounts oder durch Zuordnung zu administrativen Verantwortungsbereichen oder administrativen Rollen)
- Regelmäßige Prüfung der Wirksamkeit der Maßnahmen zur Einführung administrativer Verantwortungsbereiche (vgl. K 5.1.1) und des Least-Privilege-Prinzips (vgl. K 5.1.2)

- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.1.9 – *Beschränkung der Anzahl von Admin-Administratoren*
Die Anzahl der Admin-Administratoren sollte möglichst gering sein.

Geeignete Maßnahmen:

- Definition der Anzahl gewünschter Admin-Administratoren
- Zuweisung von Personen zur Gruppe der Admin-Administratoren

K 5.1.10 – *Regelmäßige Überprüfung der Beschränkung von Admin-Administratoren*
Wirksamkeitsprüfung des Kriteriums K 5.1.9: Es sollte eine regelmäßige Überprüfung stattfinden, dass die gewünschte Anzahl von Admin-Administratoren nicht überschritten wird.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung, dass die Anzahl von Admin-Administratoren nicht überschritten wird.
- Benachrichtigung der zuständigen Verantwortlichen bei Überschreiten (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.1.11 – *Nutzung temporärer Installations-Accounts*
Für Administrationstätigkeiten, die nur sehr selten oder einmalig durchgeführt werden (beispielsweise Installationen auf Infrastruktur- oder Softwareverteilungskomponenten), sollten dedizierte Accounts eingerichtet und genutzt werden, welche nur während der Nutzung aktiv und standardmäßig deaktiviert sind (sogenannte Installations-Accounts).

Geeignete Maßnahmen:

- Definition, für welche Administrationsaufgaben Installations-Accounts eingerichtet werden sollen
- Zuweisung der erforderlichen Rechte an die Installations-Accounts
- Übertragen der zugehörigen Zugangsdaten an die verantwortlichen Mitarbeiter
- Festlegung der Administratoren, welche Installations-Accounts anlegen und (de)aktivieren dürfen
- Standardmäßige Deaktivierung aller Installations-Accounts

K 5.1.12 – *Regelmäßige Überprüfung der Deaktivierung der Installations-Accounts*
Wirksamkeitsprüfung des Kriteriums K 5.1.11: Es sollte eine regelmäßige Überprüfung stattfinden, dass die Installations-Accounts bei Nichtgebrauch deaktiviert sind.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung, dass die nicht benötigten Installations-Accounts deaktiviert sind.
- Benachrichtigung der zuständigen Verantwortlichen bei Verstoß (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

5.2 Kriterien für die Protokollierung und Überwachung

Die Protokollierung und Überwachung wichtiger Ereignisse innerhalb eines Systems tragen entscheidend zur Steigerung der Sicherheit während des Betriebs bei. Hierzu zählen Instrumente und Prozesse für die Protokollierung, Überwachung und das Änderungsmanagement. In diesem Abschnitt werden Kriterien bezüglich der Art und Weise sicherer Protokollierung und Überwachung beschrieben. Kriterien hinsichtlich der zu protokollierenden Daten werden themenbezogen in den jeweiligen Kriteriengruppen genannt.

K 5.2.1 – *Beweissichere Protokollierung*
Die Protokollierung sollte beweissicher sein, um möglichst lückenlos und vollständig nachzuweisen, welche Benutzer, Administratoren und Admin-Administratoren zu welchem Zeitpunkt welche Aktionen ausgeführt haben. Insbesondere muss die Authentizität (d. h. nur berechtigte Protokollierungsquellen) und Integrität der Protokolldaten (d. h. beispielsweise den Schutz vor unbemerkter Veränderung oder Löschung von Protokolleinträgen) sichergestellt werden. Weiterhin müssen die Protokolle sicher aufbewahrt werden (Verfügbarkeit), nur berechtigten Personen zugänglich sein (Vertraulichkeit). Schließlich muss sichergestellt werden, dass die Protokollierungskomponente alle wichtigen Ereignisse erfasst und nicht umgangen werden kann (vgl. [2]).

Geeignete Maßnahmen:

- Einführung einer Komponente zur beweissicheren Protokollierung

K 5.2.2 – *Administration der Protokollierungskomponente*
Um Interessenskonflikte zu vermeiden, dürfen Administratoren, deren Komponenten überwacht werden, nicht gleichzeitig Administratoren der Protokollierungskomponente sein.

Geeignete Maßnahmen:

- Festlegung der Protokollierungsadministratoren

K 5.2.3 – *Überwachung*
Komplementär zur Protokollierung sollte eine Überwachung wichtiger Ereignisse durch eine Überwachungskomponente erfolgen. Im Unterschied zur Protokollierung erlaubt das Monitoring die zeitnahe und proaktive Reaktion auf zuvor definierte relevante Ereignisse. Tritt ein solches Ereignis ein, dann führt die Überwachungskomponente definierte Aktionen (wie beispielsweise das Benachrichtigen eines Administrators) aus.

Geeignete Maßnahmen:

- Einführung einer Überwachungskomponente
- Definition der relevanten Ereignisse
- Definition der relevanten Aktionen für alle Ereignisse

K 5.2.4 – *Administration der Überwachungskomponente*
Um Interessenskonflikte zu vermeiden, dürfen Administratoren, deren Komponenten überwacht werden, nicht gleichzeitig Administratoren der Überwachungskomponente sein.

Geeignete Maßnahmen:

- Festlegung der Überwachungsadministratoren

K 5.2.5 – *Verfügbarkeit der Protokollierung und der Überwachung*
Es sollte sichergestellt werden, dass die Komponente, welche für die Protokollierung und das Monitoring zuständig ist, zuverlässig funktioniert (beispielsweise durch die Einführung eines „Heartbeat"-Konzepts).

Geeignete Maßnahmen:

- Regelmäßige Überprüfung, dass die Protokollierungs- und Überwachungskomponente funktionsbereit ist.
- Festlegung eines geeigneten „Heartbeat"-Konzepts
- Umsetzung des „Heartbeat"-Konzepts

5.3 Kriterien für die Systemkonfiguration

Die folgenden Kriterien dienen dazu, die Gefahr fehlerhafter Systemkonfigurationen zu verringern. Zu den Systemkonfigurationen zählen u. a. die Konfigurationen von Infrastrukturkomponenten (wie Firewalls, Netzwerk-Routern, Sicherheitsgateway), Domain Controller, Komponenten für die Authentifizierung, für das Berechtigungsmanagement, für die Softwareverteilung, für die Protokollierung und für das Monitoring.

K 5.3.1 – *Konsistente, kompakte und restriktive Konfigurationen*
Gefährdungen in Systemen entstehen oft durch fehlerhafte Konfigurationen oder das Zusammenspiel mehrerer nicht aufeinander abgestimmter (d. h. inkonsistenter) Konfigurationen. Weiterhin können Probleme auftreten, wenn Konfigurationen Redundanzen oder veraltete Einträge enthalten. Schließlich verstoßen Konfigurationen, welche Regeln für den Zugriff von Benutzern oder Diensten definieren, häufig gegen das Least-Privilege-Prinzip. Daher sollten Konfigurationen konsistent, kompakt und restriktiv formuliert werden.

Geeignete Maßnahmen:

- Identifikation und Berücksichtigung von Abhängigkeiten innerhalb und zwischen Konfigurationen zur Sicherstellung konsistenter Konfigurationen
- Vermeidung von Redundanzen in Konfigurationen
- Vermeidung von alten und nicht mehr benötigten Konfigurationseinträgen
- Definition restriktiver Konfigurationen beispielsweise im Fall des Berechtigungsmanagements durch die sparsame Verwendung von „Wildcards".
- Dokumentation von Konfigurationseinträgen und Änderungen an Konfigurationen inkl. deren Gründe

K 5.3.2 – *Regelmäßige Überprüfung von Konfigurationen*
Wirksamkeitsprüfung des Kriteriums K 5.3.1: Konfigurationen sollten regelmäßig dahingehend überprüft werden, dass sie konsistent, kompakt und restriktiv sind.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der Konfigurationen
- Behebung von Inkonsistenzen innerhalb oder zwischen Konfigurationen
- Löschung von alten oder redundanten Konfigurationseinträgen
- Vereinfachung und Überarbeitung gewachsener Konfigurationen
- Überprüfung von Konfigurationen hinsichtlich ihrer Restriktivität

K 5.3.3 – *Regelmäßige Überprüfung auf nichtautorisierte oder nichtdokumentierte Veränderungen von Konfigurationen*
Weitere Wirksamkeitsprüfung des Kriteriums K 5.3.1: Es sollte regelmäßig überprüft werden, ob die bestehenden Konfigurationen nichtautorisiert oder nichtdokumentiert verändert wurden. Diese Wirksamkeitsprüfung dient einerseits dazu, Veränderungen zu finden, die durch nichtautorisierte Personen (z. B. Angreifer) durchgeführt wurden und andererseits durch autorisierte Personen (z. B. Administratoren), die aber die Veränderung ihrerseits nicht dokumentiert haben.

Geeignete Maßnahmen:

- Für alle Konfigurationen: Vergleich der laufenden Konfiguration mit der dokumentierten bzw. hinterlegten Konfiguration
- Optional: Einsatz eines Change-Management-System zur Dokumentation von Konfigurationsänderungen

5.4 Kriterien für das Outsourcing

Dieser Abschnitt nennt Kriterien bezüglich des Outsourcings der Softwareverteilung an einen Dienstleister.

K 5.4.1 – *Absicherung der Kommunikationsverbindungen zwischen Auftraggeber und Dienstleister*
Auftraggeber und Dienstleister sind i. d. R. über Netzwerke verbunden, häufig findet die Kommunikation über das Internet statt. Daher sollten die Kommunikationsverbindungen zwischen Auftraggeber und Dienstleister durch den Einsatz von Sicherheitsmaßnahmen wie SSL/TLS oder VPN abgesichert werden.

Geeignete Maßnahmen:

- Einführung geeigneter Maßnahmen für alle Kommunikationsverbindungen zwischen Auftraggeber und Dienstleister

K 5.4.2 – *Konfiguration der Firewall des Auftraggebers*
Bei der Konfiguration der Firewall für den Zugang des Dienstleisters auf Systeme des Auftraggebers sollte darauf geachtet werden, dass die Firewall-Regeln möglichst feingranular formuliert werden, d. h. beispielsweise, dass Start- und Endpunkt der Kommunikation mit ihrer IP-Adresse und Port-Nummern festgelegt sind und keine Wildcards verwendet werden.

Geeignete Maßnahmen:

- Identifikation und Dokumentation der minimalen notwendigen Kommunikationsverbindungen
- Erzeugung von Firewall-Regeln für die notwendigen Kommunikationsverbindungen

K 5.4.3 – *Regelmäßige Überprüfung der Konfiguration der Firewall des Auftraggebers*
Wirksamkeitsprüfung des Kriteriums 5.4.2: Es sollte regelmäßig überprüft werden, dass Firewall-Regeln möglichst feingranular formuliert werden und keine Wildcards verwendet werden.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der Einhaltung
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.4.4 – *Konfiguration von Dienstleisterzugängen und -berechtigungen*
Der Dienstleister benötigt zur Erbringung seiner Dienstleistungen Benutzer- und Dienst-Accounts mit den zugehörigen Berechtigungen. Diese müssen im System des Auftraggebers konfiguriert werden. Hierbei ist zu beachten, dass der Dienstleister nur die für seine Arbeit notwendigen Berechtigungen im System erhält (Einhaltung des Least-Privilege-Prinzips). Der Auftraggeber sollte dem Dienstleister die für den Zugriff notwendigen Zugangsinformationen (Benutzernamen + Passwörter oder Benutzerzertifikate inkl. Schlüsselmaterial) auf einem sicheren Übertragungsweg übermitteln.

Geeignete Maßnahmen:

- Identifikation und Dokumentation der für den Dienstleister notwendigen Accounts und zugehörigen Berechtigungen
- Einrichtung der notwendigen Accounts und Berechtigungen für den Dienstleister
- Übermittlung der Zugangsinformationen an den Dienstleister auf einem sicheren Übertragungsweg, z. B. Übermittlung der vertraulichen Informationen über einen separaten vertrauenswürdigen Informationsweg (engl. *out of bound*)

K 5.4.5 – *Regelmäßige Überprüfung von Dienstleisterzugängen und -berechtigungen*
Wirksamkeitsprüfung des Kriteriums 5.4.4: Es sollte regelmäßig überprüft werden, dass zum einen keine nicht benötigten Dienstleisterzugänge existieren und dass zum anderen Dienstleisterzugängen nur die minimal erforderlichen Berechtigungen zugewiesen sind.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der Einhaltung
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.4.6 – *Prüfung der Mandantenfähigkeit der Dienstleistersysteme*
Der Auftraggeber sollte auf geeignete Weise die Mandantenfähigkeit des Dienstleistersystems prüfen bzw. durch den Dienstleister oder einen externen Sachverständigen bestätigen lassen. In der Regel ist eine solche Prüfung für den Auftraggeber allein nicht möglich. Es bedarf daher der Mitarbeit des Dienstleisters oder eines externen Sachverständigen.

Geeignete Maßnahmen:

- Prüfung der Mandantenfähigkeit des Dienstleistersystems

K 5.4.7 – *Interessenskonflikte von Mitarbeitern des Dienstleisters*
Ein Dienstleister betreut in der Regel mehrere Mandanten. Hierbei kann es zu Situationen kommen, bei denen Interessenskonflikte von Mitarbeitern des Dienstleisters gegenüber verschiedenen Mandanten auftreten. Aus Auftraggebersicht ist es wichtig, dass solche Interessenskonflikte vermieden werden.

Geeignete Maßnahmen:

- Der Auftraggeber sollte auf den Dienstleister einwirken, damit Interessenskonflikte nicht entstehen.

K 5.4.8 – *Erhaltung des gewünschten Sicherheitsniveaus*
Durch das Outsourcing vergrößert sich die Angriffsoberfläche (vgl. Abschnitt 3.5). Daher sollte darauf geachtet werden, dass durch das Outsourcing von Aufgaben an einen Dienstleister das gewünschte Sicherheitsniveau eingehalten wird.

Geeignete Maßnahmen:

- Berücksichtigung des Sicherheitsniveaus bei der Vergabe von Outsourcing-Aufträgen.

5.5 Kriterien für die sichere Softwareverteilung

In diesem Abschnitt werden Kriterien für eine sichere Softwareverteilung genannt.

K 5.5.1 – *Administrative Verantwortlichkeiten für die Softwareverteilung*
Die administrative Verantwortung für die Softwareverteilungskomponente sollte von anderen administrativen Verantwortungsbereichen getrennt werden.

Geeignete Maßnahmen:

- Abgrenzung des administrativen Verantwortungsbereich für die Softwareverteilungskomponente von den administrativen Verantwortungsbereichen anderer Systemkomponenten (wie beispielsweise Infrastrukturkomponenten).
- Berücksichtigung der o. g. Abgrenzung bei der Zuweisung von zu administrativen Verantwortungsbereichen.

K 5.5.2 – *Absicherung der Software Deployment Pipeline*
Für die fehlerfreie Softwareverteilung und zum Schutz vor Schadsoftware bzw. vor Kompromittierung der Softwareverteilungskomponente sollten die einzelnen Schritte der Software Deployment Pipeline abgesichert werden.

Geeignete Maßnahmen:

- Herunterladen der Software nur von vertrauenswürdigen Quellen
- Sicherstellung, dass die Software bzw. Softwarepakete beim Durchlaufen der Software Deployment Pipeline nicht manipuliert werden

- Sicherstellung, dass alle Schritte der Software Deployment Pipeline in der definierten Reihenfolge durchlaufen werden

K 5.5.3 – *Abhängigkeiten von Softwarepaketen*
Vor der Verteilung neuer Softwarepakete müssen Abhängigkeiten innerhalb des Softwarepakets und zu bereits installierter Software geprüft werden. Weiterhin muss die Kompatibilität zur verwendeten Endgerätehardware sichergestellt werden.

Geeignete Maßnahmen:

- Prüfung der Softwarepakete auf Abhängigkeiten und Kompatibilität.
- Nutzung der Testumgebung für den Test von Softwarepaketen

K 5.5.4 – *Testen der Softwarepakete*
Die Funktionalität von Softwarepaketen sollte vor der Verteilung und Installation auf den Endgeräten ausführlich getestet werden, um zu verhindern, dass fehlerhafte Software ausgerollt wird.

Geeignete Maßnahmen:

- Aufsetzen einer Testumgebung für den Test von Softwarepaketen. Hierbei sollte die Endgeräte in der Testumgebung die gleichen Hard- und Softwareeigenschaften besitzen wie Geräte in der Produktivumgebung.
- Testen der Funktionalität der Softwarepakete einschließlich der Fehlerbehandlungsroutinen, z. B. der Deinstallation fehlerhafter oder abgebrochener Softwareinstallationen

5.6 Kriterien bezüglich Microsoft SCCM, Active Directory und Cross Forest Trust

Dieser Abschnitt nennt Kriterien, die den sicheren Einsatz und die Administration von Microsoft SCCM insbesondere in Cross-Forest-Trust-Szenarien betreffen.

K 5.6.1 – *Aktivierung der SID-Filterung*
Zur Einschränkung von Zugriffsrechten von Administratoren auf mehreren Domänen sollte die SID-Filterung aktiviert sein (insbesondere „SID-History"-Attribut, vgl. Abschnitt 4.3.1).

Geeignete Maßnahmen:

- Aktivierung der SID-Filterung für das „SID-History"-Attribut

K 5.6.2 – *Regelmäßige Überprüfung der Aktivierung der SID-Filterung*
Wirksamkeitsprüfung des Kriteriums K 5.6.1: Es sollte in regelmäßigen Abständen überprüft werden, ob die SID-Filterung aktiviert ist.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der Aktivierung der SID-Filterung
- Benachrichtigung der zuständigen Verantwortlichen bei fehlender Aktivierung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.6.3 – *Aktivierung der selektiven Authentifizierung*
Zur Einschränkung des Zugriffs auf freigegebene Ressourcen für Benutzer fremder Domänen sollte die selektive Authentifizierung aktiviert sein (vgl. Abschnitt 4.3.2). Die Authentifizierung von SCCM-Dienstkonten, die für die Softwareverteilung notwendig sind, sollte explizit erlaubt werden.

Geeignete Maßnahmen:

- Aktivierung der selektiven Authentifizierung
- Festlegung und Konfiguration der SCCM-Dienstkonten, die sich authentifizieren dürfen (vgl. hierzu auch Abschnitt 4.2.2)

K 5.6.4 – *Regelmäßige Überprüfung der Aktivierung der selektiven Authentifizierung*
Wirksamkeitsprüfung des Kriteriums K 5.6.3: Es sollte in regelmäßigen Abständen überprüft werden, ob die selektive Authentifizierung aktiviert ist.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der Aktivierung der selektiven Authentifizierung
- Benachrichtigung der zuständigen Verantwortlichen bei fehlender Aktivierung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.6.5 – *Verfügbarkeit bisheriger Dienste und Anwendungen*
Durch die Einführung des Cross Forest Trust darf es nicht zu Beeinträchtigungen hinsichtlich der Funktionalität und Verfügbarkeit bisheriger Dienste und Anwendungen in den beteiligten Domänen kommen.

Geeignete Maßnahmen:

- Identifikation möglicher Beeinträchtigungen, die durch die Einführung des Cross Forest Trust entstehen können
- Simulation der Einführung des Cross Forest Trust in einer geeigneten Testumgebung und Überprüfung auf Beeinträchtigungen in der Praxis

- Überprüfung von Beeinträchtigungen nach Einführung des Cross Forest Trust in der Produktionsumgebung

K 5.6.6 – *Minimierung von verantwortlichen Administratoren für Komponenten*

Die Anzahl der verantwortlichen Administratoren für eine Komponente (z. B. SCCM, Active Directory, Firewall) sollte möglichst klein und auf eine maximale Größe beschränkt sein. Als besonders kritisch ist hier insbesondere die Rolle der Domänenadministratoren anzusehen, da diese Rolle administrative Berechtigungen auf allen Geräten und Diensten innerhalb der Domäne (Rechner, Server, Domain Controller usw.) besitzt. Dabei ist zu beachten, dass die Gruppe von Administratoren zweier in Verbindung stehender Komponenten paarweise disjunkt ist.

Geeignete Maßnahmen:

- Definition der gewünschten Anzahl von Administratoren für jede einzelne Komponente
- Zuweisung von Personen zu den jeweiligen Gruppen von Administratoren gemäß den o. g. Gewaltenteilungsregeln.

K 5.6.7 – *Regelmäßige Überprüfung der Minimierung von verantwortlichen Administratoren für Komponenten*

Wirksamkeitsprüfung des Kriteriums refkrit:sccm:AD-Gruppe-Hauptadmins. Es sollte regelmäßig überprüft werden, dass die gewünschte Anzahl von Administratoren jeder einzelnen Komponente nicht überschritten wird und dass Administratorengruppen disjunkt sind.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung, dass die gewünschte Anzahl von Administratoren jeder einzelnen Komponente nicht überschritten wird
- Regelmäßige Überprüfung, dass die Gruppen von Administratoren zweier in Verbindung stehender Komponenten paarweise disjunkt sind
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.6.8 – *Kommunikation von SCCM-Komponenten*

Die Berechtigungen zur Kommunikation von SCCM-Komponenten bzw. mit SCCM-Komponenten sollte auf ein Minimum reduziert werden. Hier sollte die Konfiguration von Firewalls, Gateways, etc. derart angepasst werden, dass Berechtigungen der Kommunikationsendpunkte explizit und möglichst genau (d. h. beispielsweise auf Basis von IP-Adressen und Port-Nummern) festgelegt werden.

Geeignete Maßnahmen:

- Identifikation aller notwendigen Kommunikationsbeziehungen
- Konfiguration der Berechtigungen in Firewalls, Gateways, etc. gemäß der identifizierten Kommunikationsbeziehungen

K 5.6.9 – *Vermeidung domänenübergreifender administrativer Verantwortlichkeiten*

In Forest-Trust-Szenarien sollten Administratoren der vertrauenden Domäne keine administrativen Verantwortlichkeiten in der vertrauten Domäne besitzen und umgekehrt. Beispielsweise sollte der Firewall-Administrator der Domäne *A* nicht auch gleichzeitig der Domänenadministrator der Domäne *B* sein. Insbesondere bei der domänenübergreifenden SCCM-Administration sollte auf eine personelle Trennung geachtet werden. Das bedeutet, dass ein Administrator für eine SCCM-Komponente, die in dem vertrauten Forest angesiedelt ist, nicht auch gleichzeitig Administrator einer SCCM-Komponente in dem vertrauenden Forest sein sollte (und umgekehrt).

Geeignete Maßnahmen:

- Berücksichtigung vorhandener administrativer Verantwortlichkeiten in anderen Domänen bei der Vergabe von administrativen Verantwortlichkeiten in der eigenen Domäne.
- Berücksichtigung personeller Trennung bei SCCM-Administratoren unterschiedlicher Domänen.

K 5.6.10 – *Regelmäßige Überprüfung der Vermeidung domänenübergreifender administrativer Verantwortlichkeiten*

Wirksamkeitsprüfung des Kriteriums 5.6.9: Es sollte regelmäßig überprüft werden, dass in Forest-Trust-Szenarien Administratoren der vertrauenden Domäne keine administrativen Verantwortlichkeiten in der vertrauten Domäne besitzen und umgekehrt.

Geeignete Maßnahmen:

- Wirksamkeitsprüfung: Regelmäßige Überprüfung der Einhaltung
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.6.11 – *Gewaltenteilung bei der SCCM-Administration*

Innerhalb einer Domäne sollten Administratoren von Infrastrukturkomponenten nicht gleichzeitig auch SCCM-Administratoren sein, da dadurch das Prinzip der Gewaltenteilung verletzt werden würde.

Geeignete Maßnahmen:

- Berücksichtigung vorhandener administrativer Verantwortlichkeiten in der eigenen Domänen bei der Vergabe von administrativen Verantwortlichkeiten für SCCM

K 5.6.12 – *Regelmäßige Überprüfung der Gewaltenteilung bei der SCCM-Administration*

Wirksamkeitsprüfung des Kriterium 5.6.11: Es sollte regelmäßig überprüft werden, dass innerhalb einer Domäne Administratoren von Infrastrukturkomponenten nicht gleichzeitig auch SCCM-Administratoren sind.

Geeignete Maßnahmen:

- Wirksamkeitsprüfung: Regelmäßige Überprüfung der Einhaltung
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.6.13 – *Berechtigungen von SCCM-Dienstkonten*

Für SCCM werden verschiedene Dienstkonten (z. B. CAS-Dienstkonto und Datenbank-Dienstkonto) benötigt. Die Berechtigungen dieser Dienstkonten auf SCCM-Komponenten sollte auf ein Minimum beschränkt werden.

Geeignete Maßnahmen:

- Identifikation und Konfiguration der minimal notwendigen Berechtigungen von Dienstkonten auf SCCM-Komponenten

K 5.6.14 – *Regelmäßige Überprüfung der Berechtigungen von SCCM-Dienstkonten*

Wirksamkeitsprüfung des Kriterium 5.6.13: Es sollte regelmäßig überprüft werden, dass die Berechtigungen der SCCM-Dienstkonten auf ein Minimum beschränkt sind.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der Einhaltung der Beschränkung
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.6.15 – *Berechtigungen der Rollen „Authenticated Users“ und „Everyone“*
Innerhalb eines Forest Trust bekommt ein authentifizierter Benutzer eines vertrauten Forests automatisch die SID „Authenticated Users“ in dem vertrauenden Forest zugewiesen. Somit kann dieser Benutzer innerhalb des vertrauenden Forests auf alle Ressourcen zugreifen, die für die Rollen „Authenticated Users“ oder „Everyone“ freigegeben wurden. Um die Berechtigungen von Benutzern eines vertrauten Forests innerhalb des vertrauenden Forests einzuschränken, sollten daher den Rollen „Authenticated Users“ und „Everyone“ keine oder möglichst wenige Berechtigungen zugewiesen werden. Dabei ist zu berücksichtigen, dass die Änderung der Berechtigungen nicht nur Einfluss auf die Berechtigungen fremder Nutzer hat, sondern insbesondere auch auf die Berechtigungen von Nutzern der eigenen Domäne.

Geeignete Maßnahmen:

- Zuweisung möglichst weniger Berechtigungen zu den Rollen „Authenticated Users“ und „Everyone“.

K 5.6.16 – *Regelmäßige Überprüfung der Berechtigungen der Rollen „Authenticated Users“ und „Everyone“*
Wirksamkeitsprüfung des Kriterium 5.6.15: Es sollte regelmäßig überprüft werden, dass den Rollen „Authenticated Users“ und „Everyone“ keine oder möglichst wenige Berechtigungen zugewiesen werden.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der Einhaltung der Beschränkung
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.6.17 – *Vermeidung unberechtigter Rechteausweitung*
Sind innerhalb eines Forest-Trust-Szenarios in dem vertrauenden Forest Berechtigungen für Gruppen aus dem vertrauten Forest formuliert, sollte verhindert werden, dass Administratoren des vertrauten Forests auf unberechtigte Weise sich selbst oder andere Benutzer zu einer dieser Gruppen hinzufügen und somit Berechtigungen in dem vertrauenden Forest erlangen (unberechtigte Rechteausweitung, engl.: *elevation of privilege* oder *privilege escalation*).

Geeignete Maßnahmen:

- Nutzung der selektiven Authentifizierung, um gezielt Freigaben für bestimmte Benutzer einzurichten (vgl. Kriterien K 5.6.3 und K 5.6.4)
- Aktivierung der SID-Filterung (vgl. Kriterien K 5.6.1 und K 5.6.2)
- Zusätzlich: Einsatz von Testwerkzeugen, um bekannte Angriffsarten für Rechteausweitung in Windows-Domänen zu erkennen

K 5.6.18 – *Regelmäßige Überprüfung der Vermeidung unberechtigter Rechteausweitung*
Wirksamkeitsprüfung des Kriteriums 5.6.17: Es sollte regelmäßig geprüft werden, dass Administratoren des vertrauten Forests nicht auf unberechtigte Weise sich selbst oder andere Benutzer zu einer dieser Gruppen hinzufügen.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der Einhaltung der Beschränkung
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.6.19 – *Festgelegte Endgeräte für bestimmte administrative Tätigkeiten*
Es sollte festgelegte Endgeräte für jeweils verschiedene administrative Zwecke geben. Insbesondere sollte festgelegt werden, mit welchen Endgeräten welche administrativen Tätigkeiten ausgeübt werden dürfen (beispielsweise könnte festgelegt sein, dass bestimmte administrative Aufgaben nur über einen Terminalserver erledigt werden dürfen).

Geeignete Maßnahmen:

- Festlegung der Endgeräte für die jeweiligen administrativen Tätigkeiten auf Basis ihrer IP-Adresse, MAC-Adresse oder weiterer Eigenschaften sowie Konfiguration der entsprechenden Systeme (z. B. Firewall, Zielsystem)
- Sicherstellung, dass die zuvor durchgeführte Festlegung der Endgeräte auf den Systemen auch durchgesetzt wird, d. h. dass die Systeme nur administrative Aufträge von den festgelegten Endgeräten verarbeiten

K 5.6.20 – *Regelmäßige Überprüfung der festgelegten Endgeräte für bestimmte administrative Tätigkeiten*
Wirksamkeitsprüfung des Kriteriums K 5.6.19: Es sollte in regelmäßigen Abständen überprüft werden, ob bestimmte administrative Tätigkeiten ausschließlich über die dafür zugelassenen und zuvor festgelegten Endgeräte erledigt werden können. Wird hierbei festgestellt, dass eine administrative Tätigkeit auch über nicht dafür zugelassene Endgeräte ausgeführt werden kann, muss eine entsprechende Aktion ausgelöst werden (vgl. hierzu auch Abschnitt 3.3).

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der festgelegten Endgeräte für bestimmte administrative Tätigkeiten
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)

- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

K 5.6.21 – *Konfiguration von Firewalls*
Bei der Konfiguration von Firewalls für die Nutzung von SCCM sollte darauf geachtet werden, dass die Firewall-Regeln möglichst feingranular formuliert werden, d. h. beispielsweise, dass Start- und Endpunkt der Kommunikation mit ihrer IP-Adresse und Port-Nummern festgelegt sind und keine Wildcards verwendet werden.

Geeignete Maßnahmen:

- Identifikation und Dokumentation der minimalen notwendigen Kommunikationsverbindungen
- Erzeugung von Firewall-Regeln für die notwendigen Kommunikationsverbindungen

K 5.6.22 – *Regelmäßige Überprüfung der Konfiguration von Firewalls*
Wirksamkeitsprüfung des Kriteriums 5.6.21: Es sollte regelmäßig überprüft werden, dass Firewall-Regeln möglichst feingranular formuliert werden und keine Wildcards verwendet werden.

Geeignete Maßnahmen:

- Regelmäßige Überprüfung der Einhaltung
- Benachrichtigung der zuständigen Verantwortlichen bei Nichteinhaltung (vgl. hierzu auch Abschnitt 3.3)
- Zusätzlich: Einführung eines Werkzeugs zur automatischen Überprüfung, Auswertung und Benachrichtigung der o. g. Wirksamkeitsprüfung (beispielsweise durch Einsatz eines Monitoring-Systems)

6 Fazit

Bei der Planung einer zentralen Softwareverteilung in Unternehmen und Organisationen müssen zahlreiche Sicherheitsaspekte berücksichtigt werden, um zu verhindern, dass Schadsoftware eingeschleust wird, Angreifer unberechtigten Zugriff auf Informationen erhalten oder versteckte Hintertüren eingebaut werden.

Bei netzwerkübergreifender Softwareverteilung kommen Fragestellungen hinsichtlich des Vertrauens zwischen Netzen hinzu. Administratorenkonten erfordern eine besondere Betrachtung. Aufgrund ihrer weitreichenden Berechtigungen stellen sie einerseits ein attraktives Angriffsziel dar, können jedoch auch für vorsätzliche Handlungen ausgenutzt werden. Um Sicherheitsvorfälle frühzeitig zu erkennen und forensisch untersuchen zu können, sind Maßnahmen wie die beweissichere Protokollierung und Überwachung zu berücksichtigen. Schließlich kann es sinnvoll sein, die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig zu prüfen.

Im Rahmen dieses Ratgebers wurde ein Katalog von Sicherheitskriterien vorgestellt, der auf potentielle Gefährdungen hinweist und beispielhaft geeignete Sicherheitsmaßnahmen nennt. Der vorliegende Ratgeber kann einerseits zur Sensibilisierung für das Thema IT-Sicherheit bei der Softwareverteilung genutzt werden und dient andererseits als Handreichung für Administratoren, die eine zentrale, netzwerkübergreifende Softwareverteilung in ihrem Unternehmen planen und sich über die zu berücksichtigenden Sicherheitsaspekte informieren möchten.

Abkürzungen

AD	Microsoft Active Directory
ADFS	Active Directory Federation Service
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAS	Central Administration Site
CFT	Cross Forest Trust
DMZ	Demilitarisierte Zone
HMAC	Hash-based Message Authentication Code
HMdIS	Hessisches Ministerium des Inneren und für den Sport
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Informationstechnologie
MAC	Media Access Control Address
OWASP	Open Web Application Security Project
REST	Representational State Transfer
SCCM	Microsoft System Center Configuration Manager
SID	Security Identifier
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
SW	Software
TLS	Transport Layer Security
VPN	Virtual Private Network

Literaturverzeichnis

[1] American National Standard Institute (ANSI) for Information Technology: *Role Based Access Control*. Technischer Bericht ANSI INCITS 359-2004, ANSI, Feb. 2004.

[2] Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: *Orientierungshilfe „Protokollierung"*, November 2009. https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/070328_Datenschutzrechtliche_Protokollierung_beim_Betrieb_IT-Systeme/OH_Datenschutzrechtliche_Protokollierung_beim_Betrieb_IT-Systeme.pdf (besucht am 31.8.2017)

[3] Bass, Len, Ralph Holz, Paul Rimba, An Binh Tran und Liming Zhu: *Securing a Deployment Pipeline*. In: *3rd IEEE/ACM International Workshop on Release Engineering, RELENG 2015, Florenz, Italien*, Seiten 4–7, Mai 2015.

[4] Botta, David, Kasia Muldner, Kirstie Hawkey und Konstantin Beznosov: *Toward understanding distributed cognition in IT security management: the role of cues and norms*. Cognition, Technology & Work, 13(2):121–134, 2011, ISSN 1435-5566.

[5] Botta, David, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels und Brian Fisher: *Towards Understanding IT Security Professionals and Their Tools*. In: *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, Seiten 100–111, New York, NY, USA, 2007. ACM.

[6] Botta, David, Rodrigo Werlinger, Andr´e Gagn´e, Konstantin Beznosov, Lee Iverson, Sidney Fels und Brian Fisher: *Towards Understanding IT Security Professionals and Their Tools*. In: *Proceedings of the 2007 Symposium on Usable Privacy and Security*, Seiten 100–111, 2007.

[7] Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten, Version 1.0 vom 08.03.2004*, März 2004. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/Veroeffentl/Outsourcing_pdf.pdf?__blob=publicationFile&v=1 (besucht am 31.8.2017)

[8] Bundesamt für Sicherheit in der Informationstechnik: *LeitfadenInformationssicherheit – IT-Grundschutz kompakt*, Februar 2012. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzUeberblick/LeitfadenInformationssicherheit/leitfaden_node.html (besucht am 31.8.2017)

[9] Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz-Kataloge – 15. Ergänzungslieferung*, 2016. http://www.bsi.bund.de/grundschutz (besucht am 31.8.2017)

[10] Callahan, Michael: *Messy firewall rules get security professionals „grounded for life“*, Juli 2016. https://www.firemon.com/messy-firewall-rules-get-security-professionals-grounded-life/ (besucht am 31.8.2017)

[11] Chiasson, Sonia, Robert Biddle und Anil Somayaji: *Even Experts Deserve Usable Security: Design guidelines for security management systems*. In: *In SOUPS Workshop on Usable IT Security Management (USM)*, Juli 2007.

[12] Chiasson, Sonia, P.C. van Oorschot und Robert Biddle: *A Usability Study and Critique of Two Password Managers*. In: *Proceedings of the 15th USENIX Security Symposium*, August 2006.

[13] Colville, Ronni J.: *Software Distribution: Reducing Risks With Goals (ID: DF-13-7599)*. Gartner, Inc., Juni 2001. https://www.gartner.com/guest/purchase/registration?resId=331245&srcId=1-3478922230 (besucht am 31.8.2017)

[14] Colville, Ronni J.: *Four Steps to Optimize Configuration Management Process and Tools (ID: G00258557)*. Gartner, Inc., Oktober 2013. https://www.gartner.com/doc/2616318/steps-optimize-configuration-management-process (besucht am 31.8.2017)

[15] Colville, Ronni J.: *Hype Cycle for IT Operations Management (ID: G00263503)*. Gartner, Inc., Juli 2014. https://www.gartner.com/doc/2804821/hype-cycle-it-operations-management (besucht am 31.8.2017)

[16] Da Silva, Luís Ferreira und Fernando Brito E. Abreu: *Software Distribution to Remote Locations*. In: *Proceedings of the 15th European Conference on Pattern Languages of Programs*, EuroPLoP '10, Seiten 20:1–20:4, 2010.

[17] De Paula, Rogério, Xianghua Ding, Paul Dourish, Kari Nies, Ben Pillet, David Redmiles, Jie Ren, Jennifer Rode und Roberto Silva Filho: *Two Experiences Designing for Effective Security*. In: *Proceedings of the 2005 Symposium on Usable Privacy and Security*, Band 93 der Reihe *ACM International Conference Proceeding Series*, Seiten 25–34. ACM, 2005.

[18] Dhamija, Rachna und Lisa Dusseault: *The Seven Flaws of Identity Management: Usability and Security Challenges*. IEEE Security & Privacy, 6(2):24–29, 3/4 2008, ISSN 1540-7993.

[19] Dourish, Paul, Rebecca E. Grinter, Jessica Delgado de la Flor und Melissa Joseph: *Security in the wild: user strategies for managing security as an everyday, practical problem*. Personal and Ubiquitous Computing, 8(6):391–401, November 2004, ISSN 1617–4909.

[20] Dourish, Paul und David Redmiles: *An Approach to Usable Security Based on Event Monitoring and Visualization*. In: *Proceedings of the New Security Paradigms Workshop '02*, Seiten 75–81, Virginia Beach, Virginia, September 2002. ACM.

[21] Dumitras, Tudo, Priya Narasimhan und Eli Tilevich: *To Upgrade or Not to Upgrade:Impact of Online Upgrades across Multiple Administrative Domains*. In: *Proceedings of the ACM International Conference on Object Oriented Programming Systems Languages and Applications*, OOPSLA '10, Seiten 865–876, New York, NY, USA, 2010. ACM, ISBN 978-1-4503-0203-6.

[22] Eckert, Claudia: *IT-Sicherheit - Konzepte, Verfahren, Protokolle (9. Aufl.)*. Oldenbourg, 2014.

[23] Europäisches Parlament und Rat der Europäischen Union: *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*, Mai 2016. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=SV (besucht am 31.8.2017)

[24] Faldu, Rushi, Manoj Kumar Pal, Andre Della Monica und Kaushal Pandey: *Microsoft System Center - Troubleshooting Configuration Manager*. Microsoft Press, 2013.

[25] Firemon: *2016 State of the Firewall Report*, März 2016. https://www.firemon.com/resources/collateral/2016-state-firewall-report/ (besucht am 31.8.2017)

[26] Franklin Smith, Randy: *To Trust or Not to Trust - Domains and forest and the risks of trust relationships*, März 2005. http://windowsitpro.com/windows-server/trust-or-not-trust (besucht am 31.8.2017)

[27] Haight, Cameron: *Principles and Practices of DevOps (ID: G00272990)*. Gartner, Inc., März 2015. https://www.gartner.com/doc/3004719/principles-practices-devops (besucht am 31.8.2017)

[28] Hawkey, Kirstie, David Botta, Rodrigo Werlinger, Kasia Muldner, Andre Gagne und Konstanzin Beznosov: *Human, Organizational, and Technological Factors of IT Security*. In: *CHI '08: CHI '08 Extended Abstracts on Human Factors in Computing Systems*, Seiten 3639–3644, New York, NY, USA, 2008. ACM.

[29] Ion, Iulia, Rob Reeder und Sunny Consolvo: *"... no one can hack my mind": Comparing Expert and Non-Expert Security Practices*. In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, Seiten 327–346, Ottawa, Juli 2015. USENIX Association, ISBN 978-1-931971-249.

[30] Ives, Blake, Kenneth R. Walsh und Helmut Schneider: *The Domino Effect of Password Reuse*. Communications of the ACM, 47(4):75–78, April 2004.

[31] <kes>/Microsoft (Herausgeber): *IT-Landschaften 2016, Lagebericht zur Sicherheit (2), <kes>/Microsoft Sicherheitsstudie 2016*. <kes> Die Zeitschrift für Informations-Sicherheit, 32(5):50–58, Oktober 2016.

[32] Knox, Kevin und Terrence Cosgrove: *Magic Quadrant for Client Management Tools (ID: G00264801)*. Gartner, Inc., Juni 2015. https://www.gartner.com/doc/3073718/magic-quadrant-client-management-tools (besucht am 31.8.2017)

[33] Malchar, Thomas: *Professionelles Passwortmanagement „Made in Germany"*. <kes> special Die Zeitschrift für Informations-Sicherheit, Seiten 40–41, Oktober 2016.

[34] McGittigan, Jim und Sanil Solanki: *The Gartner Top 10 Recommended IT Cost Optimization Ideas, 2016 (ID: G00301094)*. Gartner, Inc., Februar 2016. https://www.gartner.com/doc/3232218 (besucht am 31.8.2017)

[35] Microsoft TechNet: *Managing Trusts*. Microsoft Corporation, März 2012. https://technet.microsoft.com/en-us/library/cc771568(v=ws.11).aspx (besucht am 31.8.2017)

[36] Microsoft TechNet: *Domain and Forest Trusts Technical Reference*. Microsoft Corporation, November 2014. https://technet.microsoft.com/en-us/library/cc738955(v=ws.10).aspx (besucht am 31.8.2017)

[37] Microsoft TechNet: *Security Considerations for Trusts*. Microsoft Corporation, November 2014. https://technet.microsoft.com/en-us/library/cc755321(v=ws.10).aspx (besucht am 31.8.2017)

[38] Microsoft TechNet: *What Are Domains and Forests?* Microsoft Corporation, November 2014. https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx (besucht am 31.8.2017)

[39] Microsoft TechNet: *Introduction to System Center Configuration Manager*. Microsoft Corporation, Juli 2016. https://technet.microsoft.com/en-us/library/mt622715.aspx (besucht am 31.8.2017)

[40] Open Web Application Security Project (OWASP): *Attack Surface Analysis Cheat Sheet*, Juli 2015. https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet (besucht am 31.8.2017)

[41] Patton, Peter C. und Bijay K. Jayaswal: *Software Management*. In: Nof, Y. Shimon (Herausgeber): *Springer Handbook of Automation*, Seiten 779–795, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg, ISBN 978-3-540-78831-7.

[42] Schendel, Jan und Nico Müller: *Digitale Forensik in der Cloud*. <kes> Die Zeitschrift für Informations-Sicherheit, 32(5):6–7, Oktober 2016.

[43] Shirey, Robert W.: *Internet Security Glossary, Version 2*. RFC 4949, März 2013. https://rfc-editor.org/rfc/rfc4949.txt (besucht am 31.8.2017)

[44] Son, Youngsu, Jiwon Kim, Donguk Kim und Jinho Jang: *Deployment Pattern*. In: *Proceedings of the 18th Conference on Pattern Languages of Programs*, PLoP '11, Seiten 10:1–10:9, 2011.

[45] Tognazzini, Bruce: *Design for Usability*. In: Cranor, Lorrie Faith und Simson Garfinkel (Herausgeber): *Security and Usability*, Kapitel 3. O'Reilly Media, Inc., 2005.

[46] Wiebusch, Sven: *Fernadministration in Windows-Netzen: Empfehlungen zur Risikominimierung*. DUD – Datenschutz und Datensicherheit, 38(8):515–518, 2014, ISSN 1862-2607.

[47] Wing, Jeannette M. und Pratyusa K. Manadhata: *An Attack Surface Metric*. IEEE Transactions on Software Engineering, 37:371–386, 2010, ISSN 0098-5589.

[48] Yurcik, William, James Barlow und Jeff Rosendale: *Maintaining Perspective on Who Is The Enemy in the Security Systems Administration of Computer Networks*. In: *In ACM CHI Workshop on System Administrators Are Users*, Seiten 345–347. ACM Press, 2003.

ISBN 978-3-8396-1240-8