Fakultät für Ingenieurwissenschaften

Master-Thesis

Strategien und Konzepte für die Implementierung einer hochsicheren Administrationsumgebung zur Absicherung von Authentifizierungssystemen gegen APT-Angriffe

Abschlussarbeit zur Erlangung des Grades eines

Master of Engineering

der Hochschule Wismar

eingereicht von:	Holger Winzer, geboren am 18. Mai 1968 in Berlin
	Studiengang IT-Sicherheit und Forensik
Matrikelnummer:	290542
Erstgutachter:	Prof. Dr.-Ing. E. Jonas
Zweitgutachter:	Prof. Dr.-Ing. habil. A. Ahrens
Zweitbetreuer:	Dr. D. Wippig,
	Bundesamt für Sicherheit in der Informationstechnik

Wismar, den 7. Oktober 2020

Aufgabenstellung

Es ist eine Strategie- und Konzeptarbeit zu erstellen, welche Institutionen (Unternehmen, Behörden und anderen Organisationen) in verständlicher Weise die Notwendigkeit der Implementierung einer hochsicheren Administrationsumgebung (HSA) zur Absicherung des Authentifizierungs- und Verzeichnisdienstes (AVD) gegenüber Advanced Persistent Threat (APT)-Angriffen darlegt.
Dabei ist es Ziel der geplanten Abschlussarbeit, in zusammenfassender und kompakter Weise darzulegen, welchen Verlauf in der Regel APT-Angriffe nehmen, welche Maßnahmen zur Absicherung bzw. Abwehr sinnvoll sind und Entscheidungshilfen anzubieten, inwieweit der mögliche Schaden bei einem Angriff den Aufwand zur Absicherung durch eine HSA rechtfertigt.
Der Themenschwerpunkt soll dabei nicht auf einer Risikoanalyse oder -bewertung liegen, sondern auf der systematischen Entwicklung von Abwehrstrategien gegen diese Art von Angriffen. Um Konzepte und Strategien zur Entwicklung einer HSA-Umgebung abzuleiten, soll zunächst auf die fachspezifischen Hintergründe eingegangen werden, die speziell bei größeren Netzwerkumgebungen von Institutionen im Einsatz sind. Anschließend werden technisch detailliert die Abläufe und Zusammenhänge beschrieben, die sich hinter einem APT-Angriff verbergen und auf Methoden und Werkzeuge eingegangen, die bei einem Angriff eingesetzt werden. Daraus sollen dann Strategien für entsprechende Abwehrmaßnahmen entwickelt und entsprechende technische und organisatorische Maßnahmen (TOM) abgeleitet werden.
Abschließend soll eine Abschätzung des Aufwandes für die Umsetzung der vorgestellten Konzepte und eine Gegenüberstellung des möglichen Schadens eines erfolgreichen Angriffs gegeben werden.

Kurzreferat und Abstract

Autor: Holger Winzer

Deutscher Titel

Strategien und Konzepte für die Implementierung einer hochsicheren Administrationsumgebung zur Absicherung von Authentifizierungssystemen gegen APT-Angriffe.

Zusammenfassung

Für eine Klasse von Bedrohungen, die als Advanced Persistent Threats (APTs) bekannt ist, beschreibt diese Arbeit neben der Darstellung des Angriffsablaufs auch Strategien und Konzepte, die eine Institution in die Lage versetzen, sich erfolgreich gegen derartige Angriffe zur Wehr zu setzen. Es werden technische und organisatorische Maßnahmen für den Aufbau einer hochsicheren Administrationsumgebung beschrieben sowie der Aufwand für diese Maßnahmen der erzielbaren Schutzwirkung und dem möglichen Schadensrisiko eines APT-Angriffs gegenübergestellt. Zum Abschluss wird ein Ausblick auf zukünftige Authentifizierungsmethoden gegeben.

Title in english

Concepts and Strategies for the Implementation of a High Security Administration Environment to Protect Authentication Systems against APT-Attacks.

Abstract

For a class of threats known as Advanced Persistent Threats (APTs), this thesis describes not only the attack process but also strategies and concepts that enable an organization to successfully defend itself against such attacks. Technical and organizational measures for setting up a highly secure administration environment are described and the effort required for these measures is compared with the protective effect that can be achieved and the possible risk of damage from an APT attack. Finally, an outlook on future authentication methods is given.

Abgabedatum: 14. Oktober 2020

Inhaltsverzeichnis

Inhaltsverzeichnis **IV**

1 Einleitung **1**
1.1 Motivation 1
1.2 Ausgangssituation 3
1.3 Forschungshintergrund 5
1.4 Zielsetzung 6

2 Grundlagen **9**
2.1 Das ISO/OSI Refererenzmodell 9
2.2 Client-Server-Architektur 12
2.2.1 Klassifikation von Client-Server-Architekturen 14
2.2.2 Sicherheitsbetrachtung im Hinblick auf APT-Angriffe 16
2.3 Aufbau und Struktur moderner verteilter Rechenzentren 18
2.4 Aufgabe und Aufbau von Authentifizierungs- und Verzeichnisdiensten 24
2.4.1 Authentifizierungsverfahren 26
2.4.2 Aufgaben des Verzeichnisdienstes 35
2.4.3 Aufbau zentraler AVD-Systeme 38
2.5 Sicherheitsmodelle und Identitätsmanagement 40
2.5.1 Zugriffskontrollmodelle 41
2.5.2 Identitätsmanagement 48

3 Advanced Persistent Thread (APT) **49**
3.1 Ziele und Strategien des Angreifers 49
3.2 Kategorisierung 55
3.2.1 CERT-Taxonomie 56
3.2.2 Cyber-Kill-Chain 57
3.2.3 MITRE ATT&CK™ 61
3.3 Instrumente und Werkzeuge des Angreifers 63
3.4 Angriffsvektoren im internen Netz 68
3.4.1 Man-In-The-Middle-Angriff (MITM) 68
3.4.2 Pass-the-Hash 71
3.4.3 Golden- und Silver-Ticket-Angriffe 74
3.4.4 Zusammenfassung der Angriffsvektoren gegen AVD-Systeme 78

4 Strategien zur Abwehr von APT-Angriffen 80
4.1 Grundprinzip der vertrauenswürdigen Quelle 80
4.2 Prinzip der Berechtigungsebenen (Schichtenmodell) 83
4.3 Strategien der Berechtigungsminimierung (Credential Partitioning) . . 90
4.4 Authentifizierungsabsicherung 93
4.5 Analytische Ereignisüberwachung 96

5 Detailkonzeption einer hochsicheren Administrationsumgebung (HSA) 101
5.1 Netzwerktopologischer Aufbau 101
5.2 Logische Struktur einer HSA 106
5.3 Komponenten und Systeme einer HSA 109
5.3.1 Administrationsarbeitsplatz in der HSA 110
5.3.2 Updateprozesse und Datenimport in einer HSA 112
5.4 Weitere technische und organisatorische Maßnahmen 115

6 Aufwand und Wirkung einer Administrationsumgebung (HSA) 117
6.1 Risikoeinschätzung 117
6.2 Aufwand für den Aufbau einer HSA 120
6.3 Schutzfunktion gegen APT-Angriffe 122
6.4 Überprüfbarkeit der vorgestellten Konzepte (Evaluation) 123
6.5 Risikofaktor versus Aufwand 125

7 Zusammenfassung und Ausblick 126
7.1 Fazit 127
7.2 Ausblick 128

Verzeichnisse 131
Abbildungsverzeichnis 132
Tabellenverzeichnis 133
Glossar 135
Abkürzungsverzeichnis 141
Literaturverzeichnis 145
Index 156

Selbstständigkeitserklärung 159

Thesen 160

Anhang 161
A.1 Prototypisches Prozessmodell einer HSA-Implementierung 161

1 Einleitung

1.1 Motivation

In der heutigen Zeit stellen Informationen enorme Werte für Unternehmen und Behörden dar. Gehen Informationen verloren, drohen neben der Beeinträchtigung des Betriebs eventuell auch ein schwer messbarer Imageschaden sowie meist auch rechtliche Konsequenzen. Dabei handelt es sich bei Informationen im IT-Zeitalter vornehmlich um ein „virtuelles Gut“, und so ist es durchaus möglich, dass der Ereignisfall eintritt, ohne dass Schäden an den informationsverarbeitenden Systemen selbst auftreten.
Als Beispiel dafür steht folgende Pressemeldung:

> *8. Juni 2020, 14:00 Uhr / Quelle Heise Security*
>
> ### Massiver Angriff auf A1 Telekom Austria
>
> Etwa ein halbes Jahr kontrollierten unbekannte Angreifer zentrale Systeme des österreichischen Telco-Riesen.
>
> [...] Die Angreifer hatten zentrale PCs und Server gekapert und gingen fast ein halbes Jahr lang quasi nach Belieben ein und aus. Um sie nachhaltig raus zu werfen [sic], war eine koordinierte Aktion vieler Experten nötig. Da wurden auf einen Schlag alle Passwörter gesperrt, Webshell-Backdoors entfernt, neue Golden Tickets für den zentralen Kerberos-Server des Active Directories erstellt und vieles mehr.[...] Weitere Nachforschungen ergaben, dass dies nur ein Symptom eines groß angelegten Angriffs auf den Telekommunikationskonzern war. Die folgenden forensischen Analysen ergaben, dass sich die Angreifer bereits im November 2019 Zugang zum Netz verschaffen konnten. Der ursprüngliche Infektionsvektor ließ sich nicht rekonstruieren; die Incident Response vermutet allgemein "gestohlene Zugangsdaten". [...]
>
> Anders als bei typischen Cybercrime-Attacken rollten die Hacker jedoch keine Ransomware aus. Es wurden keinerlei Daten verschlüsselt [...]. Das spreche für eine Advanced Persistent Threat (APT), wie sie typischerweise von staatlich gelenkten, Geheimdienst-nahen Gruppen durchgeführt werden.
>
> Quelle: [Heise Security, 2020]

Meldungen wie diese sind kein Einzelfall. Namhafte Firmen und Konzerne fürchten den Imageverlust durch derartige Schlagzeilen, suggerieren diese doch eine angebliche Schwäche der implementierten technischen Systeme, möglicherweise sogar des

gesamten Unternehmens. Die in dem oben zitierten Artikel beschriebenen Symptome werden auch in verschiedenen ähnlich gelagerten Fällen beschrieben. Die teils sehr drastischen Formulierungen in diesem Zusammenhang, wie „Totalschaden“, „Aufgabe des Netzwerks“ oder „notwendiger Hardwaretausch“ lassen dabei den Schweregrad der Vorfälle bereits vermuten.

Diese Arbeit soll Hintergrundinformationen über derartige Angriffe liefern, ein Verständnis der technischen Vorgänge ermöglichen und Maßnahmen aufzeigen, die derartige Angriffe erschweren. Unmöglich wird diese Art des Angriffs nie sein, da sie stets über das Netzwerk erfolgt. Systeme, die mit einem Netzwerk in Kontakt stehen, sind aus Richtung des Netzwerkes immer angreifbar beziehungsweise verwundbar. Letztendlich hängt es nur von den Fähigkeiten und verfügbaren Ressourcen eines Angreifers ab, ob eine potenzielle Schwachstelle genutzt werden kann oder nicht. Diesem Umstand wird im Rahmen des international anerkannten Common Criteria[1] Katalogs Rechnung getragen, in dem ein Angriffspotenzial (Basic, Enhanced-Basic, Moderate und High) definiert ist, das letztendlich nötig ist, um eine Schwachstelle real auszunutzen. [siehe ISO, 1999]

Die Problemstellung

Unternehmen, Behörden und andere Organisationen – im Folgenden bezeichnet als Institutionen – werden immer häufiger Opfer von Cyber-Angriffen. Ein nicht unerheblicher Teil dieser Angriffe zielt nicht darauf ab, Systeme einfach nur zum Erliegen zu bringen (Denial of Service, DoS) bzw. den Betrieb der Systeme zu stören. Bei einem sogenannten APT-Angriff geht es meist darum, durch gezielte Angriffsmaßnahmen an bestimmte Informationen zu gelangen. Dies kann Teil eines wirtschaftlich und/oder politisch motivierten Angriffs sein.

In verwalteten Umgebungen ist häufig der Einsatz eines zentralen Authentifizierungs- und Verzeichnisdienstes (AVD) zweckmäßig. Bei einem APT-Angriff sind diese Dienste sehr häufig ein erstes Ziel. Eine der Angriffsarten gegen den Authentifizierungsdienst wird als Golden-Ticket-Angriff bezeichnet. Diese Art von Kompromittierung ist einer der schwerwiegendsten Angriffe gegen die IT einer Institution, da damit die Integrität, Vertraulichkeit und Authentizität aller Daten verloren geht, für die der angegriffene AVD die Zugriffe regelt bzw. autorisiert. Gleichzeitig ist ein solcher Angriff für die IT-Verantwortlichen der Institution nur schwer zu detektieren.

[1] Ein von dem Common Criteria Editorial Board (CCEB) erstellter und durch die Norm ISO/IEC 15408 festgelegter Kriterienkatalog für die Bewertung der Sicherheit von Informationstechnologien. Quelle: `https://www.commoncriteriaportal.org`

Um die Durchführung derartiger Angriffe in diesem Systembereich für einen Angreifer[2] möglichst beschwerlich zu gestalten, sollten AVD-Systeme und deren Administrationsumgebung innerhalb der Institution speziell abgesichert werden. Diese Arbeit zeigt zu dieser Art von Absicherung Konzepte und Strategien auf.

1.2 Ausgangssituation

IT-Sicherheit und Informationssicherheit

Die beiden Begriffe IT-Sicherheit und Informationssicherheit werden oft synonym verwendet. [siehe Wegener, 2014, S. 9] In dieser Arbeit soll aber klar zwischen den beiden Begrifflichkeiten unterschieden werden. IT-Sicherheit beschäftigt sich mit dem Schutz von Informationen bei der Verarbeitung, Übertragung und Speicherung von Daten auf und in IT-Systemen. Im Vergleich dazu bezieht sich der Begriff Informationssicherheit auf den Schutz von Information in allen Geschäftsprozessen. Der Schwerpunkt dieser Arbeit liegt auf dem Schutz von elektronisch verarbeiteten Daten, somit wird in diesem Kontext der Begriff IT-Sicherheit als angemessen betrachtet.

An dieser Stelle wird auf ein Grundproblem der IT-Sicherheit hingewiesen: Faktisch alle in der heutigen Zeit betriebenen Rechenanlagen basieren auf der Von-Neumann-Architektur, welche Daten und Programme nicht trennt, sondern in einem gemeinsamen Speicher ablegt. [siehe Neumann, 1945; Randell, 2013] Dadurch kann kein vollkommener Schutz von Daten gewährleistet werden, wie die jüngst aufgedeckten Sicherheitslücken Meltdown und Spectre zeigen. [siehe Lipp et al., 2018] Für beide Begriffe gilt die Umsetzung der allgemeinen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Diese werden auch als CIA-Triade bezeichnet, was sich aus der Zusammensetzung der Anfangsbuchstaben der entsprechenden englischen Bezeichnung der Schutzziele ableitet. [siehe Wegener, 2014, S. 10] Eckert beschreibt die Schutzziele wie folgt: [siehe Eckert, 2018, S. 7ff.]

- Vertraulichkeit (confidentiality): Informationen dürfen nur von dafür autorisierten Personen eingesehen und geändert werden.
- Integrität (integrity): Informationsänderung darf nicht unbemerkt erfolgen.
- Verfügbarkeit (availability): Informationen müssen im vereinbarten Rahmen verfügbar sein – Quality of Service (QoS).

[2] Aus Gründen der besseren Lesbarkeit wird in dieser Masterarbeit die Sprachform des generischen Maskulinums angewandt. Es wird an dieser Stelle darauf hingewiesen, dass die ausschließliche Verwendung der männlichen Form geschlechtsunabhängig verstanden werden soll.

Diese drei allgemeinen Schutzziele werden durch die in dieser Arbeit beschriebenen Angriffe bedroht. Wird das Schutzziel Verfügbarkeit verletzt, ist dies als Denial of Service (DoS)-Attacke zu sehen. Erfahrungsgemäß ist bei APT-Angriffen die Verfügbarkeit nicht direkt gefährdet. Es besteht allerdings die Möglichkeit, dass nach einem erfolgreichem APT-Angriff Systeme bewusst zerstört werden. Man spricht davon, dass Angreifer nach dem Verlassen des Schlachtfeldes nur „verbrannte Erde“ zurücklassen. In diesem Fall ist es für eine Institution von wesentlicher Bedeutung, verlässliche Datensicherungs- und Wiederherstellungsstrategien implementiert zu haben. Neben den oben genannten allgemeinen Schutzzielen gibt es nach Eckert ergänzend spezielle Schutzziele innerhalb der Informationssicherheit: [siehe Eckert, 2018, S. 8ff.]

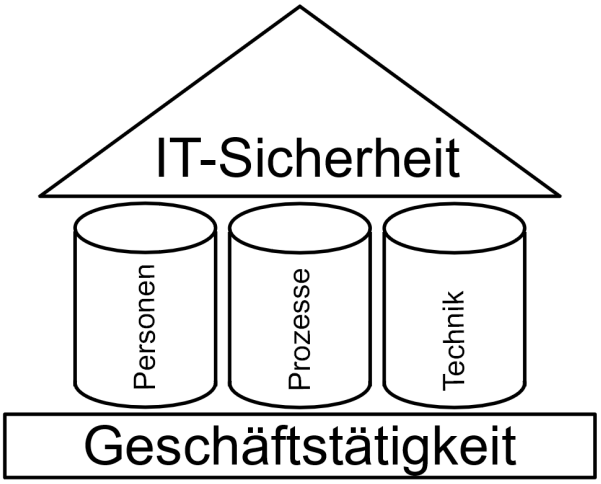
- Authentizität (authenticity): Die Echtheit und Vertrauenswürdigkeit von Informationen ist gegeben.
- Verbindlichkeit (non repudiation): Der Erhalt-von- oder eine Handlung-mit- Information ist – auch gegenüber Dritten – nachweisbar, zum Beispiel durch Signaturen.
- Zurechenbarkeit (accountability): Die eindeutige Zuordnung einer Information zu einer Identität ist gewährleistet.
- Resilienz (resilience): Die Widerstandsfähigkeit von Information gegen Störungen oder Sabotage ist gegeben.

Da die vier letztgenannten, speziellen Schutzziele nicht im Fokus von ATP-Angreifern stehen und von derartigen Angriffen nicht unmittelbar betroffen sind, werden sie in dieser Arbeit nur am Rande behandelt.

Bei der Entwicklung von technischen und organisatorischen Maßnahmen (TOM), die in Kapitel 5 aus den Abwehrstrategien abgeleitet werden, ist es wichtig, sich das Drei-Säulen-Modell der Informationssicherheit vor Augen zu führen (siehe Abbildung 1.1). Dieses Modell stellt die Säulen dar, auf denen die Sicherheit im Bereich von Geschäftsprozessen und -handlungen ruht. Wirksame Maßnahmen können demnach personeller, struktureller oder technischer Natur sein.

Lage der IT-Sicherheit in Deutschland

Zur Lage der IT-Sicherheit in Deutschland wird der aktuelle Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) herangezogen. [siehe BSI, 2019a] Demnach liegt ein Schwerpunkt der Cyber-Angriffe aktuell im Bereich Cyber-Kriminalität. Wie bereits in den vergangenen Jahren sind Infektionen durch Schadprogramme eine der größten IT-Bedrohungen sowohl für Institutionen als auch für Privatanwender. [siehe BSI, 2019a, S. 7]



Quelle: In Anlehnung an [Wegener, 2014, S. 11]

Abbildung 1.1: Drei-Säulen-Modell zur Informationssicherheit

„Die Entwickler von in der Breite verteilter Schadsoftware wie Emotet oder Trickbot adaptieren zunehmend Methoden zur Weiterverbreitung in lokalen Netzwerken (lateral movement), die bisher vor allem bei APT-Angriffen beobachtet wurden [siehe hierzu auch Abschnitt 3.2.2, Cyber Kill Chain, Anm. d. Verf.]. Sie nutzen zunächst eine sehr breit angelegte Kampagne, wählen dann aber opportunistisch sehr selektiv Ziele aus, bei denen sie sich weiter ausbreiten und weitere Malware nachladen.“ [BSI, 2019a, S. 15] Eine relativ neue Entwicklung ist demnach der Einsatz von Techniken, die bisher nur bei APT-Angriffen eingesetzt wurden. Das BSI berichtet in diesem Zusammenhang auch von einem vermehrten Einsatz von hoch spezialisierten Schadprogrammen im Kontext von kooperierender und arbeitsteilig organisierter Computerkriminalität. [siehe BSI, 2019a, S. 7] Vor diesem Hintergrund ist es für Institutionen von großer Bedeutung, über die technischen Abläufe und Möglichkeiten eines APT-Angriffs informiert zu sein.

1.3 Forschungshintergrund

Eine zentrale AVD-Umgebung, an der alle IT-Systeme einer Institution (speziell die Datenspeichersysteme) angeschlossen sind, wird meist unter dem Begriff Domäne zusammengefasst. Seit einigen Jahren empfiehlt das Bundesamtes für Sicherheit in der Informationstechnik (BSI) ebenso wie die Microsoft Corporation (MS)[3] die Einführung einer hierarchischen Struktur für den Betrieb von Domänen. Das BSI bezeichnet die Strukturierung einer Domäne als Schichtenmodell[4]. Ein solches Modell wird in

[3] MS ist mit dem Produkt Active Directory® der Marktführer für zentrale AVD-Systeme.
[4] MS Synonym hierfür: Tier-Modell. Die Bedeutung / Struktur ist identisch.

Abschnitt 4.2 näher erläutert.

Eine Kerntechnologie, die in dieser Arbeit angesprochen wird, ist das Kerberos Authentifizierungsverfahren. [siehe Eckert, 2018, S. 491ff.] Dabei handelt es sich um ein verteiltes Authentifizierungsverfahren, das etwa zeitgleich am MIT[5] [siehe Steiner et al., 1988] und an der KTH[6] [siehe Danielsson et al., 1998] entwickelt wurde. Systeme und IT-Umgebungen, die auf dieser Technologie beruhen, gehen von einer zentrale Instanz aus, die Authentifizierungen vornimmt und alle daran beteiligten Systeme vertrauen dieser Authentifizierung. Es existiert eine eindeutig abgegrenzte Menge von Objekten, die sich uneingeschränkt vertrauen. Diese Art der Authentifizierung ist seit nunmehr einigen Jahrzehnten der Quasi-Standard in allen größeren Institutionen. Wie sich gerade in den letzten Jahren herausgestellt hat, birgt diese Art der Authentifizierung auch Nachteile. In Kapitel 2 dieser Arbeit wird darauf in Abschnitt 2.4.1 näher eingegangen. Neuere Forschungen und Entwicklungen gehen von den entgegengesetzten Annahmen aus, einer *Zero-Trust-Architecture*. In Kapitel 7 wird zusammenfassend in Form eines Ausblicks auf dieser Art der Authentifizierung näher eingegangen.

1.4 Zielsetzung

Ziel dieser Abschlussarbeit ist es, Institutionen in zusammenfassender und kompakter Weise darzulegen, welchen Verlauf i. d. R. APT-Angriffe nehmen (Credential-Theft-Angriffe, Golden- und Silver-Ticket-Angriffe), welche Maßnahmen zur Absicherung bzw. Abwehr sinnvoll sind und Entscheidungshilfen anzubieten, inwieweit der mögliche Schaden bei einem Angriff den erforderlichen Aufwand zur Absicherung rechtfertigt.

Erreicht eine Institution, wie sie im Abschnitt 1.1 definiert wurde, von der Anzahl der Mitarbeiter her eine gewisse Größe, ist die Einführung eines zentral geführten Authentifizierungs- und Verzeichnisdienstes (AVD) faktisch eine Notwendigkeit. Dies folgt aus dem Umstand, dass ab einer größeren Anzahl von vernetzen Arbeitsstationen der Aufwand einer dezentralen Administration nicht mehr vertretbar ist. Diese Situation kann bereits bei kleinen Institutionen ab einer Mitarbeiteranzahl von etwa 20 Personen der Fall sein. Gerade Institutionen solcher Größe verfügen aber höchstwahrscheinlich nicht über die Mittel und Kenntnisse, um eine entsprechende Absicherung bezüglich der in dieser Arbeit beschriebenen Angriffe durchzuführen. Mit dieser Arbeit soll eine Sensibilisierung von IT-Verantwortlichen und Geschäftsführungen

[5] Projekt Athena, Massachusetts Institute of Technology, Cambridge, MA 02139 , 1988
[6] Heimdal Kerberos, Königliche Technische Hochschule (KTH), Stockholm, Schweden, 1996

speziell kleinerer Institutionen für die Gefahrenlage erfolgen und eine daraus folgende Motivation geschaffen werden, entsprechende Gegenmaßnahmen ab- und einzuleiten.

Aufbau und Struktur der Arbeit

Um Konzepte und Strategien zur Entwicklung einer hochsicheren Administrationsumgebung – im Folgenden HSA[7] genannt – abzuleiten, wird zunächst in Kapitel 2 auf die fachspezifischen Hintergründe eingegangen, die speziell bei größeren Netzwerkumgebungen von Institutionen im Einsatz sind. In Kapitel 3 werden technisch detailliert die Methoden, Werkzeuge und Abläufe eines üblichen APT-Angriffs dargelegt, um anschließend in Kapitel 4 Strategien für entsprechende Abwehrmaßnahmen abzuleiten. Dies sind unter anderem die Einführung einer Zwei-Faktor-Authentifizierung (z. B. durch Smartcards) und damit verbunden weitere Absicherungsmöglichkeiten, wie beispielsweise eine Kerberos-gebundene Authentifizierungsabsicherung (Authentication Mechanism Assurance, AMA).

In Kapitel 5 werden aus den vorgestellten Abwehrstrategien entsprechende technische und organisatorische Maßnahmen (TOM) abgeleitet, die innerhalb des internen Netzwerks einer Institution durchzuführen sind, um einen Absicherungseffekt zu erhalten. Abschließend wird in Kapitel 6 eine Einschätzung des Aufwandes für die Umsetzung der vorgestellten Konzepte und eine Gegenüberstellung des möglichen Schadens eines erfolgreichen APT-Angriffs gegeben.

Im Anhang dieser Arbeit wird in Form eines Prozessmodells prototypenhaft die Implementierung einer HSA dargestellt.

Abgrenzungen

Diese Arbeit beschäftigt sich mit Angriffsstrategien, die unter dem Begriff APT-Angriff zusammengefasst werden, und entsprechenden Abwehrmaßnahmen gegen derartige Angriffe. Bei der Betrachtung von Vorgehensweisen eines Angreifers wird vorausgesetzt, dass dieser sich bereits im Netzwerk des Opfers befindet. Eine These dieser Arbeit besagt, dass in der untersten Schicht (Schicht 2) des in Abschnitt 4.2 vorgestellten 3-Ebenen-Sicherheitsmodells eine persistente Bedrohungslage durch kompromittierte Arbeitsstationen existiert. Die Methoden und Werkzeuge (Malware, wie zum Beispiel aktuell Emotet), die nötig sind, um sich als Angreifer in das Netzwerk des Opfers in diese Ebene einzuschleusen und entsprechende Abwehrmaßnahmen, um diese Kompromittierung zu verhindern, sind nicht Bestandteil dieser Arbeit.

[7] MS Synonym für eine hochsichere Administrationsumgebung in diesem Kontext ist: „enhanced security administrative environment“ – ESAE

Der Themenschwerpunkt dieser Arbeit soll nicht auf einer Risikoanalyse oder Risikobewertung liegen, sondern auf der systematischen Entwicklung von Abwehrstrategien gegen APT-Angriffe. In Abschnitt 6.1 wird daher keine detaillierte Risikoanalyse gemäß BSI-Grundschutz [siehe BSI, 2019b] durchgeführt. Dies würde den Rahmen dieser Arbeit sprengen. Vielmehr liegt der Fokus dieser Arbeit auf Informationen und Handlungsempfehlungen für kleine, mittelständische Institutionen. Der Betrieb einer HSA bei Großunternehmen wird als selbstverständlich vorausgesetzt.

Die in Abschnitt 1.2 angesprochene Notwendigkeit für die Implementierung von Datensicherungs- und Wiederherstellungsstrategien in allen Ebenen der elektronischen Datenspeicherung innerhalb einer Institution ist nicht Bestandteil dieser Arbeit und wird entsprechend auch nicht bei den empfohlenen technischen und organisatorischen Maßnahmen behandelt.

2 Grundlagen

In diesem Kapitel werden die Voraussetzungen behandelt, die maßgeblich sind, um die in den darauf folgenden Kapiteln behandelten Methoden und Abläufe im Detail zu verstehen. Im ersten Abschnitt wird zunächst kurz auf das ISO/OSI-Kommunikationsmodell und die Grundprinzipien der Client-Server-Architektur eingegangen. Anschließend wird der Aufbau moderner Rechenzentren dargestellt. Hier ist es von essenzieller Bedeutung, zu verstehen, wie technische Abläufe im Betrieb geregelt und wie Zuständigkeiten verteilt sind. Dies erleichtert das Verständnis für entsprechende Rollenkonzepte, die im Abschnitt 4 entwickelt werden. Anschließend werden AVD-Systeme technisch detailliert vor- und die verwendeten Authentifizierungsverfahren dargestellt sowie grundlegende Informationen zu Sicherheitsmodellen und Identitätsmanagement gegeben. Für die Einschätzung der Sicherheit von AVD-Systemen ist das Verständnis dieser Strukturen essenziell, da sie einen Teil derartiger Systeme bilden können.

2.1 Das ISO/OSI Refererenzmodell

Als OSI-Modell wird eine Standarddarstellung für Netzwerkprotokolle bezeichnet, welche grundlegend den Datenaustausch zwischen zwei Kommunikationspartnern beschreibt. Es dient seit seiner Definition 1977 als Referenzmodell in allen Bereichen der Telekommunikation. Der Einsatz dieses Modells ermöglicht die reibungslose Zusammenarbeit von IT- und Telekommunikationssystemen verschiedener Hersteller. Diese Eigenschaft wird allgemein als *Open Systems Interconnection (OSI)* bezeichnet.

Entwicklungsgeschichte

Das British Standards Institute[1] trat 1977 mit der Forderung nach einem Standardarchitekturmodell an die International Organization for Standardization (ISO) heran. Die daraufhin von der ISO gegründete Arbeitsgruppe[2] beauftragte wiederum das American National Standards Institute (ANSI) mit der Entwicklung von Vorschlägen für ein Referenzmodell. Die von der ANSI entwickelten Vorschläge für ein diesbezügliches Modell basierten auf Datenbank- und Kommunikationsmodellen der Canepa-Group[3],

[1] British Standards Institute (auch abgekürzt als BSI): Weltweit erste Normungsorganisation und Gründungsmitglied der ISO. Die Abkürzung BSI ist in dieser Arbeit jedoch reserviert für das Bundesamt für Sicherheit in der Informationstechnik.

[2] ISO Technical Committee 97, Subcommittee 16

[3] Canepa-Group: Ein Entwicklungsteam der Firma Honeywell Information Systems, geleitet von Mike Canepa, massgebliche Entwicklung Charlie Bachmann.

die sich Mitte der 70er Jahre mit der Entwicklung derartiger Modelle befasst hatte. Bereits zu diesem Zeitpunkt existierende Modelle, wie die System Network Architecture (SNA) des Herstellers IBM und die Protokolle des damals im Aufbau befindlichen Advanced Research Projects Agency Network (ARPANET) wurden dabei berücksichtigt. 1977 wurde von der Canepa-Group ein Datenbankkommunikationsmodell entwickelt, welches auf sieben Schichten basiert. Firmenintern wurde dieses Modell als Distributed Systems Architecture (DSA) bezeichnet. Dieses Modell bildete die Grundlage für den Entwurfsvorschlag der ANSI. Im März 1978 präsentierte die Canepa-Group ihren Entwurf eines Kommunikationsmodells vor der ISO Arbeitsgruppe. Die ISO entschied daraufhin, dass dieses Referenzmodell größtenteils die Anforderungen an ein offenes Kommunikationsmodell (OSI) für vernetzte Systeme erfüllt und gleichzeitig genug Spielraum für zukünftige Erweiterungen lässt. Im Juni 1979 wurde von der ISO ein entsprechend siebenschichtiges Referenzmodell als Standardmodell präsentiert und standardisiert, welches auf den Entwürfen der Canepa Group und deren DSA-Modell basierte. [siehe Alani, 2014] Dieses Modell ist heute als OSI-Modell bekannt und als ISO/IEC Standard 7498-1 definiert. [siehe ISO, 1982] Eine entsprechende DIN ISO 7498 ist äquivalent.

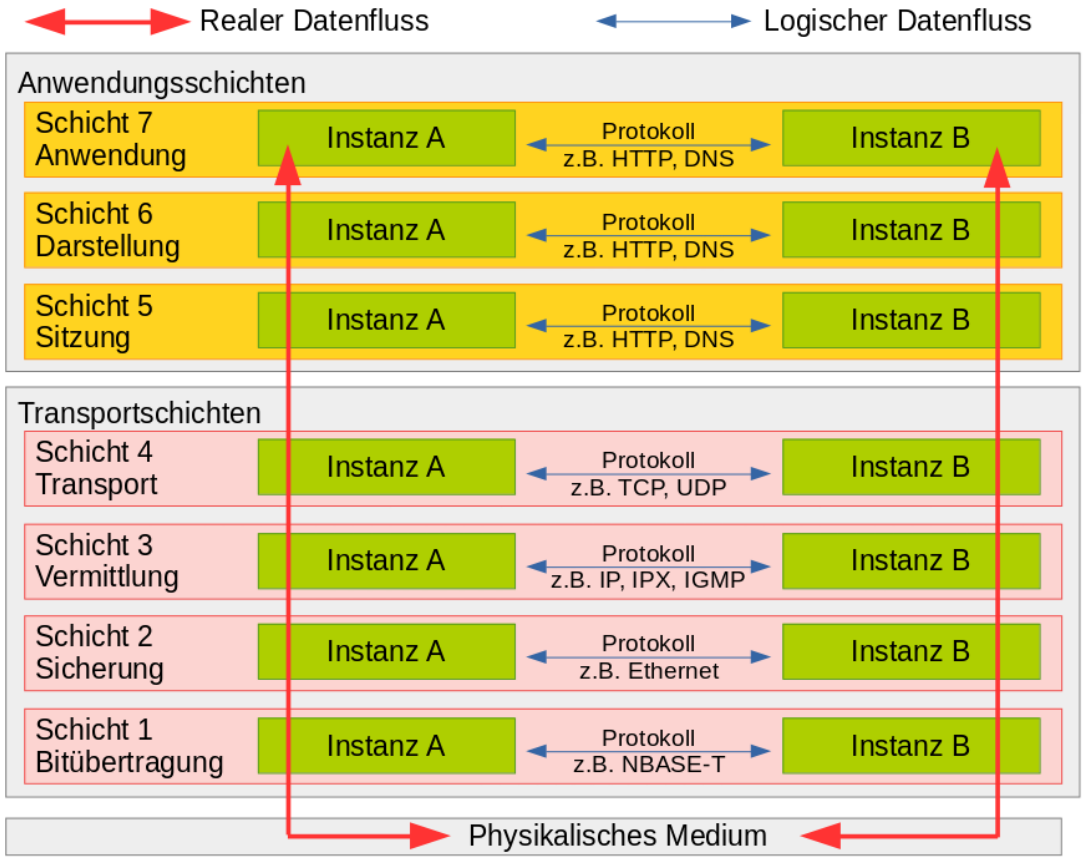
Motivation

Um zwischen zwei Kommunikationspartnern, die im Fall einer elektronischen Kommunikation als Anwendung oder Prozess interpretiert werden, einen sicheren Datenaustausch zu gewährleisten, sind verschiedenste technische Hürden zu bewältigen. Diese reichen von der Realisierung der rein elektrischen Übertragung durch ein Übertragungsmedium, über die Behandlung von Übertragungsfehlern sowie Anforderungen an die Sicherheit, bis hin zu der Interpretation der übertragenen Daten in der Anwendung oder dem verarbeitenden Prozess. Um diese Problematik auch im Umfeld von technischen Realisierungen verschiedenster Hersteller bewältigen zu können, wird ein Referenzmodell benötigt, das den Herstellern von Systemen – sei es Hardware oder Software – einen Standard zur Orientierung vorgibt, um auch in Verbindung mit Produkten anderer Hersteller reibungslos zu funktionieren.

Schichtenaufteilung

Im OSI-Referenzmodell werden die Kommunikationsabläufe zwischen zwei Kommunikationspartner in sieben Schichten (auch Ebenen genannt) aufgeteilt. Jeder Teilnehmer muss in jeder der sieben Schichten eine sogenannte Instanz besitzen, die die Spezifikationen, die in dieser Schicht erfüllt sein müssen, implementiert hat. Dabei gilt, dass die Spezifikationen für jede Schicht unabhängig und getrennt umgesetzt werden. Auf beiden Teilnehmerseiten stellt jede Instanz Dienste für die Instanz der unmittelbar

darüber liegenden Schicht bereit. Es ergibt sich so ein realer Datenfluss, der vertikal durch die Schichten erfolgt. Betrachtet man dagegen den logischen Datenfluss zwischen den beiden Teilnehmern A und B, so erfolgt der Datenfluss zwischen den Instanzen einer Schicht horizontal in Form von standardisierten Protokollen. [siehe Eckert, 2018, S. 99ff.] Dies ist in Abbildung 2.1 dargestellt.



Quelle: In Anlehnung an [Eckert, 2018, S. 100]

Abbildung 2.1: Datenfluss im OSI-7-Schichten-Modell

Einordnung von APT-Angriffen

Angreifern ist die Funktionsweise von entsprechenden Instanzen und Protokollen, basierend auf dem OSI-Modell, sehr wohl bewusst. Gleichwohl sind die im Abschnitt 3.3 besprochenen Werkzeuge meist Programme, die in die höheren Schichten (Anwendungsschichten 4 bis 7) des OSI-Modells einzuordnen sind. Grundsätzlich gilt hierbei aber folgendes Prinzip: Gelingt einem Angreifer eine Kompromittierung der Kommunikation in einer Schicht, so ist die gesamte Kommunikation oberhalb dieser Schicht ebenfalls betroffen. Als Beispiel sei folgendes Szenario beschrieben: Einem Angreifer gelingt es, in die verschlüsselte Kommunikation eines WLAN-Netzes einzudringen,

da er Kenntnis über den Pre Shared Key (PSK) erlangt.[4] Die WLAN-Kommunikation ist in diesem Beispiel laut Abbildung 2.1 in Schicht 2 des OSI-Modells einzuordnen. Da der Angreifer nun in der Lage ist, den WLAN-Verkehr mitzuschneiden, ergibt sich auch eine Gefährdung der über dieses WLAN geführten Kommunikation der höheren Protokollebenen.

2.2 Client-Server-Architektur

Die Wurzeln dessen, was heute unter dem Begriff *Client-Server-Architektur* diskutiert und realisiert wird, finden sich im Personal Computer (PC)- und Abteilungsrechnerbereich. [siehe Niemann, 1995, S. 9] Die für diese Arbeit genutzte Kategorisierung basiert auf [Bengel, 2015, S. 21ff.].

Entwicklungsgeschichte

Rechensysteme, ihr Einsatz und der Betrieb waren in den vergangenen Jahrzehnten einem starken Wandel unterzogen. Dabei lässt sich die historische Entwicklung chronologisch in folgenden Schritten skizzieren: [siehe Bengel, 2015, S. 1]

1. Stapelverarbeitung (Batch-Processing-Systeme),
2. Stapelverarbeitung (Timesharing Systeme),
3. Personal Computer und Workstation,
4. Client-Server-Systeme,
5. verteilte Systeme und
6. Web-Systeme.

1. und 2. Stapelverarbeitung (Batch-Processing- und Timesharing-Systeme)

Bei den ersten Rechensystemen handelte es sich um Großrechner und Minicomputer. Die Datenverarbeitung auf diesen Systemen wurde meist in Form einer Stapelverarbeitung (Batch Processing oder Timesharing Betrieb) durchgeführt. Am Anfang stand dabei die Abarbeitung von Befehlen und Daten, die auf Lochkarten gespeichert waren. Die Verarbeitung bestand lediglich aus Einlesen, Durchführung von Berechnungen und Ausgabe als Liste oder als sequentielle Daten zur weiteren Verarbeitung. [siehe Plattner, 1993, S. 925]

3. Personal Computer und Workstation

Etwa ab 1980 begann der Einsatz von Personal Computern und Workstations[5].

[4] Beispielsweise durch einen Angriff auf den 4-Wege-Handshake des WPA2-Protokolls kombiniert mit einem Brute-Force-Angriff oder einer Wörterbuchattacke. [siehe Rogall et al., 2019, S. 4 ff.]

[5] Als Workstation (deutsch: „Arbeitsstation“) wird in diesem Zusammenhang ein ausgesprochen fortschrittlicher Arbeitsplatzrechner für technisch-wissenschaftliche Zwecke bezeichnet.

Dieser Schritt wurde möglich durch die Entwicklung leistungsfähiger Mikroprozessoren und das Aufkommen von lokalen Netzwerken (Local Area Network, LAN), über die viele Rechensysteme miteinander gekoppelt werden konnten. Das in Abschnitt 2.1 beschriebene ISO/OSI-Referenzmodell bot dabei die Grundlage dafür, dass Anwendungen und Prozesse über LANs große Datenmengen innerhalb von Millisekunden austauschen konnten. Anfangs wurden die Betriebsmittel (Ressourcen) der Arbeitsstationen unstrukturiert im Netzwerk zur Verfügung gestellt. Jeder Rechner konnte Dienste und Betriebsmittel eines mit ihm über das LAN verbundenen Rechners nutzen. Man spricht in diesem Fall von einem *Peer-to-Peer Netz*. Die Bereitstellung von Ressourcen auf jedem Rechner verursachte jedoch einen hohen Verwaltungsaufwand.

4. Client-Server-Systeme

In der weiteren Entwicklung ging man dazu über, Dienste und Ressourcen auf bestimmten Rechensystemen zusammenzufassen. Dies erleichterte die Verwaltung und Administration der Systeme, die nun als *Server* fungierten. Die ersten so bereitgestellten Server waren Druck- und Dateiserver. Die Rechensysteme, die selbst keine Ressourcen bereitstellen, sondern über das LAN auf Serversysteme zugreifen, wurden als *Clients* bezeichnet. Mit der steigenden Komplexität von Anwendungen wurden die Serversysteme in ihrer logischen Ablaufstruktur von Prozessen immer komplexer.

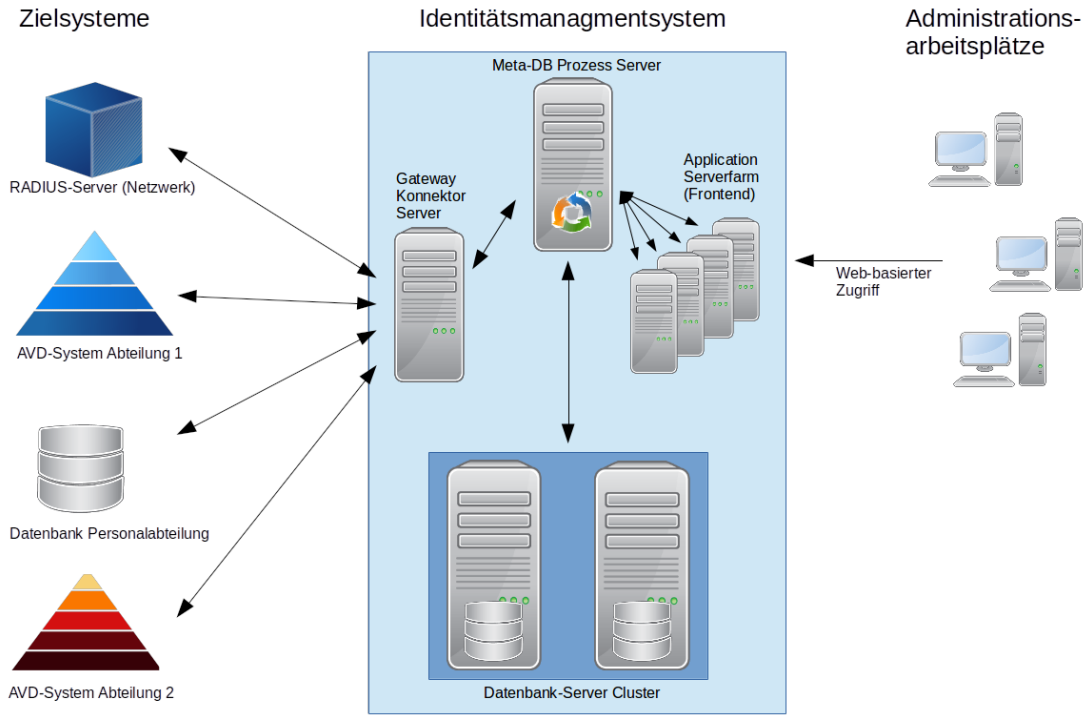
5. Verteilte Systeme

Diese zunehmend komplexere Struktur führte dazu, Prozesse auf mehreren Rechnern (Server) im Netzwerk abzubilden. Es entwickelte sich eine kooperative Ablaufstruktur von Prozessen innerhalb dieser Servergruppierungen. Ein Anwendungssystem, mit logisch auf mehrere Systeme verteilten Funktionseinheiten, die nach außen hin als ein Anwendungsserver erscheinen, wird als *verteiltes System* bezeichnet. Eine beispielhafte Darstellung eines solch komplexen Anwendungssystems[6] ist in Abbildung 2.2 wiedergegeben. Kooperative Verarbeitung ermöglicht dabei eine hohe Flexibilität der Zuordnung von Ressourcen an die jeweiligen Funktionseinheiten eines verteilten Systems. [siehe Bengel, 2015, S. 4] Die Funktionseinheit, die als Schnittstelle zum Client und zum Anwender fungiert, wird als *Frontend* bezeichnet, die Systeme, die im Hintergrund arbeiten, als *Backend*.

6. Web-Systeme

In der heutigen Zeit werden verteilte Systeme meist mit einem webbasierten

[6] In diesem Beispiel handelt es sich um eine Metaverzeichnis-Anwendung mit verschiedenen Konnektoren zu Verzeichnis- und anderen Datenbanksystemen.



Quelle: Eigene Darstellung

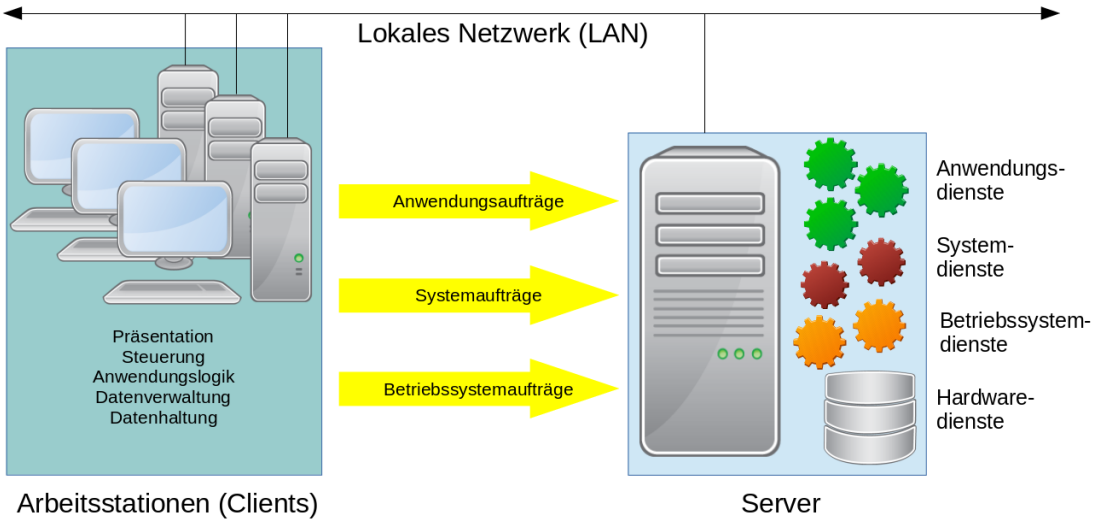
Abbildung 2.2: Beispielhafte Darstellung einer auf mehreren Servern verteilten Anwendung (Identitätsmanagementsystem)

Frontend ausgestattet. Dies bietet Institutionen eine weitestgehende Unabhängigkeit auf der Clientseite, da entsprechende Browser auf allen relevanten Client-Plattformen existieren und eine HyperText Markup Language (HTML)-basierte Benutzerschnittstelle einfach zu bedienen ist. Dokumente und Multimedia-Objekte können so auf einfache Weise über das LAN bereitgestellt werden. [siehe Dreyfus, 1998, S. 36ff.]

2.2.1 Klassifikation von Client-Server-Architekturen

Der Leitgedanke der Client-Server-Architektur ist die effektive Bereitstellung und Nutzung mehrfach verwendbarer Dienste. [siehe Niemann, 1995, S. 10] Dies wird in Abbildung 2.3 beispielhaft dargestellt. Bei der Umsetzung dieser Architektur werden folgende Schritte durchgeführt:

- Identifizierung von Diensten, die mehrfach verwendet werden können.
- Herauslösung dieser Dienste aus den Anwendungssystemen, in denen sie genutzt werden.
- Eine Realisierung in einmaliger, allgemeingültiger Form.
- Die netzwerkweite Bereitstellung mittels sinnvoller Schnittstelle – Application Programming Interface (API).



Quelle: Eigene Darstellung

Abbildung 2.3: Schematische Darstellung der Client-Server-Architektur

Client-Server-Modell

„Das am weitesten verbreitete Modell für verteilte Programme ist das *Client-Server-Modell*: Ein Prozess, der Client, fordert eine Operation oder einen Service von einem anderen Prozess, dem Server an.“ [Bengel, 2015, S. 22] In diesem Basismodell existieren mehrere Clients und ein Server. Der große Nachteil dieses einfachen Modells ist der im Zentrum stehende Server. Er bildet im Hinblick auf die Performance und die Verfügbarkeit einen Engpass, da seine Betriebsmittel begrenzt sind. Fällt der Server aus, sind die von ihm bereitgestellten Dienste für alle Clients nicht mehr verfügbar.

Verteilte Systeme und verteilte Prozesse

Die Lösung für den oben beschriebenen Engpass ist die Verteilung von Diensten (Services) auf mehrere Server, die als Gesamtheit für Clients wie ein Server erscheinen. In einer derartigen Umgebung wird ein Server, der einen Service von einem anderen Server in Anspruch nimmt, selbst zum Client. Die Server müssen somit untereinander in Interaktion treten. Dies geschieht über definierte Protokolle und bezieht gegebenenfalls auch einen systeminternen Authentifizierungsprozess mit ein. Speziell dieser Punkt ist für eine Sicherheitsbetrachtung innerhalb einer AVD-Umgebung von Bedeutung.

Client-Server-Server

Zwischen den (eventuell verteilten) Servern und den mit ihnen kommunizierenden Clients kann ein weiterer Server liegen, der als Kommunikationsknotenpunkt fungiert. Dieser Server kann dabei folgende Aufgaben erfüllen: [siehe Bengel, 2015, S. 54]

- Er ist Stellvertreter für die dahinter liegenden Server, da diese vielleicht in einem anderen Netzwerk liegen (*Proxy*).
- Er ist Vermittler zwischen dem anfragenden Client und einem auf Anfragen wartenden Server (*Broker*).
- Er vermittelt den für die Anfrage des Clients am besten geeigneten Server (*Trader*).
- Er filtert die entsprechenden Anfragen des Clients und Antworten des Servers (*Filter*).
- Er sorgt für gleichmäßige Lastverteilung der Server durch Verteilung der Anfragen auf mehrere Server (*Balancer*).
- Der vom Client angeforderte Service setzt sich aus Einzelservices zusammen, die koordiniert abgearbeitet werden müssen (*Koordinator*).
- Es werden aus der Anfrage des Clients mehrere sinnvolle Serveranfragen generiert (*Agent*).

Client-Server-Ketten

Die Anfragen beziehungsweise die Aufgaben, die ein Client an einen Server stellt, sind möglicherweise so komplex, dass sie nicht in Gänze von einem Server abgearbeitet werden können. Wenn die Abarbeitung einer Clientanfrage jedoch klar definiert und chronologisch zwischen mehreren Servern aufgeteilt werden kann, spricht man bei der Bearbeitung der Anfrage von einer *Serverkette*. Ein Server gibt dabei sein Ergebnis an einen zweiten Server weiter, für den er dabei wiederum als Client fungiert. Beispiele für eine Client-Server-Kette sind verteilte Berechnungen, die strukturell aus verschiedenen Aufgaben bestehen und dabei eine Kette bilden. Das Ergebnis einer abgeschlossenen Aufgabe bildet dabei die Eingabe für eine darauf folgende Aufgabe. Die Verbindung zwischen den aufeinander folgenden Aufgaben wird dabei als *Pipe* bezeichnet.

Client-Server-Bäume

Wird bei Client-Server-Ketten innerhalb der Abarbeitungskette auf einem Server mehr als ein Teilergebnis erzeugt und werden diese dann an mehrere Server als neue Anfragen weitergeleitet, so spricht man von *Client-Server-Bäumen*.

2.2.2 Sicherheitsbetrachtung im Hinblick auf APT-Angriffe

Wesentlich bei der Betrachtung von Client-Server-Anwendungen, insbesondere von verteilten Systemen im Hinblick auf die in dieser Arbeit behandelten APT-Angriffe, ist die Tatsache, dass zumindest bei der Kommunikation über Nachrichten oder RPCs ein

in der Regel verschlüsselter und authentifizierter Kanal benutzt wird. Gerade innerhalb der Serverkonstellation eines verteilten Systems sind diese Kommunikationskanäle genauer zu betrachten. Am Beispiel des Identitätsmanagementsystems in Abbildung 2.2 auf Seite 14 sind folgende Kommunikationskanäle innerhalb der verteilten Systeme vorhanden:

- Zwischen dem Meta-DB-Prozess-Server und dem Datenbank-Server-Cluster,
- zwischen dem Meta-DB-Prozess-Server und dem Gateway-Konnektor-Server und
- zwischen dem Meta-DB-Prozess-Server und jedem der Applikationsserver.

Dies wird durch die in Abbildung 2.2 dargestellten Verbindungspfeile verdeutlicht. Die Verbindung zum Datenbank-Server Cluster in diesem Beispiel beruht auf dem Protokoll Structured Query Language (SQL). Dieser Kanal wird in der Regel durch eine Authentifizierung mittels Benutzername und Password abgesichert. In vielen Fällen wird diesbezüglich ein Benutzerkonto in einem zentralen AVD-System geführt. Ein derartiges Benutzerkonto wird auch als *Dienstkonto* (Service Account) bezeichnet. Da diese Art von Konten für die Kommunikation zwischen Rechnersystemen benutzt werden, haben sie meist die Eigenschaft, dass das zugehörige Passwort nicht abläuft, also nicht in regelmäßigen Abständen geändert wird. Angesichts dieser Eigenschaft bilden sie eine besondere Schwachstelle gegenüber Angreifern, sofern nicht andere Maßnahmen zur Absicherung, wie beispielsweise die Erhöhung der Kennwortkomplexität, getroffen werden.

Vorstellbar ist zum Beispiel folgender Brute-Force-Angriff: Ein Angreifer versucht, durch wiederholte Authentifizierungsversuche mit einem derartigen Dienstekonto unter Einsatz verschiedener Passwortkombinationen das Passwort entweder erfolgreich zu erraten oder im ungünstigstem Fall zu erreichen, dass dieses Konto auf dem AVD-System gesperrt wird. Dieser Fall kann eintreten, wenn für diese Art von Konto eine maximale Anzahl von Authentifizierungsfehlversuchen im AVD-System konfiguriert ist. Eine Sperrung hätte in diesem Fall zur Folge, dass der Meta-DB-Prozess-Server nicht mehr mit der entsprechenden Datenbank kommunizieren kann. Ein Totalausfall des gesamten verteilten Systems wäre die Folge, was gleichbedeutend mit einem DoS-Angriff ist.

2.3 Aufbau und Struktur moderner verteilter Rechenzentren

Von Rechenzentren (RZ) wird grundsätzlich gesprochen, wenn an einem oder mehreren Orten zentral die Recheninfrastruktur einer Institution zusammengefasst wird. Das BSI bezeichnet diesen Bereich als „IT-Betriebs-Bereich“ [siehe BSI, 2019b, INF.2]. Bei kleineren Institutionen kann es sich dabei um einen kleinen umfunktionierten Abstellraum (Serverraum), bei größeren Institutionen um ganze Gebäudeteile bis hin zu speziell für diesen Zweck errichtete Funktionsgebäude handeln. Weitere Funktionsbereiche sind mitunter mit dem Betrieb eines Rechenzentrums verbunden:

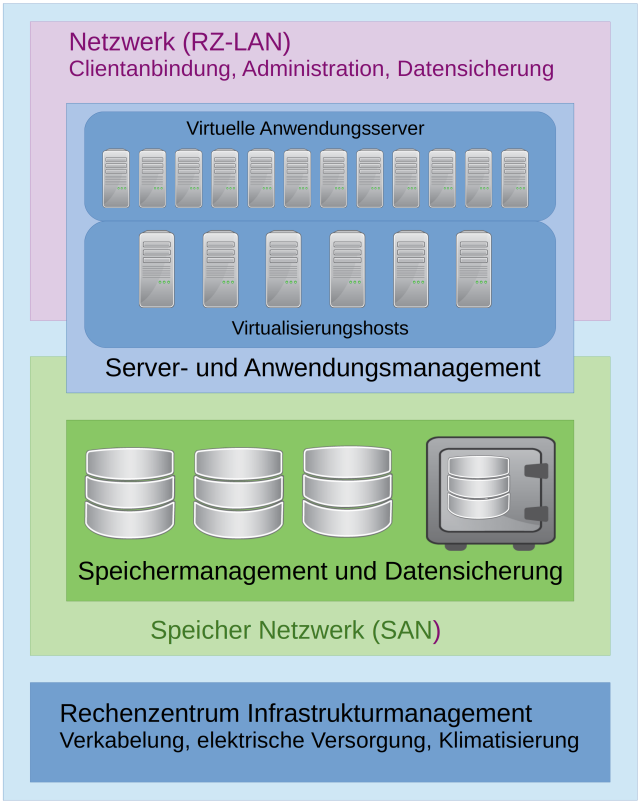
- Sicherheits- und Zugangskontrolltechnik,
- Stromversorgung, unterbrechungsfrei mitunter batteriegestützt,
- Klima- bzw. Kälteversorgung mittels Kühlungssystemen und
- spezielle Löschanlagen zur Brandbekämpfung.

Das BSI spricht in diesem Kontext von „technischen Support Bereichen“ [siehe BSI, 2019b, INF.2 S. 1ff]. Um eine Einordnung für die Schutzziele Integrität, Vertraulichkeit und Authentizität zu gewährleisten, ist eine Betrachtung des logisch-strukturellen Aufbaus einer zentralen Rechenarchitektur innerhalb eines Rechenzentrums erforderlich, denn daraus lassen sich Aufgaben und entsprechende Rollen und Berechtigungen ableiten, die in späteren Abschnitten dieser Arbeit bei der Beurteilung von APT-Angriffen herangezogen werden. Ein grundsätzlicher logischer Aufbau der Rechenarchitektur in einem Rechenzentrum mit Darstellung der Funktionsebenen und Aufgaben ist in Abbildung 2.4 dargestellt. Innerhalb großer Institutionen ist es sinnvoll, nicht nur ein Rechenzentrum (RZ) zu betreiben, sondern die Rechentätigkeit auf mehrere Standorte zu verteilen. Die Verfügbarkeit wird dadurch erhöht. Fällt an einem Standort die Stromversorgung der Anlagen aus, können die Rechendienstleistungen von einem anderen Standort übernommen werden. Die Kopplung von RZ-Funktionen erfolgt dabei in mehreren Ebenen, wie Abbildung 2.5 zeigt.

Virtualisierung

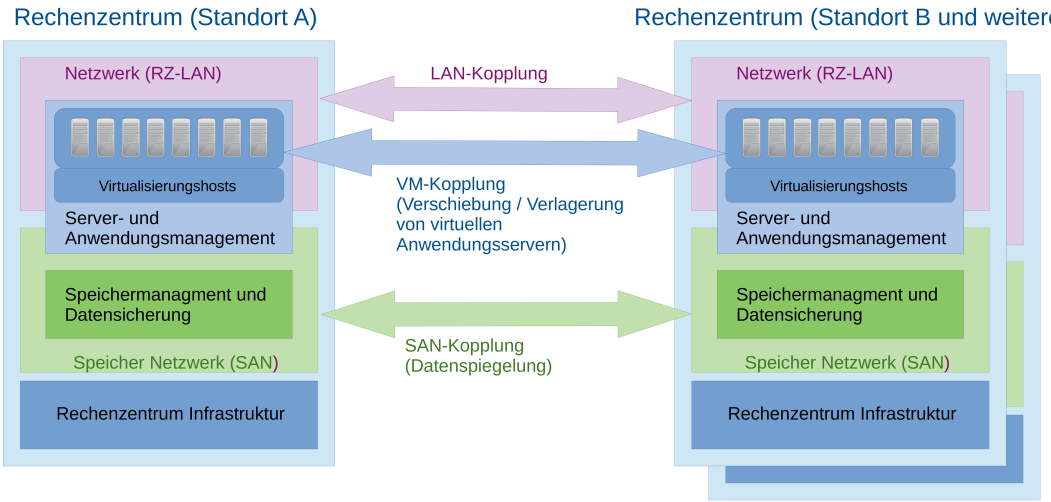
Die Entwicklung der Virtualisierungstechnologie hat den Betrieb von Rechenanlagen in den letzten beiden Jahrzehnten auf revolutionäre Weise verändert. In der IT-Technik spricht man dabei von Virtualisierung, wenn eine Abstraktionsebene[7] eingeführt wird, um logische Ressourcen zu generieren, die auf einer real existierenden Ressource

[7] Abstraktion in diesem IT-technischen Sinn bedeutet Komposition und Generalisierung. [siehe Glinz, 2005, Kap.12] Es können dabei Ressourcen aus mehreren Teilressourcen zusammengesetzt werden unter Verallgemeinerung der technischen Merkmale.



Quelle: Eigene Darstellung

Abbildung 2.4: Struktur und Aufgaben eines Rechenzentrums



Quelle: Eigene Darstellung

Abbildung 2.5: Ebenen der Kopplung mehrerer Rechenzentren

aufbauen. Dieses Vorgehen bietet Institutionen die Möglichkeit, Ressourcen effektiver auszunutzen. Institutionen konnten in den vergangenen Jahren durch die Einführung der Virtualisierungstechnologie erhebliche Kosteneinsparungen realisieren, bedingt unter anderem durch weniger Raum- und Energiebedarf für Rechentechnologien. Die Entwicklung von *Cloud Computing* als eine Art von IT-Infrastruktur wurde erst durch die Virtualisierungstechnologie möglich.
Kumar unterscheidet dabei verschiedene Arten von Virtualisierungsebenen: [siehe Kumar et al., 2015, Kap.IIff.]

Speichervirtualisierung

(Storage virtualization), bedeutet die Zusammenfassung von Datenspeichern und die zentrale Verwaltung der einzelnen Speicherbereiche. Das einzelne Datenspeichergerät (Festplatte) ist dabei nicht mehr als solches sichtbar, sondern nur noch eine logische Speichereinheit (Logical Unit Number, LUN). Für die Nutzung virtueller Speicherbereiche durch Server werden spezielle Netzwerke verwendet, die als Storage Area Network (SAN) bezeichnet werden. Diese Technologie bietet signifikante Vorteile, wie eine effektivere Ausnutzung von Datenspeichern und eine zentrale Verwaltung.

Servervirtualisierung

(Server virtualization), ermöglicht die Nutzung einer physikalischen Recheneinheit (Host) durch mehrere Betriebssysteme gleichzeitig. Auf der realen Hardware wird dabei eine Abstraktionsschicht eingeführt, die es möglich macht, eine oder mehrere virtuelle Maschinen (VM) zu betreiben. Diese Art der Abstraktion bietet Vorteile im Hinblick auf die effektive Ausnutzung von vorhandenen Hardware-Ressourcen (CPU, Arbeitsspeicher, I/O), aber auch ein gewisses Maß an Hardwareunabhängigkeit, da eine VM auf einer virtuellen Hardwareabstraktion beruht und damit auf einem Host mit vergleichbarer Abstraktion lauffähig ist, auch wenn die darunter liegende reale Hardware unterschiedlich ist.

Netzwerkvirtualisierung

(Network virtualization), ermöglicht die Aufteilung eines physikalischen Netzwerkes in mehrere virtuelle Netze, sogenannte Virtual Local Area Networks (VLAN). Dies bringt zum einen eine erhöhte Flexibilität bei der Zuordnung von Endgeräten zu Netzwerksegmenten, aber auch einen positiven Performance-Aspekt. Durch die VLAN-Segmentierung können Broadcast-Domänen[8] verkleinert werden, wodurch die Netzlast durch Broadcast-Pakete sinkt. Ebenfalls erfolgt eine Absicherung des Netzwerkverkehrs durch VLAN-Segmentierung.

[8] Ein logischer Verbund innerhalb dessen ein Broadcast alle Teilnehmer erreicht.

Anwendungsvirtualisierung

(Application virtualization), ermöglicht die Abstraktion von Anwendungen gegenüber einem darunter liegenden Betriebssystem. Dadurch werden Anwendungen unabhängiger von bestimmten Betriebssystemressourcen, wie beispielsweise Dynamic Link Library (DLL) in bestimmten, vorausgesetzten Versionen.[9]

Arbeitsspeichervirtualisierung

(Memory virtualization), bezeichnet den Prozess der Abstraktion von physikalisch vorhandenen Speicher. Eine frühe Form dieser Virtualisierungsart ist die *Virtuelle Speicherverwaltung*, wie sie in allen heute gängigen Betriebssystemen praktiziert wird. [siehe Eckert, 2018, S. 47] Durch diese Technik kann beispielsweise real vorhandener Arbeitsspeicher durch *Swapping* erweitert werden. Betrachtet man Arbeitsspeichervirtualisierung im Zusammenhang mit oben beschriebener Servervirtualisierung, so können sich mehrere VMs auf einem Host den vorhandenen physikalischen Arbeitsspeicher teilen.

Desktopvirtualisierung

(Desktop virtualization), bezeichnet eine spezielle Form der Clientvirtualisierung. Dabei wird eine komplette Arbeitsstationsinstallation (Desktop) virtualisiert. Eine entsprechende Umgebung mit einer Vielzahl von Desktop-Virtualisierungen wird als Virtual Desktop Infrastructure (VDI)-Umgebung bezeichnet. Dabei verlagert sich der Hardwareeinsatz für Endanwender-Desktops, die in einer Institution eingesetzt werden, hin zu sogenannten *Thin-Clients* und zentral bereitgestellten VDI- oder Terminalservern.

Heterogene Netzwerke

Eine Netzwerkumgebung wird als heterogenes Netzwerk bezeichnet, wenn die Komponenten des Netzwerks und die daran angeschlossenen Geräte in den Ebenen des OSI-Modells, wie im Abschnitt 2.1 beschrieben, unterschiedlich sind in Bezug auf Hersteller, Technologie und Software.

Im Gegensatz hierzu waren in den 80er- und 90er-Jahren oft homogene Kommunikationstechnologien, wie Großrechneranwendungen üblich, die konsequent von einem Hersteller geliefert und betrieben wurden. Solche im engen technologischen Rahmen gefassten Netzwerke mit einheitlicher Hardware, einheitlichen Netzwerkprotokollen und Netzwerktopologien haben ihre Vorteile. Die Wartung und Verwaltung ist über-

[9] Ein schon älteres Beispiel für eine Anwendungsvirtualisierung ist der *Windows-XP-Modus*, der mit dem Betriebssystem MS Windows 7 eingeführt wurde, um eine Laufzeitumgebung für ältere Anwendungen bereitzustellen, die ursprünglich für MS Windows XP erstellt wurden.

sichtlicher und überschaubarer. Die Programmkompatibilität ist gegeben. Dieser Umstand wird jedoch meist durch eine direkte Herstellerabhängigkeit erkauft.

Heterogene Netzwerke hingegen bieten den großen Vorteil der allgemeinen Herstellerunabhängigkeit. Technologien sind so flexibel einsetzbar. In der heutigen Zeit bezeichnen heterogene Netzwerkumgebungen Netze, in denen Betriebssysteme der Hersteller Microsoft (Windows), Apple (macOS, iOS) und unixoide Betriebssysteme – insbesondere Linux Derivate – gleichzeitig eingesetzt werden. Im Netzwerkbereich, beim Einsatz von Netzkomponenten wie Switches und Routern, sind homogene Netzausprägungen heute eher selten. Die von vielen Institutionen aus wirtschaftlichen Gesichtspunkten geforderte Herstellerunabhängigkeit bei der Neu- und Ersatzbeschaffung überwiegt hier meist die technischen Argumenten einer leichteren Administration der Komponenten. Die Auslegung des Begriffes „heterogen“ wird je nach Hersteller und Anbieter einer Technologie mal enger oder weiter gefasst. Im Netzwerkbereich hat sich aktuell das Protokoll Ethernet gegenüber Token Ring und TCP/IP gegenüber NetBUI als Standard durchgesetzt, der von allen Herstellern unterstützt wird.

Auf den höheren Ebenen des OSI-Referenzmodells, ab Schicht 5 (Anwendungsschichten) wird es bei dem Einsatz der Protokolle durchaus komplizierter. Als Beispiel sei hier auf die Authentifizierungsverfahren hingewiesen, die in Abschnitt 2.4.1 näher beschrieben werden. Der Softwarehersteller Microsoft Corporation (MS) setzt oft eine homogene Netzwerkumgebung, bestehend ausschließlich aus MS Windows Clients und Servern voraus, die problemlos mit der Kerberos-Implementierung der Microsoft Corporation umgehen können. [siehe Microsoft, 2018] In der Praxis existieren aber heterogene Umgebungen, in denen Fachverfahren und Anwendungen existieren, die eventuell auf älterern Protokollen wie NTLM oder Simple Bind beruhen. Gerade bei der Sicherheitsbetrachtung in Bezug auf APT-Angriffe ist es von sehr großer Bedeutung, sich Klarheit darüber zu verschaffen, wie und mit welchen Methoden und Protokollen in einer IT-Umgebung verfahren wird.

Aufgaben und Rollen im Rechenzentrumsbetrieb

Aus den in Abbildung 2.4 dargestellten Strukturebenen lassen sich folgende Aufgaben und Rollen innerhalb des Rechenzentrumsbetriebs ableiten:

Anwendungsadministration

Die Anwendungsadministration ist verantwortlich für den Betrieb der Anwendungen, die meist auf Anwendungsservern, wie im Abschnitt 2.2.1 beschrieben, betrieben werden. Häufig sind diese Server virtualisiert, werden demnach im

Rahmen einer Servervirtualisierung betrieben. Die dazugehörige Rolle hat administrativen Zugriff auf die jeweiligen virtuellen Maschinen (VMs).

Serveradministration

Die Serveradministration ist verantwortlich für den Betrieb der Servervirtualisierungsumgebung. Die entsprechende Rolle hat demnach administrativen Zugriff auf die Virtualisierungsserver (Hosts) selbst. Ein Zugriffsrecht in dieser Ebene bedeutet meist gleichzeitig auch einen administrativen Zugriff auf alle auf den Hosts laufenden VMs, da auf deren virtuelle Konsolen zugegriffen werden kann.[10]

Speicheradministration

Die Aufgabe dieser Rollengruppe ist das Management und die Bereitstellung der zentralen Speichergeräte innerhalb einer Institution. Meist wird damit auch das Management der Datensicherungen verknüpft.

Netzwerkadministration

Dieser Rollengruppe fällt die Aufgabe zu, das Institutionsnetzwerk zu betreiben. Im Rahmen dieser Rolle ist der Vollzugriff auf den Netzwerkverkehr, in der Regel mindestens bis zur Schicht 3 des ISO/OSI Schichtenmodells, möglich.

Betrieb Zugangstechnik, Klima- und Kältetechnik sowie Stromversorgung

Im Rahmen dieser Rollengruppe wird die Anlagen- und Stromversorgungstechnik sowie Kälte- und Klimatechnik betrieben, die zur Gebäude- und Gebäudeleittechnik gehört. Bei größeren Institutionen sind hier mitunter eigene Haustechniknetze in Betrieb.

Sicherheitsbetrachtung im Hinblick auf APT-Angriffe

Die oben aufgezählten Aufgaben werden schon aufgrund der benötigten fachlichen Qualifikation innerhalb der Institutionen meist von verschiedenen Personen wahrgenommen. Zur Bewältigung der Aufgaben sind zudem bestimmte Berechtigungen, aber auch bestimmte technische Zugänge zu Managementsystemen notwendig. Die Absicherung dieser Zugänge kann auf sehr unterschiedliche Weise erfolgen. Oft werden diese Systeme zur Authentifizierung und Autorisierung mit dem zentralen AVD-System gekoppelt. Dies vereinfacht das Management von Benutzerkonten für das Betriebspersonal, birgt aber auch Gefahren im Hinblick auf einen möglichen APT-Angriff.

[10] Einige am Markt befindliche Virtualisierungslösungen, wie zum Beispiel vSphere des Herstellers VMware, erlauben im Enterprise-Umfeld eine sehr granular konfigurierbare Rollen- und Berechtigungsstruktur.

Folgendes Szenario wäre denkbar: Ein zentrales AVD-System ist durch einen Angreifer kompromittiert worden, wie in Kapitel 3 beschrieben. Die Zugänge zu den Managementsystemen für die Energieversorgung und die Klimatechnik des Rechenzentrums der Institution werden durch Benutzerkonten und Passwörter geschützt, die in diesem kompromittierten AVD-System verwaltet werden. Einem Angreifer wäre es nun möglich, unbemerkt ein entsprechendes Benutzerkonto des Betriebspersonals zu verwenden und sich damit Zugang zu Systemen zu verschaffen, die die direkte Kontrolle der Energieversorgung oder der Klimatechnik ermöglichen. Durch diesen nicht autorisierten Zugriff könnte ein erheblicher Schaden entstehen, z. B. durch einen manipulierten Stromausfall oder Hardwareschäden durch Störung der Klimaanlage.

2.4 Aufgabe und Aufbau von Authentifizierungs- und Verzeichnisdiensten

Bei einem zentralen Authentifizierungs- und Verzeichnisdienst-System handelt es sich in der Regel um ein verteiltes Serversystem (siehe Abschnitt 2.2.1), das folgende Dienste zur Verfügung stellt:

- Authentifizierungsdienst,
- Verzeichnisdienst und
- spezielle Dateiserverdienste zur Verwaltung von Clients.

Das gesamte AVD-System dient dabei der Verwaltung und Zuweisung von Identitäten, Rollen und zugeordneten Berechtigungen[11].

Begriffsdefinition der Identität

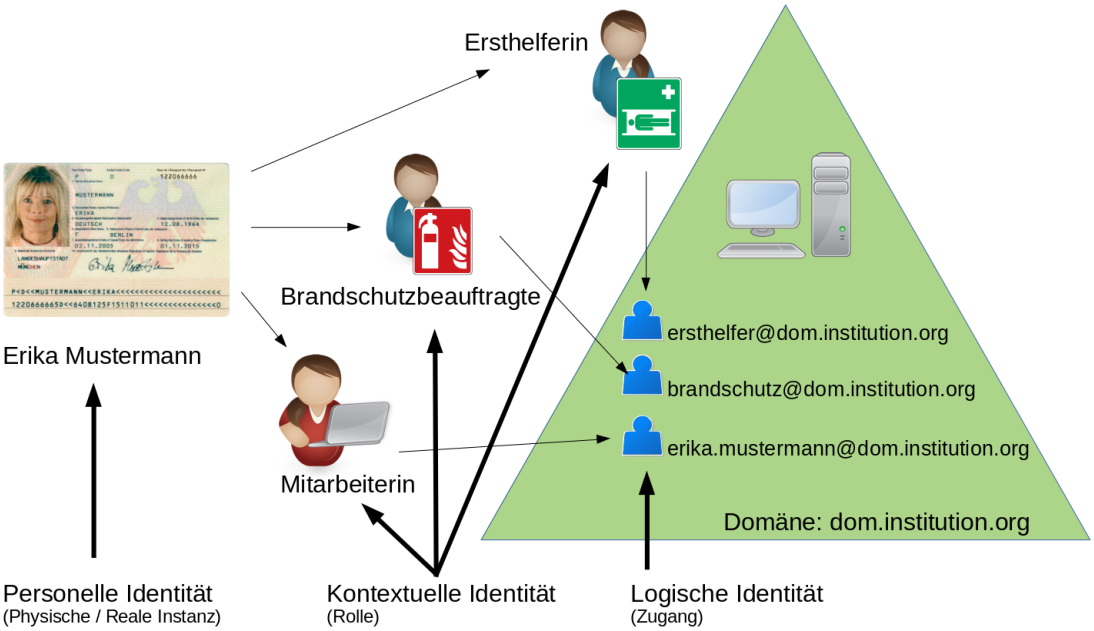
Tsolkas definiert den Identitätsbegriff wie folgt:

> - „Eine Identität repräsentiert eine bestimmte Kombination von Eigenschaften und Rollen eines Objekts (physisch, kontextuell, logisch), die mit einem eindeutigen Bezeichner benannt wird. Die einzelnen Rollen und Eigenschaften bestimmen die Art, wie eine Identität agiert und interagiert (z. B. welche Informationen mit anderen Identitäten ausgetauscht werden).
> - Es lassen sich Gruppen von Identitäten bilden, die über die gleichen Eigenschaften verfügen.

[11] Ein AVD-System des Hersteller Microsoft Corporation bietet zusätzliche Dienste zur zentralen Verwaltung von Richtlinien und Einstellungen für Benutzer und Computer innerhalb einer Domäne.

- Durch die Übernahme von Rollen kann eine Person mehrere kontextuelle und logische Identitäten besitzen. Ein Mitarbeiter kann demnach im Unternehmen mehrere Identitäten leben, indem er andere Rollen und Eigenschaften annimmt.“ [Tsolkas et al., 2017, S. 24ff.]

Ein Schwerpunkt dieser Arbeit liegt auf kontextuellen und logischen Identitäten, die über Rollen verknüpft sind. Eine logische Identität bezeichnet Tsolkas auch als technische Identität. [siehe Tsolkas et al., 2017, S. 26] Der Begriff technische Identität wird in Bezug auf die in dieser Arbeit betrachteten AVD-Systeme äquivalent zu dem Begriff Konto oder Benutzerkonto verwendet. Ein Konto wird im Verzeichnisdienstteil eines AVD-Systems als Konten-Objekt abgebildet, welches über definierte Attribute verfügt, wie z. B. einen Benutzernamen oder ein Passwort (siehe Abbildung 2.12 auf Seite 39). Der Zusammenhang zwischen den verschiedenen Identitätsformen wird in Abbildung 2.6 verdeutlicht.



Quelle: In Anlehnung an [Tsolkas et al., 2017, S. 27]

Abbildung 2.6: Zusammenhang der personellen, kontextuellen und technischen Identität

Technische Identitäten (Konten) können verschiedenen Identitätsträgern zugeordnet werden. In einem AVD-System werden nicht nur Benutzerkonten verwaltet, deren Repräsentant eine natürliche Person ist. Auch Computersysteme (Server und Clients) sowie Dienste (Applikationen) können im AVD-System über eine technische Identität verfügen. Man bezeichnet diese Arten von Identitäten dann als Computerkonto oder Dienstkonto.

2.4.1 Authentifizierungsverfahren

Im Rahmen der Berechtigungszuweisung innerhalb eines IT-Systems muss eine logische Identität ermittelt werden. Dieser Prozess wird Authentifizierung genannt. Der Prozess der Zugriffskontrolle mittels Authentifizierung wird bei Tsolkas wie folgt definiert: „Bei der Zugriffskontrolle über Authentifizierung werden während des Prozesses der Authentifizierung entweder eine Identität, eine Person oder ein Computersystem überprüft. Authentifizierung (v. griechischen „authentikós“ für Urheber, der Echte, der Wirkliche), bedeutet, eine Identität durch eine identitätsgebundene Information zu überprüfen und zu bestätigen. Dies kann auf verschiedene Art und Weise erfolgen.“ [Tsolkas et al., 2017, S. 129] Tsolkas weist weiterhin daraufhin, dass Authentisierung im englischen Sprachgebrauch mit Authentifizierung gleichgesetzt wird. In der deutschen Sprache jedoch meint Authentisierung die eigene Identität zu überprüfen. [siehe Tsolkas et al., 2017, S. 129] Im Rahmen des Überprüfungsprozesses kann die Identität durch drei unterschiedliche Arten von Nachweisobjekten verifiziert werden:

- Wissen in Form eines Kennwortes oder einer PIN.
- Anwendung eines in Besitz befindlichen Objekts (z. B. Token oder Smartcard).
- Darstellung einer Eigenschaft des eigenen Subjekts (z. B. Biometrie).

Von besonderer Bedeutung in dieser Arbeit sind Identitätsnachweise mittels Kennwort und durch Besitz einer Smartcard als Schlüsselspeicher, der durch eine PIN geschützt wird.

Charakterisierend für ein Authentifizierungsverfahren ist seine Effektivität, die durch die Abbruchrate ausgedrückt werden kann, und die damit verbundene Benutzerakzeptanz. Im Zusammenhang mit der Benutzerakzeptanz wird häufig über ein Verfahren mit einmaliger Authentifizierung im Laufe einer Sitzung gesprochen (Single Sign-on Verfahren). Prinzipiell sind Systeme mit benutzerfreundlicher einmaliger Authentifizierung, die das Benutzerkennwort nur einmal abfragen, dazu gezwungen, dieses – oder den Hash des Kennwortes – zu speichern. Dies birgt prinzipielle Sicherheitsrisiken, da der Speicherort ein Angriffsziel darstellen kann.

Klassische Authentifizierungsverfahren

Zu den ältesten Methoden der Identitätsfeststellung in der IT gehört die Authentifizierung durch eine Benutzerkennung und ein zugeordnetes Kennwort. Dieses Informationspaar wird auch als Anmeldeinformation (credential) bezeichnet. Es handelt sich dabei um eine wissensbezogene Authentifizierung, bei der die Benutzerkennung eine in der Regel öffentliche und das Kennwort eine private Information darstellt. Das Kennwort stellt bei dieser Authentifizierungsvariante den sicherheitskritischen Teil dar. Es

sollte nicht an unsicheren Orten gespeichert werden. Man unterscheidet Kennwörter bezüglich ihrer Anwendung und Komplexität wie folgt:

- Einmalkennwörter (One-Time Password, OTP): Ändern sich nach jeder Benutzung im Rahmen einer Anmeldung.
- Permanente Kennwörter: Haben keine zeitliche Befristung, sollten jedoch eine gewisse Komplexität und Zeichenlänge aufweisen.
- Zeitlich befristete Kennwörter: Müssen nach Ablauf eines definierten Zeitraums geändert werden.

Die Zeichenlänge und Komplexität[12] lässt sich bei modernen AVD-Systemen als Kennwort-Richtlinie (Password Policy) definieren. Da diese beiden Parameter den kryptografischen Schlüsselraum bilden, müssen sie zur Absicherung gegenüber Brute-Force-Angriffe entsprechend gewählt werden.

Die kennwortbasierte Authentifizierung wird in vielen klassischen Authentifizierungsprotokollen angewendet, wie beispielsweise:

- Simple Bind (LDAP-Authentifizierung),
- Challenge-Response-Verfahren (z. B. NTLM, SSL) und
- ticketbasierte Verfahren (z. B. Kerberos).

In weiteren Kapiteln dieser Arbeit spielen gerade die klassischen Authentifizierungsprotokolle NTLM und Kerberos eine zentrale Rolle. Daher wird im Folgenden auf diese beiden Protokolle konkret eingegangen.

NTLM

Die NT Lan Manager (NTLM) Protokollfamilie gehört zur Klasse der Challenge Response Authentifizierungsverfahren. [siehe Proehl, 2012, S. 57] Es wurde ursprünglich von der Microsoft Corporation Mitte der 90er-Jahre als proprietäres Protokoll zur Authentifizierung innerhalb der Windows-Produktreihe entwickelt. Dort ist es fester Bestandteil des Windows Security Support Provider Interface (SSPI) Frameworks. Die Open Source Entwicklung *SAMBA*[13] beruht auf einer mittels Reverse Engineering entwickelten Version von NTFS [siehe Glass, 2003]. Durch Einwirkung der USA und der EU hat die Microsoft Corporation die Spezifikationen zu NTLM im Jahr 2007 veröffentlicht [siehe Microsoft, 2007].

[12] Die Komplexität einer Zeichenkette beschreibt die Vorgaben, welche Zeichengruppen (Zahlen, Kleinbuchstaben, Grossbuchstaben, Sonderzeichen) verwendet werden müssen.

[13] Quelle: `http://www.samba.org`

Im Rahmen des NTLM-Protokollprozesses werden drei Nachrichten übermittelt: [siehe Glass, 2003, S. 3]

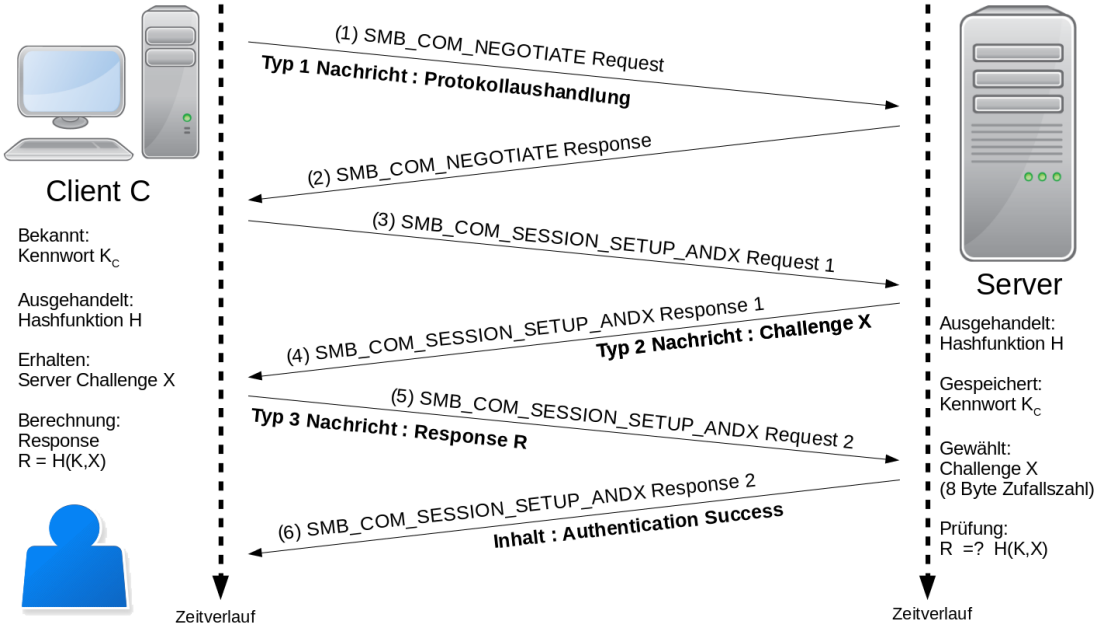
1. Die Protokollaushandlung (Negotiation)
   Der NTLM initiierende Client sendet eine Anfrage zum Server, in der er die Protokollvarianten anfragt (Typ 1 Nachricht).

2. Die Challenge
   Der Server antwortet mit den Protokollvarianten, die er akzeptiert, und einer Zufallszahl, der eigentlichen Challenge (Typ 2 Nachricht).

3. Die Antwort (Response)
   Der Client antwortet mit Domänen- und Benutzernamen und dem, mit dem Kennwort verschlüsselten, Hashwert der Zufallszahl. (Typ 3 Nachricht).

Der prinzipielle Ablauf eines NTLM Authentifizierungsprozesses ist in Abbildung 2.7 dargestellt. Im Rahmen des NTLM Authentifizierungsprozesses wird das Kennwort niemals im Klartext übermittelt, sondern lediglich eine Challenge und eine Response in Form des verschlüsselten Kennwortes und einer 8-Byte-Zufallszahl. Diese Daten können von einem Angreifer abgehört werden. Im Abschnitt 3.4.1 wird ein entsprechender Angriff näher vorgestellt. Um einen Replay-Angriff zu unterbinden, darf jede Challenge nur einmal verwendet werden. Die verschiedenen Protokollversionen unterscheiden sich in Form der Typ 3 Nachricht (Response) in der Implementierung und Berechnung des Kennworthashs in Bezug auf die Zeichenkettenlänge, die in die Berechnung einfließt. Unterschieden werden sechs verschiedene Typ 3 Nachrichten:

- Die LM (LAN Manager) Antwort, wird von Windows 9x Clients gesendet,
- die NTLM Antwort von Windows-NT-basierten Systemen (2000 und XP),
- die NTLMv2 Antwort, verwendet ab Windows NT Service Pack 4,
- die LMv2 Antwort, ersetzt die LM Antwort in Umgebungen mit NTLMv2,
- die NTLMv2 Sitzungsantwort, wenn NTLMv2 Sitzungssicherheit ausgehandelt wurde und
- die anonyme Antwort als Sonderfall, wenn keine echte Authentifizierung angefordert wurde.



Quelle: In Anlehnung an [Microsoft, 2007, S. 68] und [Proehl, 2012, S. 58]

Abbildung 2.7: Darstellung des NTLM Authentifizierungsprozesses

Im Geltungsbereich eines AVD-Systems kann das Verhalten der beteiligten Systeme und die Benutzung der verschiedenen NTLM-Protokollversionen mithilfe einer Sicherheitsrichtlinie granular vorgegeben werden. Die unterschiedlichen Verhaltensweisen der beteiligten Clients und der AVD-Server, in diesem Fall die Domain Controller, sind in Tabelle 2.1 dargestellt.

Allen Versionen von NTLM gleich ist die Eigenschaft, dass das Kennwort für jede erneute Challenge, das bedeutet für jeden erneuten Authentifizierungsvorgang, zur Berechnung des Hashwertes vorliegen muss. Eine Single Sign-on (SSO) Implementierung ist also nur möglich, wenn das Kennwort auf dem Client zwischengespeichert wird. Die Ursprungsversion von NTLM, die heute auch NTLMv1 genannt wird, ist hinsichtlich der Hash-Ermittlung als unsicher zu betrachten und sollte nicht mehr verwendet werden.

NTLM Pass-Through-Authentifizierung

Um eine NTLM-Authentifizierung auch in größeren Umgebungen mit zentral gespeicherten Benutzernamen und Kennwörtern durchführen zu können, wurde seitens des Herstellers Microsoft Corporation die Protokollerweiterung *NTLM Pass-Through Authentication* eingeführt. [siehe Microsoft, 1996] In dieser Protokollerweiterung werden vom Server die vom Client in Schritt 5 (siehe Abbildung 2.7) erhaltenen Daten (Response) und die Challenge an den Domain Controller als NETLOGON_NETWORK_-

Tabelle 2.1: NTLM Kompatibilitätsebenen – LMCompatibilityLevel

NTLM Setting	Client Verhalten	DC Verhalten
Level 0 Sendet LM and NTLM Antworten; keine NTLMv2 Sitzungssicherheit.	LM und NTLM wird benutzt, aber keine NTLMv2 Sitzungssicherheit.	Akzeptieren LM, NTLM und NTLMv2 Authentifizierungen.
Level 1 NTLMv2 Sitzungssicherheit wenn ausgehandelt.	LM und NTLM wird benutzt; NTLMv2 Sitzungssicherheit, wenn der Server es unterstützt.	LM, NTLM, and NTLMv2 Authentifizierung wird unterstützt.
Level 2 Es werden nur NTLM Antworten gesendet.	Nur NTLM wird benutzt und NTLMv2 Sitzungssicherheit, wenn der Server es unterstützt.	LM, NTLM, and NTLMv2 Authentifizierung wird unterstützt.
Level 3 Es werden nur NTLMv2 Antworten gesendet.	Benutzt NTLMv2 Authentifizierung und NTLMv2 Sitzungssicherheit, wenn der Server es unterstützt.	LM, NTLM, und NTLMv2 Authentifizierung wird unterstützt.
Level 4 DCs weisen LM Antworten ab.	Benutzt NTLMv2 Authentifizierung und NTLMv2 Sitzungssicherheit, wenn der Server es unterstützt.	Akzeptiert NTLM and NTLMv2; LM Authentifizierung wird abgewiesen.
Level 5 DCs weisen LM und NTLM Anfragen ab.	Benutzt NTLMv2 Authentifizierungund und NTLMv2 Sitzungssicherheit, wenn der Server es unterstützt.	Akzeptiert nur NTLMv2; LM und NTLM wird abgewiesen.

Quelle: In Anlehnung an [Cook et al., 2001, S. 18]

INFO-Nachricht gesendet. Der Domain Controller übernimmt daraufhin die Überprüfung der Response mithilfe des in der zentralen Datenbank gespeicherten Kennworts. Ist die Überprüfung erfolgreich, sendet der Domain Controller eine NETLOGON_VALIDATION_SAM_INFO4-Nachricht an den Server zurück, die u. a. Autorisierungsdaten des authentifizierten Benutzers enthält. Der Server sendet daraufhin die in Schritt 6 (siehe Abbildung 2.7) dargestellte Authentication-Success-Nachricht an den Client.

Kerberos

Das Kerberos-Authentifizierungsprotokoll geht einen anderen Weg, um die Identität zu bestätigen. [siehe Kohl et al., 1993] Es handelt sich dabei um ein ticketbasiertes Protokoll, welches ein Ticket bzw. einen Sitzungsschlüssel (Session Key) und einen Authentikator benutzt, um eine Authentifizierung erfolgreich durchzuführen. Beide Faktoren basieren auf einem asymmetrischen Kryptosystem. In einer Kerberos-Umgebung wird jede Identität als *Principal* bezeichnet. Man unterscheidet hierbei in Benutzer- und

Dienste-Principals. Eine dritte, als vertrauenswürdig geltende Instanz (Trusted Third Party, TTP), ist das Kerberos-Schlüsselverteilungscenter (Kerberos Key Distribution Center, KDC). Diese Rolle ist zentraler Bestandteile eines AVD-Servers bzw. eines Domain Controllers.

Es gibt im Rahmen der Kerberos-Implementierung zwei Anforderungen, die im realen Praxisbetrieb einer Institution häufig zu Problemen führen und dem exklusiven Einsatz dieses Protokolls entgegenstehen. [siehe Proehl, 2012, S. 67]

1. Die System-Uhrzeit aller beteiligten Systeme muss annähernd synchron sein, da wie im Folgenden beschrieben, ein Zeitstempel als Parameter des Authentifizierungsprozesses verwendet wird.

2. Die Domain Name System (DNS) Funktionalität muss auf allen beteiligten Systemen eine identische Struktur aufweisen und zu exakt den gleichen Ergebnissen führen, da ein Kerberos-Principal-Name aus einem DNS-Namensteil zusammengesetzt wird.

Bei den nachfolgenden Abbildungen haben die verwendeten Abkürzungen folgende Bedeutung:

- C: Name des Clients (Prinzipal)
- S: Name des Servers (Prinzipal)
- IP: Netzwerkadresse
- LT: Gültigkeitszeitraum
- TGS: Ticket Granting Server
- KAS: Kerberos Auth. Server
- KDBM: Administrationserver
- K_x: Privater Schlüssel von x
- $K_{x,y}$: Sitzungsschlüssel von x und y
- $\{abc\}K_x$: abc verschlüsselt mit Schlüssel von x
- $T_{x,y}$: Ticket von x für die Benutzung durch y
- A_x: Authentikator von x
- WS: Workstation
- Z: Zeitstempel

Ein Kerberos-Ticket wird nach Darstellung (2.1) gebildet. Als Parameter wird u. a. ein Gültigkeitszeitraum (LT) verwendet. Die so erstellten Tickets können im Gültigkeitszeitraum beliebig oft verwendet werden. Ein Kerberos Authentikator hingegen wird gemäß Darstellung (2.2) gebildet.

$$Ticket = \{S,C,IP,Z,LT,K_{S,C}\}K_S \tag{2.1}$$

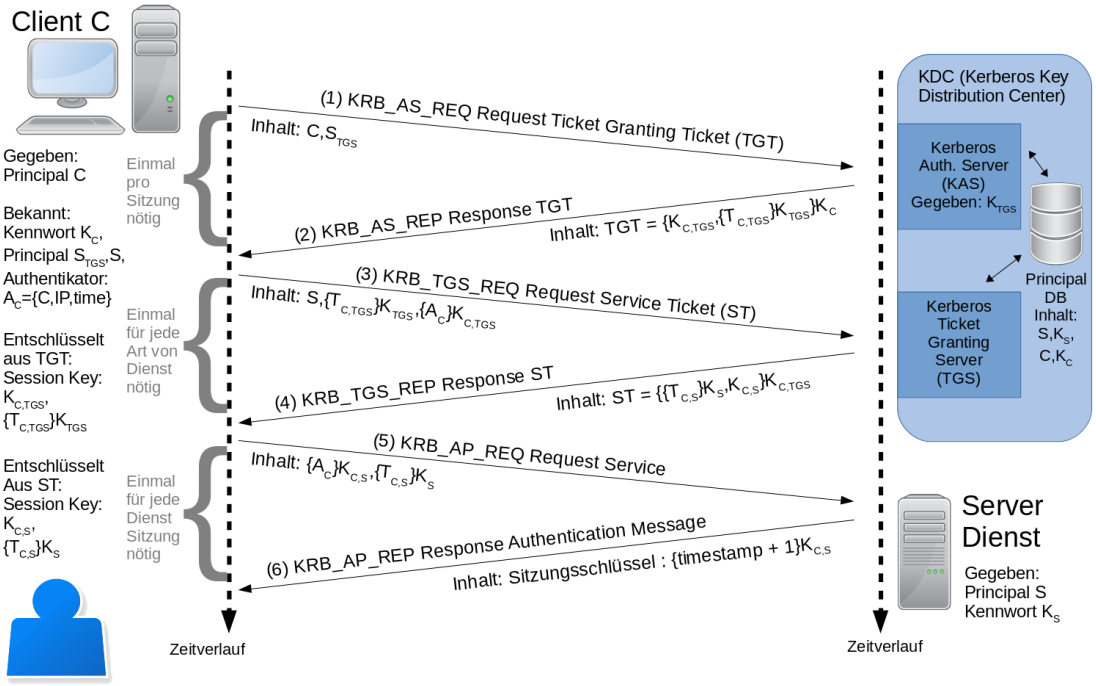
$$Authentikator = \{C,IP,Z\}K_{S,C} \tag{2.2}$$

Ein vom KAS erstelltes Ticket Granting Ticket (TGT) wird gemäß Darstellung 2.3 gebildet. Daraufhin erstellte Kerberos Service Ticket (ST) besitzen die in Darstellung 2.4 beschriebenen Komponenten.

$$TGT = \{K_{\mathrm{C,TGS}}, \{T_{\mathrm{C,TGS}}\}K_{\mathrm{TGS}}\}K_{\mathrm{C}} \tag{2.3}$$

$$ST = \{\{T_{\mathrm{C,S}}\}K_{\mathrm{S}}, K_{\mathrm{C,S}}\}K_{\mathrm{C,TGS}} \tag{2.4}$$

Der genaue Ablauf einer Kerberos-Authentifizierung wurde von Steiner et al. definiert [siehe Steiner et al., 1988] und wird in Abbildung 2.8 dargestellt.



Quelle: In Anlehnung an [Steiner et al., 1988] und [Proehl, 2012, S. 71]

Abbildung 2.8: Darstellung des Kerberos Authentifizierungsprozesses

Eine Zusammenfassung der Funktionsweise der Kerberos-Authentifizierung liefert Pröhl:

> „Anstatt Langzeitschlüssel oder Passwörter über das Netzwerk zu senden, kommt Kerberos mit verschlüsselten Nachrichten aus. Der Kerberos-Server (KDC) übermittelt dem Client Principal und dem Service Principal ein gemeinsames Geheimnis in Form eines Session Key. Diese Übertragung ist mit den jeweiligen Langzeitschlüsseln verschlüsselt. Die beiden

> Principals beweisen sich dann gegenseitig ihre Kenntnis dieses gemeinsamen Geheimnisses und authentisieren sich somit. Ab nun werden kurzlebige Authentisierungsmerkmale eingesetzt, die wiederum zwischengespeichert werden können, um wiederholt auf Dienste zugreifen zu können. Langzeitschlüssel oder Passwörter müssen vom Client dafür nicht gespeichert werden.“ [Proehl, 2012, S. 74]

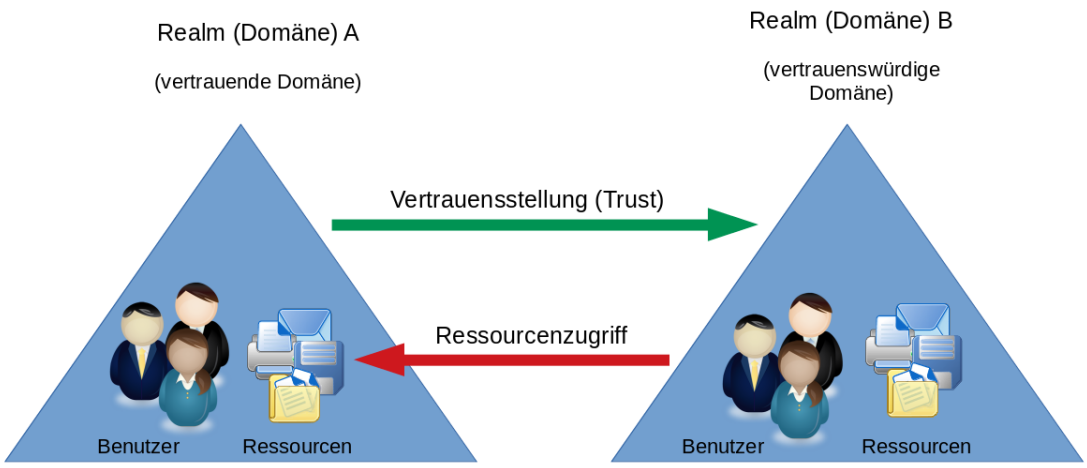
In der Praxis jedoch wird der Gültigkeitszeitraum ausgestellter Tickets auf mehrere Stunden beschränkt. Wird ein Single Sign-on Mechanismus angestrebt, der einen längeren Zeitraum als den Gültigkeitszeitraum der Tickets beinhaltet, muss das Kennwort bzw. der Kennworthash auf dem Client zwischengespeichert werden.

Kerberos-Vertrauensstellung

Der Kontroll- bzw. Zuständigkeitsbereich einer Kerberos-Umgebung, d. h. die Menge aller direkt zugeordneten Principals wird als Kerberos-Realm bezeichnet. In Bezug auf eine kombinierte Authentifizierungsumgebung (NTLM und Kerberos), wie sie in dieser Arbeit funktional als AVD-System bezeichnet wird, ist die Bedeutung des Begriffes Kerberos-Realm gleichzusetzen mit dem Begriff Domäne. Ein Kerberos-Realm bzw. eine Domänenstruktur wird in der Literatur üblicherweise mit einem dreieckigen Struktursymbol gekennzeichnet.

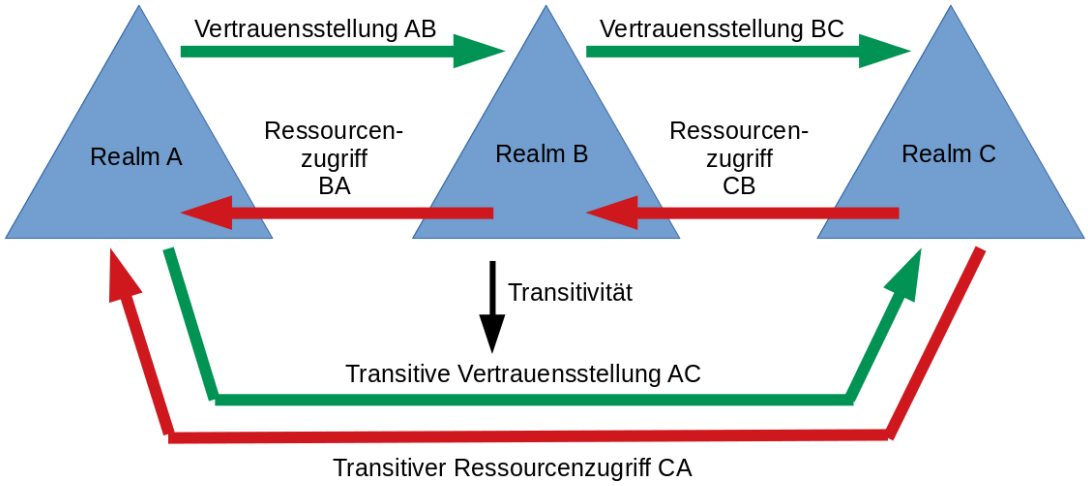
Zwischen zwei unabhängigen Kerberos Realms kann ein logischer Kanal eingerichtet werden, der als Kerberos-Vertrauensstellung (Realm Kerberos-Trust) bezeichnet wird. Eine derartige Vertrauensstellung bezeichnet dabei genauer das Vertrauen in eine Authentifizierung, die nicht von der eigenen Authentifizierungsstelle durchgeführt wurde, sondern von einem vertrauenswürdigen Realm. Abbildung 2.9 verdeutlicht den Zusammenhang. Die Vertrauensstellung basiert auf dem Austausch eines gemeinsamen Schlüssels (Shared Key) zwischen der vertrauenden und vertrauenswürdigen Kerberos-Struktur. Derartig eingerichtete Vertrauensstellungen sind grundsätzlich einseitig. Wird eine Vertrauensstellung auch in entgegengesetzter Richtung benötigt, wird ein zweiter Schlüsselaustausch nötig. Im Ergebnis spricht man von einer bidirektionalen oder beidseitigen Vertrauensstellung.

Kerberos-Strukturen können über beliebig viele Vertrauensstellungen verknüpft werden. Die dabei entstehenden Ketten von gekoppelten Strukturen können, müssen aber nicht zwangsläufig, über eine Transitivität verfügen, wie in Abbildung 2.10 dargestellt. Die Technik der Kerberos-Vertrauensstellung wird in Abschnitt 5.2 im Rahmen der logischen Anbindung einer HSA angewendet.



Quelle: Eigene Darstellung

Abbildung 2.9: Darstellung der Kerberos-Vertrauensstellung



Quelle: Eigene Darstellung

Abbildung 2.10: Darstellung der Kerberos-VS-Struktur und -Transitivität

Moderne Authentifizierungsverfahren

Authentifizierungsverfahren wurden bezüglich des Sicherheitsaspektes in den vergangenen Jahrzehnten stetig weiterentwickelt. Zu den moderneren Verfahren zählen derzeit folgende:

- Zwei-Faktor-Authentifizierung (2FA) beziehungsweise
- Multi-Faktor-Authentifizierung (MFA),
- kontextbezogene und risikobasierte Authentifizierung,
- Authentifizierung basierend auf biometrischen Merkmalen sowie
- smartcardbasierte Authentifizierung mit Zertifikaten.

Grundlegendes Merkmal bei diesen Verfahren ist die Verlagerung beziehungsweise Verknüpfung des Authentifizierungsnachweises „Wissen“ mit einem zweiten Faktor. Bei kontextbezogenen Authentifizierungsmechanismen werden Richtlinien in Bezug auf Parameter des Authentikators (wie z. B. geografischer Ort, Uhrzeit, IP-Adresse oder Gerätetyp) in den Authentifizierungsprozess einbezogen. Erfolgt beispielsweise ein Authentifizierungsprozess am Wochenende von einer Arbeitsstation, die mittels VPN-Tunnel, extern angebunden ist, wird ein Token[14] verlangt. Wird dieser Anfrageprozess jedoch von einer Arbeitsstation aus dem internen LAN unter der Woche durchgeführt, wird nur ein Kennwort abgefragt.

Aktuelle Authentifizierungsprotokolle, die primär im Fokus von webgestützten Authentifizierungssystemen entwickelt wurden, sind:[15]

- OAuth, Open Standard for Access Delegation [Jones et al., 2012],
- OpenID Connect 1.0 [Zhang et al., 2017],
- Security Assertion Markup Language (SAML) [Rosenberg et al., 2004, S.20],
- Fast IDentity Online (FIDO) [Pereira et al., 2018] und
- Active Directory® Authentifizierungsbibliothek (ADAL) [Bertocci, 2016].

Eine Authentifizierungsabsicherung mittels Besitz (Smartcard) innerhalb einer hochsicheren Administrationsumgebung (HSA) wird in Abschnitt 4.4 näher betrachtet.

2.4.2 Aufgaben des Verzeichnisdienstes

Im Wesentlichen handelt es sich bei einem zentralen Verzeichnisdienst um eine streng hierachische und objektorientierte Datenbank, welche netzwerkseitig über das LDAP-Protokoll (Lightweight Directory Access Protocol) angesprochen wird. Die Objekte

[14] Eine zusätzliche Hardwarekomponente, die im Rahmen des Authentifizierungsprozesses eingesetzt wird, um beispielsweise ein One-Time Password-(OTP) in Form eines Zahlencodes zu generieren.

[15] Weiterführende Literatur zu den angegebenen Standards sind in den Literaturhinweisen zu den Standards gegeben.

der Datenbank werden nach einem Objektschema angeordnet, welches die Position, die Objektattribute und die Berechtigungen innerhalb der Hierachie genau definiert. Sie dient unter anderem der Datenverwaltung von Benutzer-, Computer- und Gruppenobjekten. Die Zugriffskontrolle mittels des RBAC-Zugriffsmodells (siehe Abschnitt 2.5.1) auf alle Daten, die im Verwaltungsbereich eines AVD-Dienstes angesiedelt sind, wird über derartige Objekte innerhalb der Datenbank abgebildet.

Entwicklungsgeschichte

Nusser beschreibt, dass der Verzeichnisdienst, in der Art, wie er heute Verwendung findet, aus einer funktional reduzierten Form des in den 80iger Jahren entstandenen X.500 Standards hervorgegangen ist. [siehe Nusser, 1998, S. 107ff] Dieser Standard wurde demnach entwickelt, um ein physisch verteiltes, jedoch logisch einheitliches Verzeichnis zu schaffen, das Informationen über Benutzer, Organisationen und Ressourcen beinhaltet. Der X.500-Standard war wesentlicher Bestandteil des OSI-Referenzmodells, der erstmals im Jahr 1988, von der CCITT, heute als ITU-T bekannt, als Standard veröffentlicht wurde. [siehe Eichler, 1993] Das CCITT beschreibt ein Directory wie folgt: „The Directory is a collection of open systems which cooperate to hold a logical database of information about a set of objects in the real world.“ [CCITT, 1989, VIII.8 S. 6] Nusser beschreibt auch, dass das heute verwendete Verzeichnisdienstprotokoll LDAP, dem OSI-Protokoll DAP nachempfunden ist. [siehe Nusser, 1998, ebd.] Folgende Entwicklungsstufen sind für die heutige Version des LDAP-Verzeichnisdienstes relevant:[16]

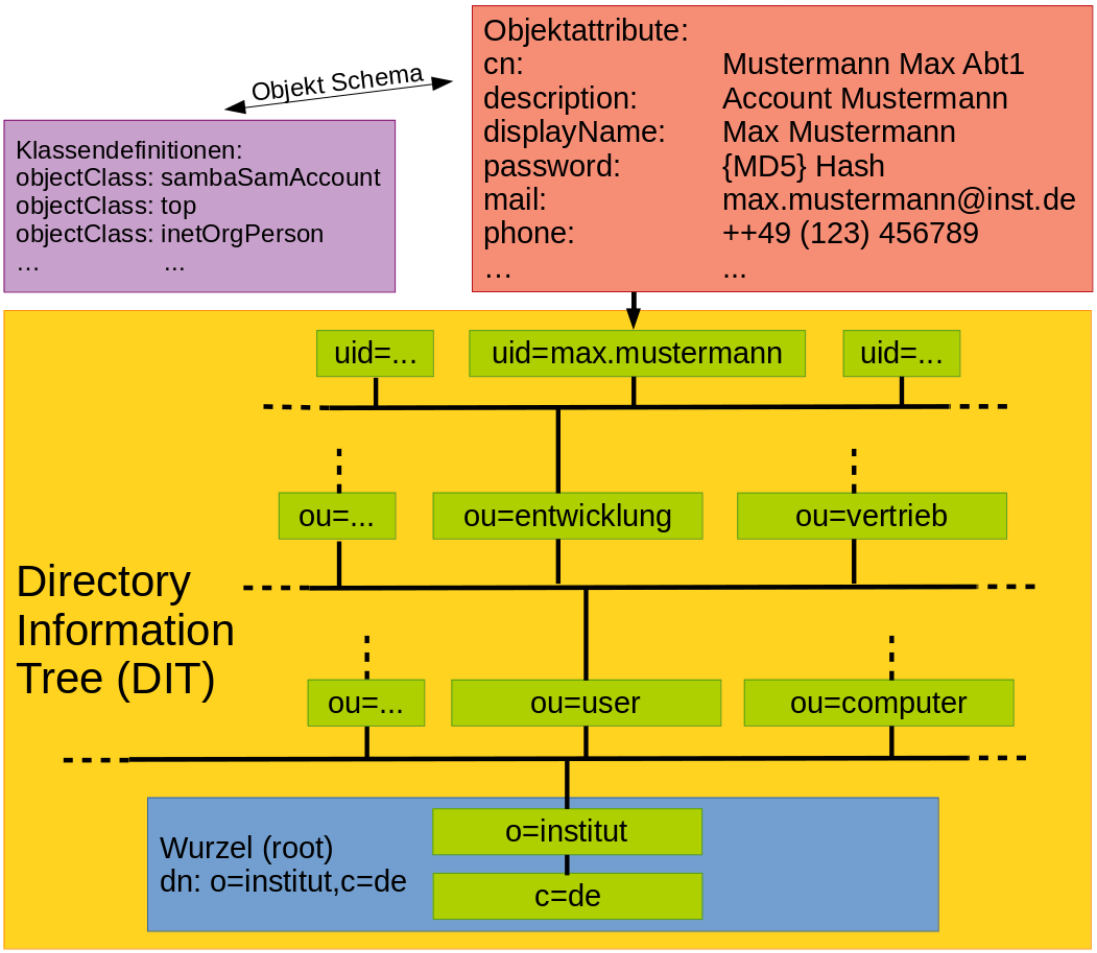
- 1993: Erste Veröffentlichung des Lightweight Directory Access Protocols als RFC1487[Yeong et al., 1993].
- 1995: LDAPv2 wird als RFC1777 veröffentlicht [Yeong et al., 1995].
- 1995: LDAP API wird als Standard RFC1823 veröffentlicht [Howes et al., 1995].
- 1997: LDAPv3 wird als RFC2251 definiert [Wahl et al., 1997].
- 1997: LDAPv3 Objekt-Schema wird als RFC2256 definiert [Wahl, 1997].
- 2006: LDAPv3 wird als neue RFC4510 spezifiziert [Zeilenga, 2006a].
- 2006: Schemastruktur wird als RFC4520 definiert [Zeilenga, 2006b].

Datenmodell

Häckelmann et al. zufolge ist die wesentliche Aufgabe eines Verzeichnisdienstes die Verwaltung eines Datenbestandes, der in X.500-Terminologie als Directory Information Base (DIB) bezeichnet wird. [siehe Häckelmann et al., 2000, S. 389] Die DIB ist als

[16] Weiterführende Literatur zu den angegebenen Standards sind in den Literaturhinweisen zu den Standards gegeben.

baumartige Struktur organisiert. Soll dieser Aspekt betont werden, wird der Datenbestand als Directory Information Tree (DIT) bezeichnet. Ein beispielhafter Ausschnitt eines Objektbaums ist in Abbildung 2.11 dargestellt.



Quelle: In Anlehnung an [CCITT, 1989, VIII.8 S. 9]

Abbildung 2.11: Beispielhafte Darstellung eines Directory Information Tree

Die Kernaufgabe liegt nach Häckelmann et al. im Integrationsaspekt sowie der zentralisierten Datenhaltung. „Anstatt verschiedene Teilnehmerverzeichnisse zu verwalten und zu benutzen, sollen in einem Verzeichnissystem die Adressen verschiedener Dienste integriert werden. Telefonbücher, Adreßbücher, Fax-Listen, E-Mail-Adressen etc. sind folglich in einem einzigen System zusammenzufassen. Außerdem sollen über solche Systeme Redundanzen, die zu Inkonsistenzen und einem Verlust an Aktualität führen können, vermieden werden. Anstelle vieler lokaler Verzeichnisse existiert nur ein zentraler Datenbestand mit aktuellen und konsistenten Adressen“ [Häckelmann et al., 2000, S. 389].

Häckelmann et al. beschreiben weiterhin, dass die Benutzung von Verzeichnisdiens-

ten nicht nur auf Personen beschränkt ist, sondern auch von anderen Softwaresystemen erfolgen kann. „Neben der naheliegenden Integration in E-Mail-Systeme, können Anwendungen, die in irgendeiner Form auf sich im Zeitablauf ändernde Adressen von Personen, Organisationen, Geräten oder anderen Einrichtungen zugreifen, Nutzer von Verzeichnissystemen sein. Verzeichnissysteme können beispielsweise verwendet werden, um in einem Workflow-Management-System Bearbeiter für einzelne Arbeitsschritte zu adressieren, um in Netzwerken Drucker oder andere Ressourcen anzusprechen, deren Adressen im Verzeichnis hinterlegt sind, oder um in der Prozesssteuerung einzelne Maschinen anzusteuern.“ [Häckelmann et al., 2000, S. 389]

Innerhalb moderner Verzeichnisdienste existieren mitunter mehrere, voneinander getrennte hierarchische Zweige, die auch als Partitionen bezeichnet werden. Sie trennen funktionale Datenbankbereiche. In Verzeichnisdiensten des Herstellers Microsoft Corporation gibt es neben der regulären Objektpartition[17] eine Konfigurations-, Schema- und mitunter eine DNS-Partition, sofern der DNS-Dienst auf dem Domain Controller (DC) domänenintegriert betrieben wird.

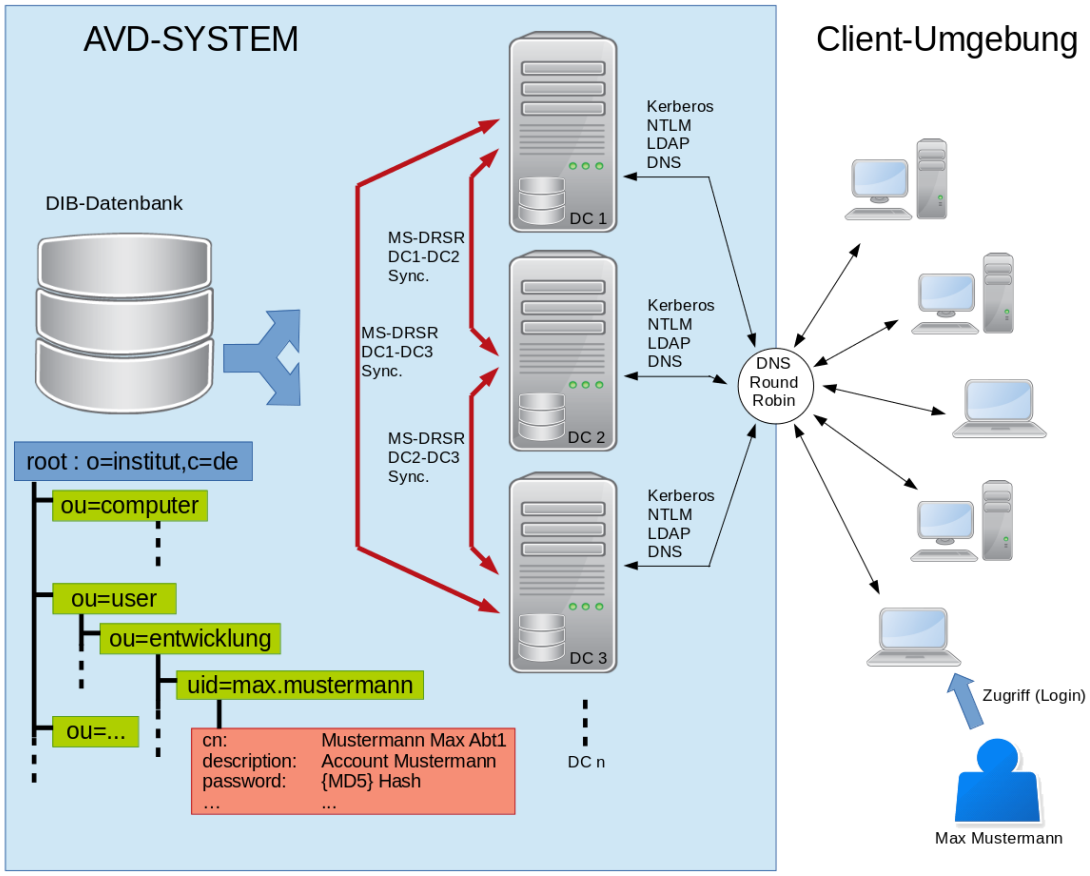
2.4.3 Aufbau zentraler AVD-Systeme

Aus Performancegründen und auch aus Gründen der Verfügbarkeit können die zentralen Dienste, die innerhalb einer Domäne zur Verfügung gestellt werden müssen, von zwei oder mehr Serversystemen bereitgestellt werden. Diese Serversysteme bilden dann ein verteiltes System, wie es in Abschnitt 2.2.1 beschrieben wurde. Kennzeichnend für solch ein System ist die einheitliche Darstellung der Dienste nach außen. Aus Sicht der anfragenden Clients ist es unerheblich, mit welchem der Server aus dem Verbund kommuniziert wird, da alle DC über den gleichen Datenbestand verfügen. Auch bei der zugrunde liegenden Datenbank handelt es sich in diesem Fall um eine verteilte Datenbank. Die Datenbank liegt mit identischem Informationsstand auf jedem DC vor. Dieser Umstand bedingt eine schnelle und reibungslose Übertragung von Änderungen an der verteilten Datenbank. Zu diesem Zweck sind auf jedem DC aktueller Ausprägung Synchronisations- und Replikationsverfahren implementiert. Der Hersteller Microsoft Corporation (MS) benutzt aktuell zu diesem Zweck das Directory Replication Service Remote Protocol (MS-DRSR)-Verfahren. Dieses Protokoll ist in jedem MS Domain Controller implementiert und kann nicht abgeschaltet oder deaktiviert werden. Das Verfahren stellt sicher, dass die einzelnen Domain Controller zu jedem Zeitpunkt über identische Informationen verfügen[18]. Eine gleichmäßige

[17] Die Microsoft Corporation bezeichnet die reguläre Partion als: „Standardmäßiger Namenskontext“.

[18] Die Synchronität ist beispielsweise bei einem benutzerseitigen Kennwortänderungsprozess ein kritischer Punkt. Der eigentliche Änderungsprozess wird von einem der beteiligten DC durchgeführt.

Verteilung der Anfragelast vonseiten der Clients wird meist durch ein DNS-Round-Robin-Verfahren erzielt. Clients sprechen in diesem Fall einen DC nicht explizit über seinen FQDN an, sondern vielmehr benutzen sie den DNS-Namen der Domäne. Hinter diesem DNS-Eintrag sind alle IP-Adressen der DCs verzeichnet, die für diese Domäne die entsprechenden Dienste bereitstellen. Diese Technik sorgt dafür, dass alternierend jede DNS-Anfrage auf einen anderen DC verweist, was in erster Linie die Performance des Gesamtsystems erhöht. Werden gleichzeitig aufseiten der Clients fehlertolerante Systeme verwendet, d. h. Systeme die bei erfolglosen Verbindungsversuchen mit einer Ziel-IP des AVD-Systems eine erneute DNS-Anfrage stellen, kann auch die Verfügbarkeit des Gesamtsystems gesteigert werden.



Quelle: Eigene Darstellung

Abbildung 2.12: Darstellung eines verteilten AVD-Systems

In Abbildung 2.12 ist der prinzipielle Aufbau eines verteilten AVD-Systems dargestellt. Die von einem AVD-System bereitgestellten Dienste werden in Tabelle 2.2

Die Änderung muss sofort auf alle anderen DC repliziert werden, damit ein unmittelbar nach dem Änderungsprozess erfolgender normaler Authentifizierungsprozess nicht fehl schlägt.

aufgeführt. Die Porteinteilung orientiert sich dabei an dem bei der Internet Assigned Numbers Authority (IANA) registrierten und zugewiesenen Portschema[19].

Tabelle 2.2: Netzwerkdienste eines AVD-Systems

Dienst	IP Protokoll	Port
Kerberos Authentifizierung	TCP / UDP	88
LDAP	TCP / UDP	389
LDAPS (SSL)	TCP	636
SMB (Netlogon & Sysvol)	TCP	445
DNS (optional)	TCP / UDP	53
LDAP Global Catalog (optional)	TCP	3268
LDAP Global Catalog (SSL)	TCP	3269
RPC Endpoint Mapper	TCP	135

Quelle: In Anlehnung an [Microsoft, 2020]

2.5 Sicherheitsmodelle und Identitätsmanagement

Im Informationssicherheitsbereich existieren verschiedene Sicherheitsstandards. Die Orientierung an Standards erleichtert den Daten- und Informationsaustausch zwischen Institutionen. Die wichtigsten werden hier kurz mit ihrer Zielgruppe bzw. ihrem Themenbereich aufgelistet:[20] [siehe Raab-Düsterhöft, 2018, S. 17ff]

- ISO Standards der Reihe ISO/IEC 2700x
  Die Standards zur Informationssicherheit der internationalen Normungsorganisation ISO befassen sich mit dem Aufbau eines Informationssicherheit Management Systems (ISMS).

- BSI-Standards
  Diese Standards bieten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen im Rahmen der Informationssicherheit. Die BSI-Standards der Reihe 200-X lösen seit 2017 die mittlerweile veralteten Standards der Reihe 100-X ab.

- Control Objectives for Information and related Technology (COBIT)
  Der COBIT Standard beschreibt Methoden zur Kontrolle von Risiken, die sich durch den IT-Einsatz zur Unterstützung geschäftsrelevanter Abläufe ergeben.

[19] Quelle: `https://www.iana.org`

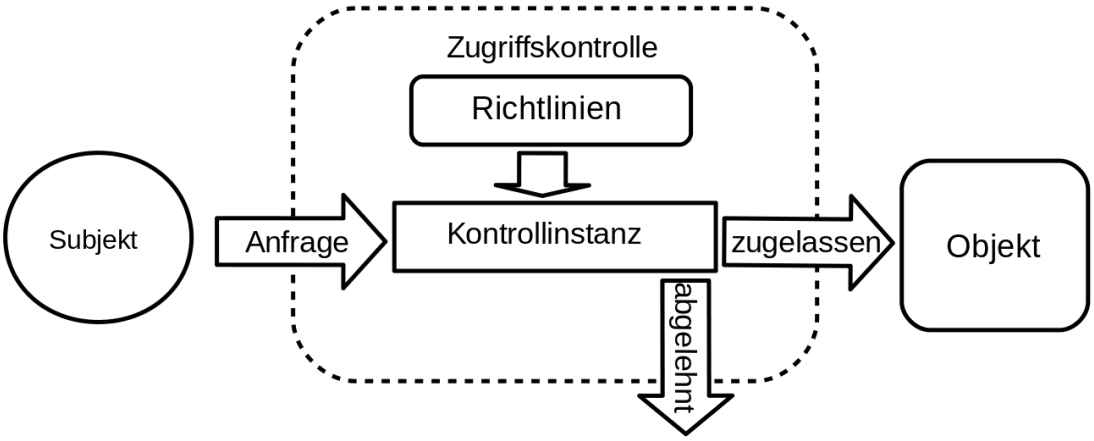
[20] Weiterführende Literatur zu den angegebenen Standards sind in den Literaturhinweisen zu den Standards gegeben.

- Information Technology Infrastructure Library (ITIL®)
  Die ITIL® ist eine Zusammenstellung von Büchern und Publikationen zum Thema IT-Service-Managements (ITSM). Inhalt sind Best-Practice-Vorschläge für Prozesse, wie sie in IT-Infrastrukturen mittlerer und großer Unternehmen vorkommen. [Cater-Steel et al., 2006; Bucksteeg et al., 2012; Cervone, 2008; Barafort et al., 2002]

2.5.1 Zugriffskontrollmodelle

Zur Überwachung und Steuerung des Zugriffs auf Daten und Ressourcen sind unterschiedliche Arten von Zugriffskontrollmechanismen verfügbar. Grundsätzlich dienen diese Kontrollinstanzen der Wahrung der Schutzziele Integrität und Vertraulichkeit von Informationen.

Prinzipiell beruht ein Zugriffsmodell darauf, dass Anfragen basierend auf den jeweils festgelegten Richtlinien entweder zugelassen oder abgelehnt werden, wie in Abbildung 2.13 dargestellt.



Quelle: In Anlehnung an [Edelkamp, 2016, S. 4]

Abbildung 2.13: Prinzip einer Zugriffskontrolle

Bei den zugrunde liegenden Zugriffskontrollmodellen werden folgende Arten unterschieden:

- Zugriffsmatrix-Modell (access matrix model)

  In diesem Modell wird der Zustand eines Systems durch eine Matrix modelliert. Das Modell ist auch als Referenzmonitor-Modell bekannt. [siehe Graham et al., 1972]

  Die Matrix ist definiert als $M_t :\mid \mathcal{S}_t \mid \times \mid \mathcal{O}_t \mid$, wobei gilt:

  - Die Spalten der Matrix werden durch die endliche Menge $\mathcal{O}_t$ der Objekte und
  - die Zeilen der Matrix werden durch die endliche Menge $\mathcal{S}_t$ der Subjekte zum Zeitpunkt t definiert.

    Subjekte können auch Objekte sein, d. h. es gilt $\mathcal{S}_t \subseteq \mathcal{O}_t$.
  - Es gilt: $M_t : \mathcal{S}_t \times \mathcal{O}_t \rightarrow 2^{RE}$ wobei RE die endliche Menge der Zugriffsrechte festlegt.

    Ein Eintrag $M_t(s,o) = \{re_1, \ldots, re_n\}$ beschreibt die Menge der Rechte, die das Subjekt s zum Zeitpunkt t an dem Objekt o besitzt.

  Für jeden Zeitpunkt t modelliert die Zugriffsmatrix M_t die in dem betreffenden Zustand gültigen Zugriffsrechte der Subjekte an den Objekten des Systems. [siehe Eckert, 2018, S. 244]

- Discretionary Access Control (DAC)

  Die Zugriffskontrollentscheidung basiert in diesem Modell direkt auf Subjekt s und Objekt o. Das Subjekt s kann die Zugriffsrechte re eines dedizierten Objektes o selbst festlegen. Die Sicherheitseigenschaften sind in diesem Fall objektbezogen. Fast alle Betriebssysteme unterstützen DAC. Zugriffsrechte auf Dateisysteme aber auch auf Netzwerklaufwerke werden basierend auf DAC geregelt.

- Mandatory Access Control (MAC)

  In diesem Modell existieren Sicherheitseigenschaften durch systembestimmte (regelbasierte) Festlegungen. Vom Subjekt s festgelegte Rechte werden von systemweiten Regeln dominiert und überschrieben.

- Role Based Access Control (RBAC)

  Im RBAC-Modell werden Rollen definiert, denen Rechte auf Objekte zugeordnet sind. Durch die Zuordnung des Subjekts s zu bestimmten Rollen erhält es letztendlich in diesem Modell Zugriff auf Objekte. Das Modell ist geeignet, sowohl MAC als auch DAC umzusetzen.

  In den in dieser Arbeit betrachteten Authentifizierungs- und Verzeichnisdienst-Systemen ist das RBAC-Modell Grundbestandteil der Zugriffskontrolle. Es wird daher im folgendem Abschnitt genauer beschrieben.

- Attribute Based Access Control (ABAC)

  Attribute, die sowohl Subjekt als auch Objekt besitzen, entscheiden in diesem Modell durch einen flexiblen Vergleich die Zugriffskontrollentscheidung.

Die aufgezählten Modelle sind geeignet den Zugriff auf Objekte zu regeln. Sie kontrollieren jedoch nicht, auf welche Art und Weise Informationen durch ein Subjekt verändert beziehungsweise weiterverarbeitet werden. Die Weiterverarbeitung wird in diesem Zusammenhang als Informationsfluss bezeichnet. Eckert schreibt hierzu, dass Informationsflüsse durch systembestimmende Strategien nur sehr restriktiv und nur auf einfache Weise festgelegt werden können. [siehe Eckert, 2018, S. 244] Das Bell-LaPadula-Modell ist ein Beispiel dafür, wie Informationsflüsse durch systembestimmende Regeln gesteuert werden können. Da es die Grundlage für das in Kapitel 4, Abschnitt 4.2 vorgestellte Schichtenmodell bildet, wird es weiter unten in diesem Abschnitt im Detail beschrieben.

RBAC-Modell

Die grundlegende Systematik der Berechtigungsvergabe durch Rollen und damit verbundene Problematiken, wie z. B. Funktionstrennungen, wurden bereits 1992 von Ferraiolo et al. in einem Bericht des National Institute of Standards and Technology (NIST) beschrieben. [siehe Ferraiolo et al., 1995] Ein RBAC-Rahmenwerk wurde 1996 von Sandhu entwickelt. [siehe Sandhu, 1996] Ausgehend davon hat das NIST im Jahr 2000 ein vereinheitlichtes Modell für RBAC vorgeschlagen, welches 2004 als Standard verabschiedet wurde. [siehe ANSI, 2004]
Eckert beschreibt das rollenbasierte Sicherheitsmodell durch einen Tupel wie folgt: [siehe Eckert, 2018, S. 253ff]

$$RBAC = (\mathcal{S}, \mathcal{O}, RL, \mathcal{P}, sr, pr, session) \tag{2.5}$$

Der Tupel setzt sich zusammen aus:

- $\mathcal{S}$: die endliche Menge der Benutzer des Systems,
- $\mathcal{O}$: die endliche Menge der zu schützenden Objekte,
- RL: die endliche Menge von Rollen,
- $\mathcal{P}$: die endliche Menge der Zugriffsberechtigungen und
- $sr, pr, session$: Relationen.

Jede Rolle beschreibt eine Aufgabe und damit die Berechtigung der Rollenmitglieder. Die Rolleneigenschaft eines Subjektes $s \in \mathcal{S}$ wird durch die Abbildung sr gemäß Darstellung 2.6 moduliert:

$$sr : \mathcal{S} \rightarrow 2^{RL} \tag{2.6}$$

Wenn gilt:

$$sr(s) = \{R_1, \ldots, R_n\} \tag{2.7}$$

dann ist das Subjekt s autorisiert in den Rollen $R_1, \ldots, R_n$ aktiv zu sein.

Über die Berechtigungsabbildung:

$$pr : RL \rightarrow 2^{\mathcal{P}} \tag{2.8}$$

wird jeder Rolle $R \in RL$ die Menge derjenigen Zugriffsrechte zugeordnet, die die Mitglieder der Rolle während ihrer Rollenaktivitäten wahrnehmen dürfen.

Die Relation:

$$session \subseteq \mathcal{S} \times 2^{RL} \tag{2.9}$$

beschreibt Paare (s, rl), die als Sitzung bezeichnet werden. Es muss gelten, $rl \subseteq sr(s)$.

Für ein Subjekt $s \in \mathcal{S}$ und für eine Sitzung $(s, rl) \in session$ gilt, dass s alle Berechtigungen der Rolle $R \in rl$ besitzt.
Wenn (s, rl) eine Sitzung ist, bedeutet es, dass s aktiv in den Rollen $R \in rl$ ist.

Weiterhin schreibt Eckert, dass ein Subjekt welches sich gleichzeitig in unterschiedlichen Sitzungen befindet, potenziell alle Berechtigungen aller Rollen besitzt, in denen es aktiv ist. Um Berechtigungen wahrzunehmen, muss ein Subjekt aktiv in einer Rolle sein, für die die Berechtigung erteilt wurde. [siehe Eckert, 2018, S. 254ff.]

Der zeitliche Zusammenhang zwischen aktivem Rollenbesitz und Benutzeranmeldung ist im Rahmen einer Kerberos Authentifizierung, wie sie in Abschnitt 2.4.1 beschrieben wurde und wie sie detailliert noch im Abschnitt 4.4 (Authentifizierungsabsicherung) dargestellt wird, ausgesprochen kritisch zu betrachten. Eine Rollenzuweisung erfolgt in der Regel zum Zeitpunkt der Anmeldung am System. Ein zu diesem Zeitpunkt erstelltes Kerberos TGT beinhaltet zu diesem Zweck Informationen über Gruppenmitgliedschaften. Diese Art von Anmeldung besitzt eine zeitlich begrenzte Gültigkeit. Wird im Laufe dieses Zeitraums, seitens des Kontrollsystems, eine Änderung an Mitgliedschaften vorgenommen, beispielsweise ein Rollenentzug durch Löschung einer Gruppenmitgliedschaft, wird dieser erst wirksam, wenn erneut eine Anmeldung erfolgt.

Edelkamp zieht zum Einsatz von RBAC folgendes Fazit: [siehe Edelkamp, 2016, S. 16]

- Rollenkonzepte sind sehr flexibel verwendbar und skalieren gut.
- Statische und dynamische Ausschlüsse von Rollen können modelliert werden.
- Direktes Nachbilden bekannter Organisations- und Rechtestrukturen in Unternehmen ist möglich.
- Rollenbasierte Zugriffskontrolle ist de-facto-Standard in Unternehmen und Unternehmenssoftware.
- Intuitive und relativ einfache Abbildung der Rollen auf Geschäftsprozesse (Workflows) im Prinzip möglich.
- Änderungen der Abbildung zwischen Rollen und Rechten sind selten.
- Änderung der Rollenmitgliedschaften sind häufig.

Bell-LaPadula-Modell

Nach Eckert gilt das 1973 entwickelte Bell-LaPadula-Modell [Bell et al., 1973] als das erste vollständig formalisierte Sicherheitsmodell, dem eine dynamische Zugriffsmatrix zugrunde liegt. [siehe Eckert, 2018, S. 265]
In dem Modell sind folgende Zugriffsrechte definiert:

- *read-only* erlaubt einen rein lesenden Zugriff,
- *append* befähigt Daten an ein bestehendes Objekt anzufügen,
- *execute* berechtigt zur Ausführung einer Datei,
- *read-write* erlaubt den lesenden und schreibenden Zugriff auf ein Objekt und
- *control* ermöglicht die Rechtemodifikation.

Die Zugriffsmatrix wird zudem um sogenannte Sicherheitsklassen *SC* erweitert, mit deren Hilfe den agierenden Subjekten unterschiedliche Vertrauensstufen zugeordnet werden können. Dabei wird ein Element $X \in SC$ durch ein Tupel (A,B) beschrieben, wobei A eine *Sicherheitsmarke* und B eine Menge von *Sicherheitskategorien* ist. Eckert beschreibt das Prinzip der Zugriffsbeschränkungen in diesem Modell mit der Einführung zweier Begriffe: [siehe Eckert, 2018, S. 265ff.]

1. Der Begriff der Sicherheitsklassen, auch *Clearance* genannt.
2. Der Begriff der Sicherheitsklassifikation, auch *Classification* genannt.

Die Menge aller Sicherheitsklassen und -klassifikationen bildet *SC*. Allen Subjekten s wird eine Sicherheitsklasse $sc(s) \in SC$, allen Objekten o eine Sicherheitsklassifikation $sc(o) \in SC$ zugeordnet. Dabei gilt, die Sicherheitsklasse $sc(s)$ ist die maximale

Sicherheitsstufe, die s einnehmen darf. Zum Zeitpunkt der Authentifizierung muss ein Subjekt seine aktuelle Sicherheitsklasse $sc_{\text{akt}}(s)$ angeben, wobei diese nicht die maximale Sicherheitsklasse überschreiten darf. Es gilt:

$$sc_{\text{akt}}(s) \leq sc(s) \tag{2.10}$$

Die Menge aller Sicherheitsklassen unterliegen einer partiellen Ordnung, $(SC, \leq)$, die antisymetrisch, transitiv und reflexiv ist.
Für alle $X, V \in SC$, mit $X = (A, B), Y = (A', B')$ gilt:

$$X \leq Y \Leftrightarrow A \leq A' \wedge B \subseteq B' \tag{2.11}$$

Weiterhin weist Eckert daraufhin, dass in diesem Modell zwei systembestimmte Regeln existieren [Eckert, 2018, S. 265ff.]:

1. Die *Simple-Security*, auch bekannt als *no-read-up Regel*.

   Mit dieser Regel ist definiert, dass ein Lese- oder Ausführungszugriff auf ein Objekt o durch ein Subjekt s nur dann zulässig ist, wenn s das entsprechende Zugriffsrecht r besitzt und die Objekt-Sicherheitsklasse kleiner oder gleich der Subjekt-Sicherheitsklassifikation ist. Nach dieser Regel gilt:

   $$r \in M_t(s, o) \wedge sc(s) \geq sc(o) \tag{2.12}$$

2. Die **-Eigenschaft*, auch bekannt als *no-write-down Regel*.

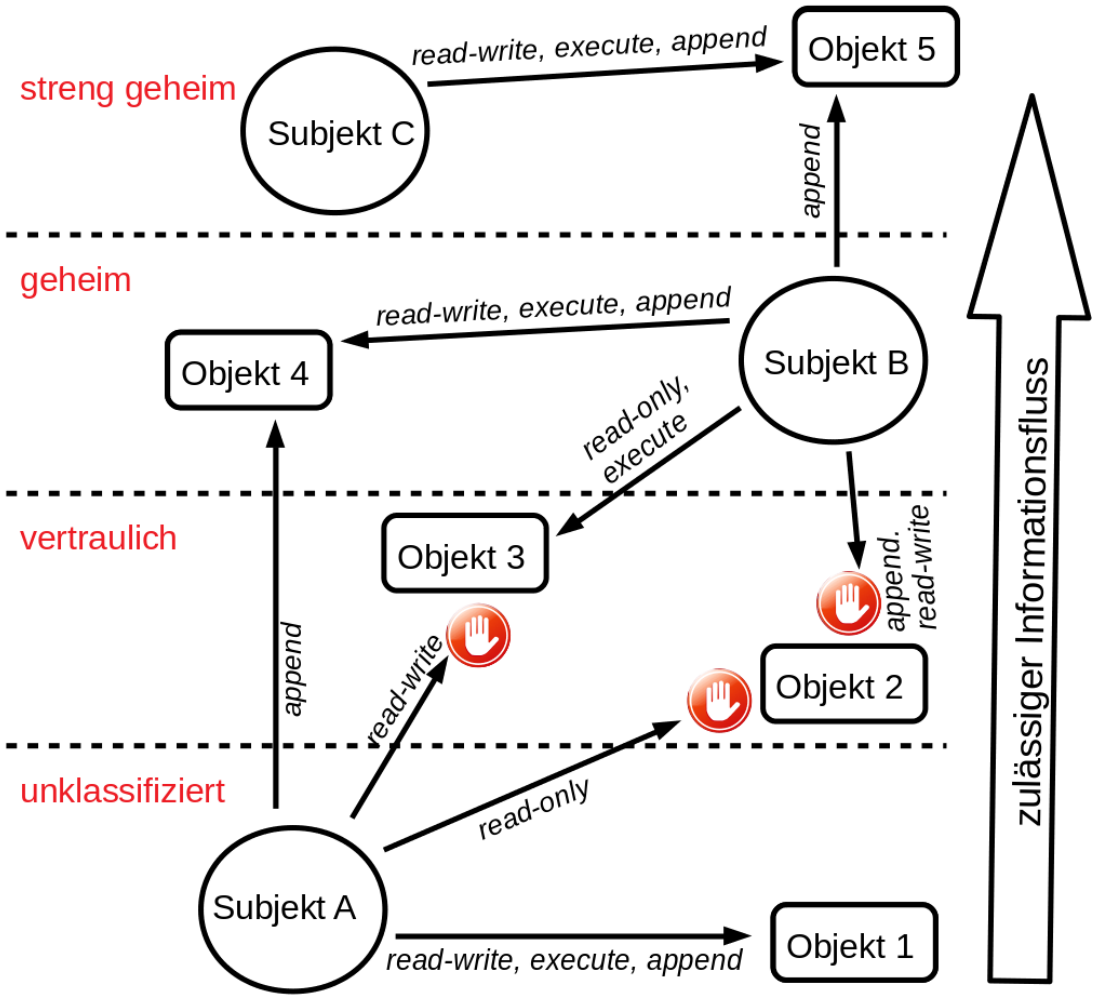
   Durch diese Eigenschaft ist definiert, dass ein Ausführungszugriff auf ein Objekt o durch ein Subjekt s nur zulässig ist, wenn die Objekt-Sicherheitsklasse mindestens so hoch ist, wie die Subjekts-Sicherheitsklassifikation. Es gilt:

   $$append \in M_t(s, o) \wedge sc(s) \leq sc(o) \tag{2.13}$$

   Gleichzeitig ist definiert, dass ein Lese-Schreib-Zugriff auf ein Objekt o nur zulässig ist, wenn die Objekt-Sicherheitsklasse gleich der Subjekts-Sicherheitsklassifikation ist. In diesem Fall gilt:

   $$read - write \in M_t(s, o) \wedge sc(s) = sc(o) \tag{2.14}$$

Diese beiden einfach zu überprüfenden Bedingungen gewährleisten, dass Informationsflüsse in diesem Modell nur von unten nach oben entlang der partiellen Ordnung, $(SC, \leq)$, oder innerhalb einer Sicherheitsklasse auftreten können.



Quelle: In Anlehnung an [Eckert, 2018, S. 267]

Abbildung 2.14: Beispielhaftes Bell-LaPadula-Sicherheitsmodell

In Abbildung 2.14 ist ein beispielhaftes Bell-LaPadula-Sicherheitsmodell mit den Sicherheitsklassen *unklassifiziert, vertraulich, geheim* und *streng geheim* dargestellt. Ein zulässiger Informationsfluss ist in diesem Beispiel nur von unten nach oben möglich und nicht umgekehrt.

Heute wird das Bell-LaPadula-Modell auch in Form der Multi-Level Security (MLS) eingesetzt. Es ist beispielsweise Teil von SE-Linux und der Solaris Trusted Extensions des Herstellers Oracle. Weiterhin bildet es die Basis für das in Abschnitt 4.2 vorgestellte Schichtenmodell.

2.5.2 Identitätsmanagement

Im Abschnitt 2.4 wurde der Begriff der Identität definiert und genauer betrachtet. In einem zentralen AVD-System werden eine Vielzahl von technischen Identitäten gespeichert, die meist auch einer physischen, personellen Identität zuzuordnen sind. Da es sich bei den Informationen, die für derartige Identitäten in der Datenbank des AVD-Systems gespeichert werden – wie z. B. Namen, E-Mail-Adresse – um personenbezogene Daten handelt, ist es, gerade in größeren Institutionen, angebracht, den Personen auch eine direkte Kontrolle über ihre Daten zu ermöglichen. Eine passende Schnittstelle hierzu bieten AVD-Systeme direkt meist nicht. Köhntopp definiert wie folgt: „*Identitätsmanagement* (genauer: Identitätenmanagement als das Management der möglichen verschiedenen Teilidentitäten) bedeutet, dass eine Person grundsätzlich wählen kann, was sie jeweils ihren Kommunikationspartnern über sich offenbart und in welcher Rolle sie auftritt.“ [Köhntopp, 2001, S. 56]

Um eine Vielzahl von Identitäten zentral zu verwalten werden spezielle Identitätsmanagementsysteme (IdM-Systeme) eingesetzt. Derartige Systeme speichern Informationen zu Identitäten in sogenannten Metaverzeichnissen und haben meist direkte Schnittstellen zu AVD-Systemen, aber auch zu weiteren Systemen, wie beispielsweise Personalverwaltung, Post- und Telefonsystemen sowie weiteren dedizierten Datenbanken einer Institution. Meist bieten diese Systeme auch eine direkte (Web-)Schnittstelle an, um Daten, die zur eigenen Identität gehören, durch die Person selbst pflegen zu lassen. Derartige Portale werden als Self-Service-Portal bezeichnet. Sie bieten z. B. die Möglichkeit, einen Kennwortrücksetzungsprozess eigenständig zu initiieren oder Kontaktdaten, wie Telefonnummer und Adresse selbstständig einzugeben. IdM-Systeme werden in der Regel als verteiltes System aufgebaut, wie in Abschnitt 2.2.1 beschrieben. Das auf Seite 14 in Abbildung 2.2 abgebildete System verdeutlicht die einzelnen Komponenten eines solchen Systems beispielhaft. Die dargestellten Verbindungen zu Zielsystemen, wie u. a. dem zentralen Verzeichnisdienst wird durch authentifizierte und verschlüsselte Datenkanäle realisiert. Dies ermöglicht einen automatisierten und schnellen Informationsfluss.

Im Rahmen der Sicherheitsbetrachtungen, die in dieser Arbeit angestrebt werden, sind IdM-Systeme als kritisch zu betrachten. Wie oben beschrieben, erfolgt die Kommunikation zu AVD-Systeme mittels Authentifizierung und durch Verschlüsselung abgesicherter Kanäle. Das dafür verwendete Dienstkonto hat im Verzeichnisdienst-Zielsystem mitunter erweiterte Berechtigungen, da es Schreibrechte auf das Verzeichnis benötigt. Ein Angreifer, der zuerst ein IdM-System kompromittiert, könnte über diesen Weg auch das AVD-System kompromittieren.

3 Advanced Persistent Thread (APT)

In dieser Arbeit wird eine sehr spezielle Art von Bedrohung für IT-Systeme betrachtet. Es geht um Angreifer, die vorrangig ein Ziel, meist genau eine Institution, im Focus ihres Angriffs haben. Oft wird dabei Schadsoftware verwendet, die primär für das ausgewählte Ziel entwickelt wurde. Die Angreifer lassen sich gewöhnlich viel Zeit, um das richtige Ziel anzugreifen und die gesuchten Daten zu stehlen oder zu manipulieren (Kompromittierung). Entsprechende lang andauernd im Verborgenen ablaufende Angriffe werden als Advanced Persistent Thread (APT) bezeichnet [siehe Chen et al., 2014, S. 65].
Steffens beschreibt die Entstehung des Begriffes wie folgt:

> „Die amerikanische Luftwaffe stand 2006 vor der Herausforderung, sich über Hackerangriffe gegen ihr Netzwerk mit zivilen Experten auszutauschen. Vermeiden wollten sie dabei, ihre Erkenntnisse über den Ursprung und die Täter preiszugeben. Gleichzeitig mussten sie den Experten aber vermitteln, dass es sich nicht um Allerweltsangriffe handelte. Deswegen bezeichneten sie sie als Advanced Persistent Thread (APT).“ [Steffens, 2018, S.5]

Weiterhin spricht Steffens davon [siehe Steffens, 2018, S. 6], dass eine ganze Reihe von APTs technisch deutlich weniger kompetent sind als beispielsweise die Entwicklung von Banking-Trojanern wie *Zeus* [siehe auch Kühner, 2012] und *Ursnif* [siehe auch Kono et al., 2018]. Die Herausforderung bestehe vielmehr darin, dass diese Angriffe im Vergleich zu kriminellen Aktivitäten deutlich seltener sind und daher weniger Gelegenheit bieten, entdeckt zu werden.

3.1 Ziele und Strategien des Angreifers

Kennzeichnend für einen APT-Angriff ist, dass die Angreifer versuchen, sich, nachdem sie Zugang zum Netzwerk des Opfers erhalten haben, dort so lange wie möglich unerkannt aufzuhalten. Daten werden dabei nicht auf einmal gestohlen, sondern es werden nach und nach die wesentlichen und wertvollen Informationen kompromittiert. [siehe Geschonneck, 2014, S. 15]

Motivation des Angreifers

Geschonneck unterscheidet folgende Grobklassifizierung für die Motive von Cyberkriminellen Angriffen: [siehe Geschonneck, 2014, S. 17]

- Soziale Motivation,
- technische Motivation,
- politische Motivation,
- finanzielle Motivation und
- staatlich-politische Motivation.

Die Darstellungen in dieser Arbeit konzentrieren sich dabei auf Angriffe, die den letzten drei Arten von Motivation zuzuordnen sind. Es geht dabei meist nicht um Einzeltäter, die aus sozialer Überzeugung handeln. Wie bereits in der Einleitung erwähnt, bedeuten APT-Angriffe meist ein Angriffsszenario über längere Zeit, mit teils sehr fortschrittlichen Werkzeugen, die in der Regel nicht von Einzeltätern, sondern von Tätergruppen ausgeführt werden. Es ist davon auszugehen, dass gerade staatlich-politisch motivierte Angriffe von sehr gut organisierten Einheiten durchgeführt werden. Die in Abbildung 3.3 dargestellten Angriffsphasen der Cyber-Kill-Chain werden vermutlich von darauf spezialisierten Teams durchgeführt. Allgemein ist davon auszugehen, dass derartige Angriffe wohl nur von staatlicher Seite oder von großen Unternehmen finanziert werden können, die sich dadurch politische und / oder wirtschaftliche Vorteile erhoffen.

In der Öffentlichkeit standen in den vergangenen Jahren oft politische Motive wie Wahlmanipulation im Fokus. Auch das Ausspähen von militärischen Informationen in Behörden oder Rüstungsbetrieben kann das Ziel solcher Attacken sein. In diesem Zusammenhang wird Greg Hoglund[1] wie folgt zitiert: „APT ist die von der chinesischen Regierung gesponserte E-Spionage, die das Land seit 20 Jahren betreibt, um ihren Wachstumskurs beizubehalten.“ [Bütler, 2011, S.32] Diese Definition beschreibt, auf überspitze Weise, wer hinter solch einer Art von Angriff stecken kann. Wenn in diesem Zusammenhang von Teams oder Hackergruppen gesprochen wird, sind damit mitunter nur virtuelle Zusammenschlüsse gemeint, die durchaus über Ländergrenzen hinweg existieren können [siehe Geschonneck, 2014, S. 18]. Da die Angriffe meist über Command and Control-Server (C&C-Host) ausgeführt werden, die möglichst versteckt, „in den entferntesten Ecken des Internets“ als Host betrieben werden, und die einzelnen Mitglieder einer Hackergruppen selbst über das Internet auf den C&C-Host zugreifen, ist der reale Standort eines Mitgliedes technisch nicht relevant. Dies erschwert eine Strafverfolgung in diesen Zusammenhang in besonderem Maße. Auf diese Art von Command and Control (C&C)-Hosts wird am Ende von Abschnitt 3.3 näher eingegangen.

[1] Gründer der Sicherheitsfirma HBGary, Tochteruntenehmen von Man Tech International und Lieferant von Sicherheitsoftware und -dienstleistungen der US-Regierung

Ziele des Angreifers

Per Definition geht man bei APT-Angriffen davon aus, dass sie ein konkretes Ziel verfolgen. Es gilt als wahrscheinlich, dass es dabei meist um Informationsbeschaffung geht. Die Entwicklung und der Einsatz des Stuxnet Trojaners [siehe auch Falliere et al., 2012] zeigt, dass aber auch – in diesem Fall staatlich-politisch motivierte – Sabotage ein Ziel sein kann. Bis dieses Ziel erreicht ist, versucht der Angreifer möglichst unentdeckt im Netzwerk des Opfers zu bleiben. Dabei kann es sich unter Umständen um Zeiträume von bis zu mehreren Jahren handeln.

APT-Angriffe zeichnen sich bei der Zielverfolgung durch den effektiven Einsatz teils sehr spezialisierter Werkzeuge aus, wie in den weiteren Unterabschnitten dieses Kapitels dargestellt. Dieser teils sehr kostenintensive Einsatz von Ressourcen bedingt, dass für den Angreifer ein entsprechender Nutzen der erhaltenen Informationen vorliegen muss. Geschonneck schreibt dazu: „Das Ziel der Angreifer kann sich oft ändern, abhängig von den Daten, die im Netzwerk des Opfers vorgefunden werden.“ [Geschonneck, 2014, S.15] Bütler schreibt zum Einsatz der Ressourcen: „APT-Angreifer sind hoch qualifiziert, haben eine tiefe Systemkenntnis über alle bekannten Systemschwachstellen und die verfügbaren Abwehrmaßnahmen. Nicht selten stehen Unternehmen oder sogar Staaten hinter den besonders trickreichen APT-Attacken.“ [Bütler, 2011, S.32] Von Vorteil für den Angreifer ist in jedem Fall, dass sich bestimmte IT-Strukturen in vielen Institutionen wiederfinden: Ab einer gewissen Größe ist der Einsatz von zentralen Authentifizierungs- und Verzeichnisdienstsystemen (AVD) fast unausweichlich. Bei Angriffen auf diese Systeme können Werkzeuge eingesetzt werden, die sich über Jahre hinweg bei bereits erfolgten Angriffen bewährt haben. Der wiederholte Einsatz von speziell entwickelten Angriffstechniken stellt andererseits aber auch eine Schwachstelle dar, anhand derer ein Angriff detektiert und abgewehrt werden kann, da sich Institutionen auf deren Einsatz einstellen und entsprechende Abwehrmaßnahmen durchführen können.

Strategien eines APT-Angriffs

Wie im vorherigen Abschnitt beschrieben, versuchen Angreifer im Rahmen eines APT-Angriffs möglichst lange unentdeckt zu bleiben, um ihre Ziele zu verfolgen. Daher verbieten sich aus Sicht des Angreifers alle Maßnahmen, die regulären Nutzern und Mitarbeitern auffallen oder gar zu Fehlern im System führen würden. Die im Rahmen dieser Arbeit vorgestellten Abwehrstrategien und -konzepte für zentrale AVD-Systeme beruhen auf der Annahme, dass Angreifer immer versuchen werden, Schwachstellen in der Funktionalität dieser Systeme auszunützen. Eine essenzielle Strategie, die Angreifer in diesem Zusammenhang anwenden, ist die Identitätsübernahme von Mitarbeitern

der Institution. Dies wird als Identitätsdiebstahl (Credential Theft) bezeichnet.

Der Brückenkopf im IT-Netzwerk einer Institution

Ein fundamentaler Schritt im Rahmen eines APT-Angriffes ist die Kompromittierung eines im IT-Netzwerk befindlichen Standard-Arbeitsplatz PCs. Dieser grundlegende Schritt eines APT-Angriffs erfolgt meist durch Einschleusen und erfolgreiche Installation eines Trojaners und wird als Erschließungsphase (Exploitation) bezeichnet. Auf die Methoden des Einschleusens soll in dieser Arbeit nicht im Detail eingegangen werden. Zu nennen sind folgende übliche Wege:

- Einschleusen mittels infizierter E-Mails, Anhänge wie PDF- oder Office-Dateien mit infektiösem Inhalt oder Makros,
- Vermittlung und Zugriff des Benutzers auf infizierte Webseiten, die entsprechenden Schadcode mittels des Internetbrowsers installieren,
- Kompromittierung mittels infizierter Datenträger (USB-Speicher), die an den Arbeitsplatz-PC angeschlossen werden.

Ist ein Arbeitsplatz-PC in der beschriebenen Form durch einen Trojaner kompromittiert, bildet er für den Angreifer den Brückenkopf im IT-Netzwerk der angegriffenen Institution. In dieser Phase sind normale Firewall-Systeme, die das interne Netzwerk der Institution vor Zugriffen aus dem Internet schützen sollen, in der Regel nutzlos, da ein Trojaner den Verbindungsaufbau zu seinem C&C-Host immer vom kompromitierten Arbeitsplatz PC aus initiiert. Dieser Netzwerkverkehr ist üblicherweise so getarnt,[2] dass er sich aus Sicht der Unternehmensfirewall wie normaler Internetverkehr des Arbeitsplatz-PCs darstellt. Lediglich eine eventuell verdächtige Internet-IP-Adresse des C&C-Hosts könnte in dieser Phase des APT-Angriffs auf eine verdächtige Kommunikation hinweisen. Gesteuert über den C&C-Host wird der Angreifer von diesem Brückenkopf[3] aus versuchen, sich weiter im Netzwerk zu bewegen. Dies hat zwei Gründe:

1. Ein normaler Arbeitsplatz-PC ist in der Regel nicht als permanenter Brückenkopf geeignet. Er wird – oder besser, sollte – am Ende der damit erledigten Tätigkeit des Mitarbeiters abgeschaltet werden und ist dann für weitere Schritte des Angreifers nicht verfügbar.
2. Der zuerst kompromittierte Arbeitsplatz-PC stellt meist nicht das eigentliche Ziel des Angreifers dar.

[2] Der Verkehr wird über übliche Protokolle und Ports, wie HTTP/HTTPS übermittelt.

[3] These: In größeren Institutionen – mit mehreren tausend Arbeitsstationen – ist davon auszugehen, dass in obiger Form kompromittierte Arbeitsstationen zur ständigen Bedrohungslage gehören.

Verbreitung im IT-Netzwerk der angegriffenen Institution

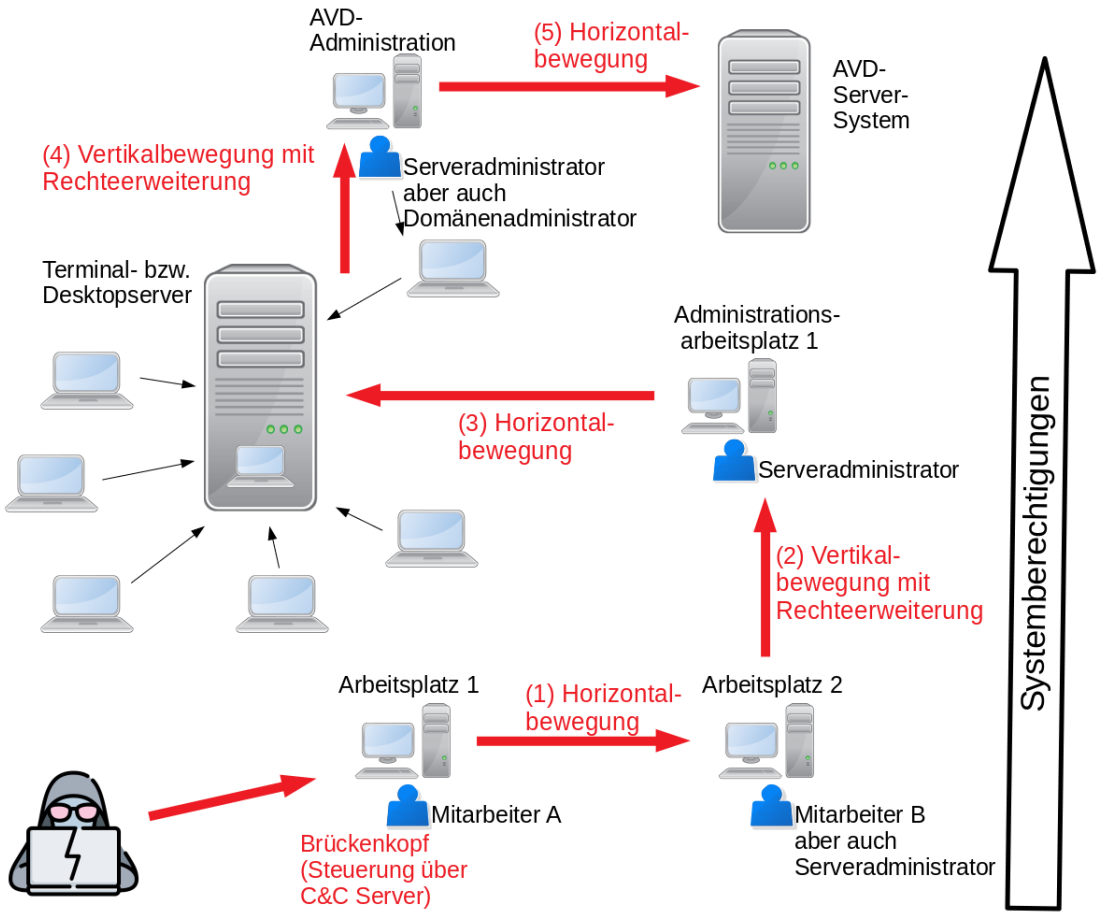
Die Schritte nach der Schaffung eines Brückenkopfes werden als Post-Exploitation-Phase bezeichnet. Mögliche Schritte des Angreifers sind in Tabelle 3.1 dargestellt.

Tabelle 3.1: Schritte der Post-Exploitation-Phase

Benennung	Englische Benennungen	Ziele des Angreifers
Aufklärung	Reconnaissance, Information Gathering, Situational Awareness, Enumeration	Informationssammlung
Steuerung	Command and Control, Code Execution	Einen oder mehrere übernommene Rechner fernsteuern
Persistenz	Persistence, Backdooring	Dauerhaften Zugriff sichern
Datendiebstahl	Credential Theft, Asset Discovery	Informationsdiebstahl oder -kompromittierung
Rechteerweiterung	Privilege Escalation	Zugang zu Identitäten mit weiteren Rechten
Ausbreitung	Lateral Movement, Pivoting, Network Colonization	Bewegung im IT-Netzwerk des Opfers
Spurenbeseitigung	Log Tampering	Spuren des Angriffs beseitigen
Systemstörung	System Disruption, Denial of Service	Funktionsstörungen an Systemen verursachen
Datenausschleusung	Data Exfiltration, Complete Mission	Gestohlene Daten aus dem internen Netzwerk kopieren

Quelle: oneconsult®, Cyber Security Experts

Die erste Bewegung weg vom Brückenkopf erfolgt in der Regel mit der Benutzer-Identität und den Berechtigungen des Benutzers, an dessen Arbeitsplatz sich der Trojaner eingeschleust hat. Dies wird in diesem Rahmen als Identitätsdiebstahl (Credential Theft) bezeichnet. Die Bewegung des Angreifers von Host zu Host, im Netzwerk des Opfers, wird als Seitwärtsbewegung (Lateral Movement) bezeichnet. Dabei wird in Vertikal- und Horizontalbewegungen unterschieden. Diese Schematisierung bezieht sich auf die möglichen Berechtigungen der Identitäten, die dem Angreifer zum Opfer



Quelle: Eigene Darstellung unter Verwendung von Ressourcen von Flaticon.com

Abbildung 3.1: Bewegungen des Angreifers im Netzwerk

fallen. Eine Horizontalbewegung beschreibt eine Kompromittierung einer weiteren Benutzeridentität, die innerhalb der gleichen Berechtigungsebene existiert, wie die bereits kompromittierte Identität. Ist es dem Angreifer bei seiner Bewegung möglich, eine Identität mit erweiterten Berechtigungen zu kompromittieren, spricht man von einer Vertikalbewegung, wie in Abbildung 3.1 dargestellt. Dieser Schritt wird als Rechte-Eskalation (Privilege Escalation) bezeichnet und kann von normalen Benutzerrechten über administrative Befugnisse auf dem lokalen Arbeitsplatz-PC bis hin zu netzwerkweiten Berechtigungen führen. Ein Angreifer wird versuchen, sich möglichst unbemerkt und schnell mittels Rechte-Eskalationen seinem eigentlichen Ziel zu nähern.

Grundsätzlich sind diese Bewegungen des Angreifers im Netzwerk des Opfers nur unter Ausnutzung netzwerkseitiger Schwachstellen der Host-Systeme oder durch Erlangung von Kennwortinformationen – beispielsweise Kennwörtern, die im Web-Browser zwischengespeichert werden – möglich. Dies kann an einem normalen Arbeitsplatz-PC möglich werden, wenn er von mehreren Mitarbeitern zu unterschiedlichen Zeiten genutzt wird, oder durch Kompromittierung eines Server- oder Terminalserver-

Host-Systems. Die in Abschnitt 3.3 vorgestellten Werkzeugsammlungen erlauben es aber auch, ein kompromittiertes System im Netzwerk des Opfers als Basis für einen Man-In-The-Middle-Angriff zu benutzen, um somit an weitere Identitäten zu gelangen. Diese Angriffsart, bei der sich der Angreifer in die reguläre Kommunikation, die zwischen zwei Host Systemen im Netzwerk des Opfers stattfindet, einschleust, wird in Abschnitt 3.4.1 näher beschrieben. Grundsätzlich wird der Angreifer versuchen, die Identitäten, deren Kennwörter oder Kennwort Hashes er ermitteln konnte, für eine weitere Bewegung im Netzwerk des Opfers zu benutzen. Dieser Angriffsvektor, genannt Pass-The-Hash wird in Abschnitt 3.4.2 näher beschrieben.

3.2 Kategorisierung

Grobauer et al. nennen drei typische Motivationen für eine Klassifizierung von IT-Sicherheitsvorfällen: [siehe Grobauer et al., 2016, S. 18]

1. Klassifikation [...] als Grundlage der Entscheidungsfindung,
2. Klassifikation [...] als standardisierte Überblickbeschreibung,
3. Klassifikation [...] zur Schaffung einer normalisierten Datenbasis über IT-Sicherheitsvorfälle.

Eine Klassifizierung von Cyberangriffen ist notwendig, um gezielte Abwehrstrategien entwickeln zu können. Im Laufe der Entwicklung der IT haben sich viele verschiedene Klassifizierungsschemata entwickelt, wie eCSIRT [siehe PRESECURE, 2002, App.C], VERIS [siehe Moreira et al., 2018] oder auch der Standard ISO27035-3 [siehe ISO, 2011]. Es würde den Rahmen dieser Arbeit sprengen, auf alle existierenden Modelle einzugehen. Die maßgeblichen Schemata, wie die CERT-Taxonomie und Structured Threat Information eXpression (STIX™) der MITRE Corporation[4] werden in den folgenden Abschnitten näher vorgestellt. Auch das IT-Sicherheitsgesetz verlangt die Meldung wesentlicher Vorfälle, welche zu Ausfällen oder Beeinträchtigungen von kritischen Infrastrukturen geführt haben oder hätten führen können. Es wird aber in diesem Zusammenhang kein international anerkanntes Schema zur Meldung von Vorfällen definiert. In der zugehörigen Verwaltungsvorschrift [siehe BMI, 2009] wird ein Schema empfohlen, das sich stark an den vorgestellten Schemata orientiert.

[4] Die MITRE Corporation ist eine Non-Profit-Organisation zum Betrieb von Forschungsinstitutionen im Auftrag der USA, die 1958 durch Abspaltung vom Massachusetts Institute of Technology (MIT) entstanden ist (https://www.mitre.org/). Seitdem ist sie an einer Vielzahl von kommerziellen Projekten – auch an geheimen Projekten – für zahlreiche Agenturen der US-Regierung beteiligt.

Grundsätzlich lassen sich heutige Angriffe in drei große Klassen einordnen: [siehe Jonas, 2019, S. 16]

1. Ungezielte Angriffe z. B. über Massenmails, mit denen Viren, Würmer und Trojaner versandt oder Phishing-Angriffe durchgeführt werden.
2. Gezielte Angriffe, z. B. zur Sabotage und Spionage, die auf bestimmte Institutionen gerichtet sind.
3. Skalpellartige Angriffe, z. B. Angriffe mit intensiver Vorbereitung und meist zerstörender Wirkung auf die Infrastruktur. [siehe auch Hubner, 2019, S. 48]

Die in dieser Arbeit betrachtete Form des APT-Angriffs zählt dabei zu den gezielten Angriffen, die aber auch durch einen vorbereitenden ungezielten Angriff durch beispielsweise Massenmails eingeleitet werden können.

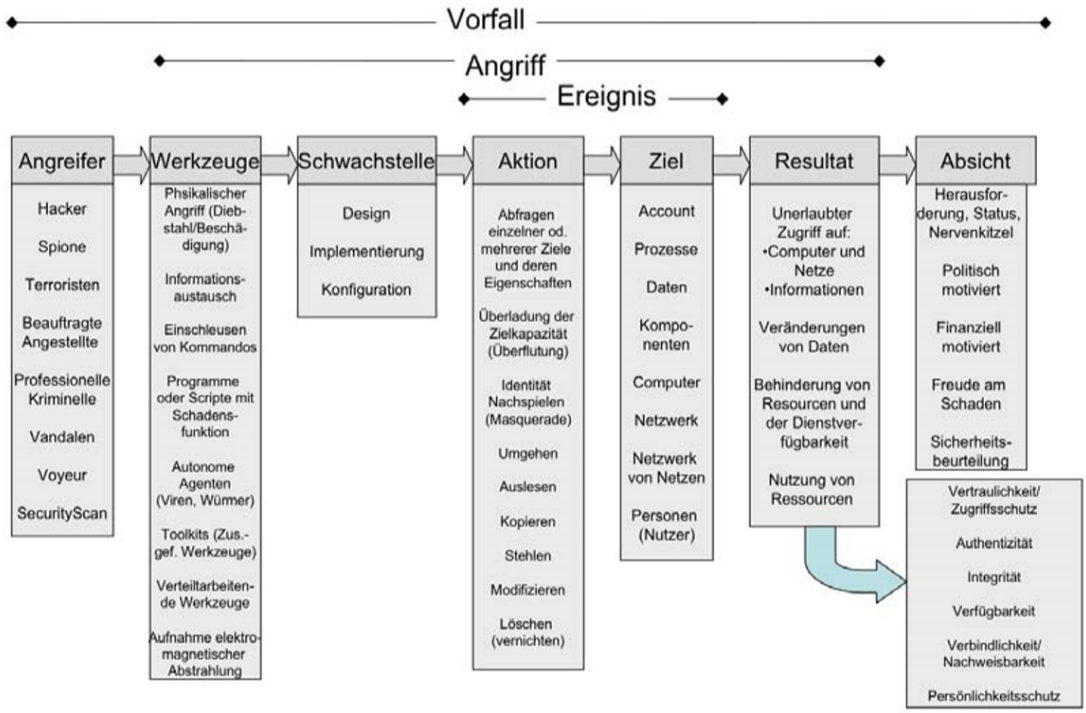
3.2.1 CERT-Taxonomie

Die wohl erste schematische Klassifikation derartige Vorgänge wurde von den Sandia National Laboratories 1998 als CERT-Taxonomie veröffentlicht. [siehe Howard et al., 1998] Bei der Erstellung des Schemas wurde dabei besonderer Wert darauf gelegt, möglichst jede Art von Sicherheitsvorfall erfassen zu können. Grundsätzlich werden dabei folgende Begriffe eingeführt:

- Systemveränderung (Event),
- Angriff (Attack) und
- Vorfall (Incident).

Eine aktualisierte und erweiterte Version ist in Abbildung 3.2 dargestellt. [siehe Kiltz et al., 2007]

Derart komplexe Angriffe auf Computersysteme und IT-Infrastrukturen lassen sich in ihrem Ablauf in mehrere Phasen einteilen. Die Phasen eines Angriffs ähneln sich. Das Wissen über diese Phasen ermöglicht es, zu erkennen, mit welchem weiteren Vorgehen des Angreifers zu rechnen ist.



Quelle: BSI Leitfaden IT-Forensik [BSI, 2011b, S.29]

Abbildung 3.2: Die erweiterte CERT-Taxonomie

Geschonneck nimmt dabei folgende Phaseneinteilung vor: [siehe Geschonneck, 2014, S. 33ff]

1. Footprinting,
2. Port- und Protokollscan,
3. Enumeration,
4. Exploiting / Penetration,
5. Hintertür einrichten und
6. Spuren verwischen.

Eine Präzisierung dieser Phaseneinteilung erfolgt durch die Entwicklung der *Cyber-Kill-Chain* wie im folgendem Abschnitt beschrieben.

3.2.2 Cyber-Kill-Chain

Die Cyber-Kill-Chain beruht auf dem Konzept der Kill-Chain, das erstmals von Lockheed Martin als militärisches Konzept vorgestellt wurde. Die Kill-Chain beschreibt eine Kette von Angriffsschritten, die letztendlich aus militärischer Sicht zur Eliminierung des Ziels führt.

Ein Angriffsszenario kann demnach in folgende Phasen aufgeteilt werden:

1. Standort des Ziels ermitteln (find),
2. genaue Beobachtung des Standorts (fix),
3. Verfolgung des anvisierten Ziels (track),
4. Auswahl der geigneten Waffe, um den gewünschten Effekt zu erzielen (target),
5. Waffen individuell auf das Ziel abstimmen (engage) und
6. Bewertung des Waffeneinsatzes gegenüber dem Ziel (assess).

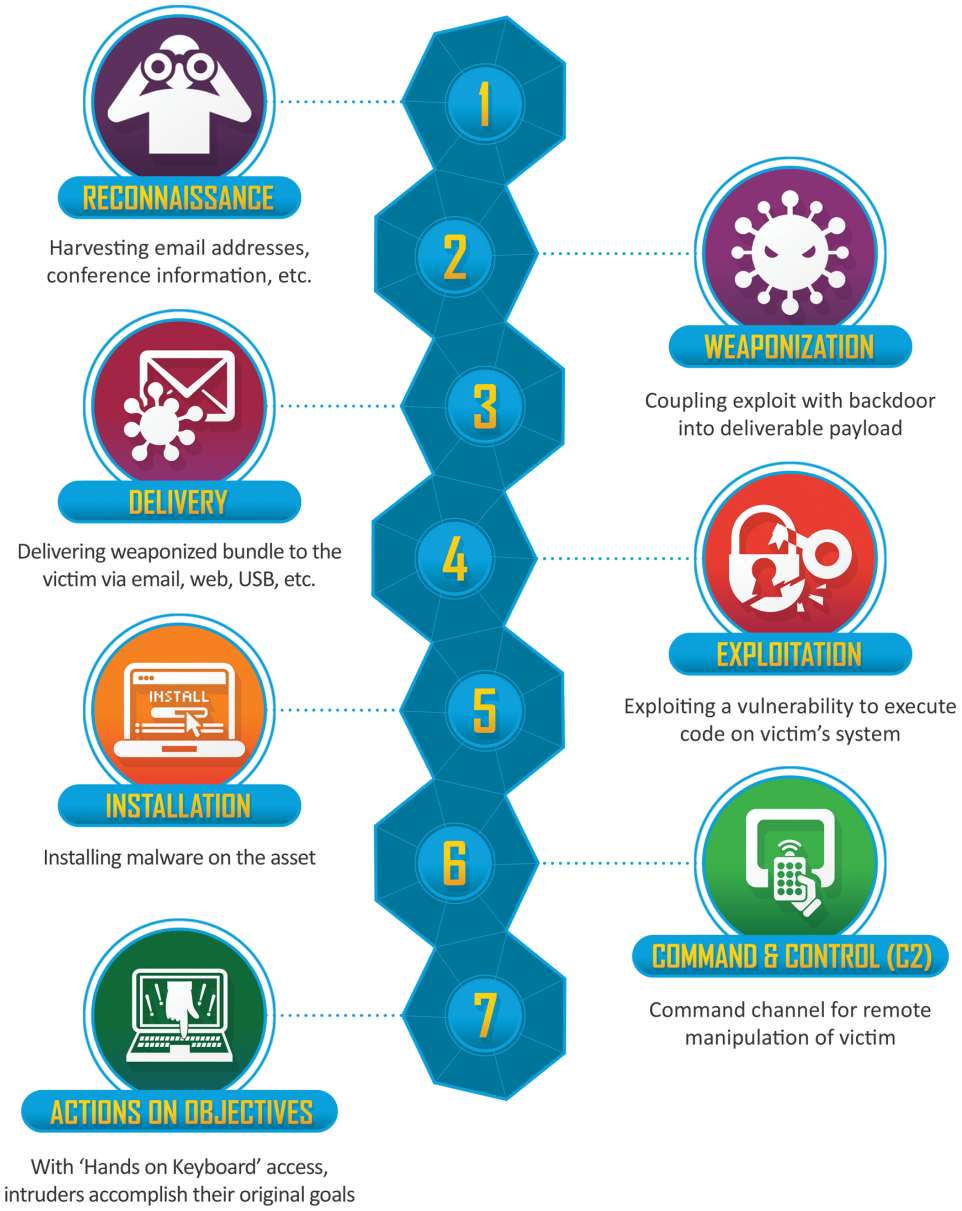
Dieser systematische Prozess (F2T2EA)[5] wird als Kette (chain) bezeichnet, da der Ausfall oder nicht erfolgreiche Abschluss einer Phase den gesamten Prozess unterbricht. [siehe Hutchins et al., 2011, S. 87ff] Im Jahr 2011 entschied sich Lockheed Martin dazu, diese ursprünglich für militärische Zwecke entwickelte Ablaufkette in leicht umgewandelter Form auch auf digitaler Ebene zu etablieren. Es entstand die Cyber-Kill-Chain, in der die Täter-Perspektive eingenommen wird und der Angriff in einzelne Angriffsstufen untergliedert wird. Die sieben Stufen des Cyber Attack Lifecycle, heute bekannt als die Cyber-Kill-Chain, sind in Abbildung 3.3 dargestellt. Die Anwendung der Cyber-Kill-Chain ermöglicht die stufenweise Identifizierung und Analyse hochkomplexer Angriffsstrukturen und gestattet dadurch, sich zielgerichtet vor APT-Angriffen zu schützen. Auch die in Abschnitt 3.2.3 auf Seite 61 beschriebene Wissensdatenbank MITRE ATT&CK™ richtet die forensischen Betrachtungen und Analysen anhand der Cyber-Kill-Chain aus.

Die einzelnen Schritte der Cyber-Kill-Chain werden im Folgenden kurz erläutert:

1. Identifizierung des Ziels (Reconnaissance)
   Die Reconnaissance oder auch bezeichnet als das Footprinting, stellt genaugenommen eine Vorstufe zum eigentlichen Angriff dar. Es werden dabei Informationen über das Angriffsziel gesammelt. Dazu zählen Informationen über die IT-Struktur, Ermittlung von IP-Adressen mittels Whois und DNS über das Kommando *nslookup* oder Erkundung der Netzarchitektur zum Beispiel mittels des Befehls *traceroute*.

2. Vorbereitung des Angriffs (Weaponization)
   Hierbei handelt es sich um eine Schwachstellen-Prüfung der im ersten Schritt ermittelten IT-Systeme, um damit das weitere Vorgehen zu bestimmen. Ergebnis ist eine Liste von IP-Adressen und Ports für die im Focus des Angreifers stehenden Systeme.

[5] Abkürzung gebildet aus den Anfangsbuchgstaben der englischen Begriffe



Quelle: Lockheed Martin

Abbildung 3.3: Darstellung der Cyber-Kill-Chain

3. Erste Schritte zur Durchführung des Angriffs entlang der Cyber-Kill-Chain (Delivery)
   Es werden Informationen über Anwendungen, Versionen, Patch Level und Betriebssysteme zu den im Fokus stehenden Host-Systemen ermittelt.

4. Systematisches Aufspüren und / oder Ausnutzen von Sicherheitslücken (Exploitation)
   Anschließend können gezielte Angriffe auf Anwendungssoftware und Betriebssystem erfolgen. Ermöglicht werden derartige Angriffe durch Ausnutzen bekannter Schwachstellen in der Programmierung, Konfiguration oder Implementierung der Systeme. Wird in dieser Phase des Angriffs ein Zero-Day-Exploit eingesetzt, das heißt, eine Schwachstelle ausgenutzt, für die es noch keine Gegenmaßnahme beziehungsweise noch kein Sicherheitspatch gibt, ist das ein Hinweis darauf, dass die Angreifer über umfangreiche Ressourcen und Geldmittel verfügen.

5. Implementierung einer Hintertür (Installation)
   Um sich den Zugriff auf die angegriffene IT-Infrastruktur dauerhaft zu sichern, auch nachdem die Sicherheitslücke, die zu dem Systemeinbruch genutzt wurde, geschlossen wird, richten sich Angreifer häufig eine Hintertür (englisch: Backdoor) ein. Dazu werden oft weitere versteckte Serverprozesse, sogenannte Rootkits oder zusätzliche Benutzerlogins mit erweiterten Berechtigungen eingerichtet.

6. Fernsteuerung des Zielsystems (Command and Control)
   Hat der Angreifer innerhalb der Institution Systeme kompromittiert, die sich ununterbrochen in Betrieb befinden (i. d. R. Serversysteme), wird er versuchen, diese als Command and Control (C&C) Systeme einzurichten. Er kann diese dann als permanentes „Sprungbrett“ nutzen, um sich weiter im Netzwerk des Opfers auszubreiten.

7. Zielerreichung (Actions on objective)
   Hat sich der Täter Zugriff auf das Zielsystem verschafft, erfolgt die eigentliche Angriffshandlung. Je nach Motivation des Täters reicht diese bei einem APT-Angriff von Datendiebstahl über Spionage bis hin zu Sabotage.

Zu 5:
Sobald eine Hintertür geschaffen wurde, wird ein Angreifer versuchen, die Spuren seiner Tätigkeiten zu verwischen. Dies erfolgt meist durch Manipulation von entsprechenden LOG-Dateien der kompromittierten Systeme.

Zu 7:
Es hat sich gezeigt, dass viele Angriffe, die aus Sicht des Angreifers erfolgreich abgeschlossen wurden, damit endeten, dass die betroffenen IT-Infrastrukturen letztendlich dauerhaft geschädigt wurden. Sobald der Angreifer sein Ziel erreicht hat, kann es passieren, dass er alle in seinem Zugriff stehenden Systeme löscht oder dauerhaft beschädigt, um beispielsweise seine Spuren zu beseitigen. Man spricht dann davon, dass der Angreifer „verbrannte Erde“ hinterlässt.

3.2.3 MITRE ATT&CK™

Die MITRE Corporation hat 2013 ATT&CK™ (Adversarial Tactics, Techniques & Common Knowledge) als systematische Kategorisierung von Angriffsverhaltensmustern eingeführt. MITRE verfügt über ein umfangreiches Cybersicherheitsteam, das vom US-amerikanischen National Institute of Standards and Technology (NIST) finanziert wird. Das MITRE ATT&CK™ Enterprise Framework ist eine ständig fortgeführte, öffentlich zugängliche Wissensbasis über cyberkriminelles Vorgehen, die auf forensischen Beobachtungen aus den vergangenen Jahren basiert. Diese Daten werden dabei in Tabellenform dargestellt und sind grob in zwei Hauptteile untergliedert.

Im ersten Teil geht es um die Taktiken und Techniken, die während eines laufenden Angriffs angewendet werden. Dabei wird als Taktik die Strategie bezeichnet, die einem Angriff zugrunde liegt. Als Technik werden die Ausführung und die Verwendung von bestimmten Werkzeugen bezeichnet, die ein Angreifer benutzt.

Der zweite Teil bezeichnet die allgemeine Wissensbasis (Common Knowledge) und gibt die bekannten Abläufe von Angriffen wieder. Ziel von MITRE ATT&CK™ ist es, eine umfassende Datenbank aller bekannten Taktiken und Techniken zu erstellen, die von Cyberkriminellen verwendet werden. Die daraus geschaffene Systematik erleichtert die Analyse eines laufenden Angriffs ebenso wie die Absicherung gegen zukünftige Angriffe. Durch die fortlaufende Analyse aktuell durchgeführter Angriffe und damit verbundener spezieller Verhaltensmuster von Angreifern gelingt ATT&CK™ auch eine Zuordnung zu bestimmten Angreifern. In Abbildung 3.4 wird die Hackergruppe APT28 beispielhaft mit Querverweisen auf die von dieser Gruppe verwendeten Techniken und Werkzeuge dargestellt. Die Kategorisierung der von Angreifern angewendeten Techniken erfolgt in Anlehnung an die in Abschnitt 3.2.2 vorgestellte Cyber-Kill-Chain in folgender Form:

1. Erster Zugriff (Initial Access),
2. Ausführungsart des Angriffs (Execution),
3. fortlaufende Implementierung (Persistence),

4. Rechteerweiterung (Privilege Escalation),
5. Abwehrsystemen ausweichen (Defense Evasion),
6. Benutzerzugriff (Credential Access),
7. Untersuchung der IT-Struktur (Discovery),
8. Seitwärtsbewegung in der IT-Struktur (Lateral Movement),
9. Sammlung von Daten (Collection),
10. Datendiebstahl (Exfiltration) und
11. Kommandosteuerung (Command and Control).

Insbesondere die Techniken zur Rechteerweiterung (4), zum Benutzerzugriff (6) und zur Seitwärtsbewegung (8) sind in dieser Arbeit relevant. Speziell hierzu werden in den folgenden Kapiteln Gegenmaßnahmen vorgestellt.

Example Group: APT28

Description:	**APT28** is a threat group that has been attributed to the Russian government.[1 2 3 4] This group reportedly compromised the Democratic National Committee in April 2016.[5]	
Aliases:	Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127 [1 2 3 4 5 6 7]	
Techniques:	• Data Obfuscation [1] • Connection Proxy [1 8] • Standard Application Layer Protocol [1] • Remote File Copy [8 9] • Rundll32 [8 9]	• Indicator Removal on Host [5] • Timestomp [5] • Credential Dumping [10] • Screen Capture [10 11] • Bootkit [7] *and more...*
Software:	CHOPSTICK, JHUHUGIT, ADVSTORESHELL, XTunnel, Mimikatz, HIDEDRV, USBStealer, CORESHELL, OLDBAIT, XAgentOSX, Komplex, Responder, Forfiles, Winexe, certutil [1 3 6]	
References:	1. FireEye. (2015). APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. Retrieved August 19, 2015. ...	

Quelle: MITRE ATT&CK™

Abbildung 3.4: Angaben zur Hackergruppe APT28 in der MITRE ATT&CK™ Datenbank

Um die MITRE ATT&CK™ Wissensbasis komfortabel nutzen zu können, ist ein ATT&CK™ Navigator als Open-Source verfügbar.[6] Er ermöglicht eine einfache grafische Darstellung der Beziehungen zwischen den einzelnen Objekten der Wissensdatenbank und eine benutzerspezifische Darstellung unterschiedlicher grafischer Ebenen (Layers). So ist es zum Beispiel möglich, Taktiken und Techniken verschiedener Hacker-Gruppierungen miteinander zu vergleichen.

[6]Quelle `https://github.com/mitre-attack/attack-navigator`

3.3 Instrumente und Werkzeuge des Angreifers

Die nachfolgend vorgestellten Werkzeuge stellen nur eine Auswahl der für Angreifer aktuell verfügbaren und gleichzeitig öffentlich bekannten Tools dar. Viele dieser Werkzeuge werden im Rahmen von quelloffenen Projekten im Internet entwickelt und fortgeführt, um bewusst Schwachstellen zu suchen. Auch im Bereich der Schwachstellenanalyse (Penetrationstest) werden diese Tools verwendet. Sie sind in diesem Bereich als Werkzeuge des Angreifers klassifiziert und somit meist den Red-Teams[7] zugeordnet.

MS Windows PowerShell, zugleich Angriffsziel und Werkzeug

Da es sich bei dem weitaus größten Teil der angegriffenen Systeme um Windows-artige Betriebssysteme handelt, konzentrieren sich auch die Werkzeuge auf diese Betriebssystemplattformgruppe. Im speziellen Fokus steht hierbei das, vom Hersteller Microsoft Corporation (MS) als legitimes Administrationswerkzeug gedachte, Automatisierungs- und Konfigurationsmanagement-Framework, die sogenannte MS Windows PowerShell. Durch ihre enge Einbindung in das MS Betriebssystem Windows bietet es sich für Angreifer an, die Windows PowerShell Funktionalität für Angriffe zu nutzen. Für Angreifer entfällt damit meist die Notwendigkeit, einen eigenen binären Schadcode auf den angegriffenen Systemen zur Ausführung zu bringen. Eine Erkennung des Angriffs wird dadurch erschwert. Seit 2009 ist die PowerShell fester Bestandteil jeder MS-Windows-Installation. Dieses Framework bietet in einer Grundinstallation bereits hunderte von Befehlen – in diesem Zusammenhang von MS als Commandlet (abgekürzt: Cmdlet) bezeichnet – welche über das .NET Framework Zugriff auf Systemfunktionen bieten. Im Rahmen der Post-Exploitation-Phase bietet der Einsatz von Windows PowerShell dem Angreifer folgende Vorteile:

- Einfacher Zugriff auf Netzwerk Sockets,
- einfaches Interface zur MS Windows Management Instrumentation (WMI),
- direkter Zugriff auf das Win32 Application Programming Interface (API),
- eine Laufzeitumgebung für PowerShell Skripte und
- ein einfacher Zugang zu kryptographischen Bibliotheken des Zielsystems.

[7] Im Bereich der Schwachstellenanalyse werden die beiden Parteien als Red-Team (Angreifer) und als Blue-Team (Verteidiger) bezeichnet.

PowerShell Empire

Die Werkzeugsammlung PowerShell Empire[8] ist ein auf Linux basierendes Post-Exploitation-Framework, dessen Einsatz auf dem Zielsystem nur sehr geringe Spuren (Footprint) hinterlässt. Da es auf einem Agenten basiert, kommt es ohne einen direkten Aufruf der PowerShell auf dem Zielsystem aus, der von einem Intrusion Detection System detektiert werden könnte. Der Einsatz des Toolkits bleibt aufgrund seiner agentenbasierten Arbeitsweise und des geringen Entwicklungsalters – es wurde 2016 auf der HackMiami vorgestellt – noch von vielen IDS-Systemen unentdeckt. Die Kommunikation mit dem Agenten erfolgt dabei über einen verschlüsselten Kommandokanal. Mit dem PowerShell Empire Toolkit sind folgende Angriffsschritte durchführbar:

- Systemerkundung (Host Reconnaissance),
- Rechteerweiterung (Privilege Escalation) und
- Querbewegung (Lateral Movement)

Das Toolkit unterscheidet dabei folgende Komponenten:

- Der Agent ist der Programmteil, der im Rahmen des Angriffs auf dem angegriffenen Host aktiv installiert ist. Er wird im Rahmen der Kompromittierung installiert.
- Der Listener ist der Prozess auf dem C&C-Host des Angreifers, der auf die Verbindung des Agenten auf den kompromittierten Host wartet.
- Der Stager ist ein Programmcode, der durch den Agenten auf dem angegriffenen Host ausgeführt wird und mit dessen Hilfe direkte Kommandos und Skripte auf dem anzugreifenden Host ausgeführt werden können.

Meist wird PowerShell Empire auf Systemen installiert, die auf Kali-Linux basieren. Das können auch kleine, handliche und preiswerte Raspberry Pi Systeme sein.

Nishang

Das Toolkit Nishang[9] ist, ebenso wie PowerShell Empire, eine Sammlung von Skripten, die speziell für Penetration Tester im Red-Team-Bereich entwickelt wurden. Im Gegensatz zum PowerShell Empire Toolkit basiert das Nishang Toolkit aber selbst auf MS Windows PowerShell und wird daher auf Windows-basierten Systemen eingesetzt. Das Toolkit wurde von Nikhil Mittal entwickelt[10] und wird vorzugsweise für die Angriffsphasen *Reconnaissance* und *Privilege Escalation* verwendet.

[8] Quelle: `https://www.powershellempire.com/`
und `https://github.com/EmpireProject/Empire`
[9] Quelle: `https://github.com/samratashok/nishang`
[10] Quelle: `http://www.labofapenetrationtester.com/`

Die verschiedenen Skripte werden im Toolkit in folgende Kategorien unterteilt:

- ActiveDirectory
- Antak-WebShell
- Backdoors
- Bypass
- Client
- Escalation
- Execution
- Gather
- MITM
- Misc
- Pivot
- Prasadhak
- Scan
- Shells
- Utility
- powerpreter

In jeder dieser Kategorien sind zahlreiche Skripte vorhanden, die Angreifern in der Post-Exploitation-Phase nützlich sein können. [siehe Diathesopoulos, 2017, S. 28ff] Das Nishang Toolkit benötigt zur Ausführung eine *PowerShell RemoteShell*[11] auf dem Host-System des Opfers. Die Ausführung der Skripte wird mittlerweile durch zahlreiche Anti-Virus- und Anti-Malware-Systeme erkannt und mitunter blockiert. Die Skript-Sammlung gehört mittlerweile zum Standardumfang einer Kali-Linux Installation.

PowerSploit

Das PowerSploit Framework[12] von Matt Graeber [siehe Graeber, 2012] basiert auf dem zuvor von ihm vorgestellten PowerSyringe und wurde erstmals im Mai 2012 vorgestellt. [siehe Graeber, 2011] In den folgenden Jahren wurde es von Graeber, Bialek, Campbell und Weiteren im Rahmen eines Open Source Projektes weiterentwickelt. Mit diesem Framework sind Angriffe unter anderem in folgenden Phasen des APT-Angriffes möglich: [siehe Kazanciyan et al., 2014, S. 2ff]

- Reconnaissance
- Code Execution
- Persistence
- Anti-Virus Bypass

Auch das weiter hinten vorgestellte Tool Mimikatz ist in diesem Framework enthalten.

BloodHound

Das Programm *BloodHound*[13] bildet für den Angreifer ein entscheidendes Werkzeug in der Erkundungsphase. Mit ihm ist es möglich, die IT-Struktur des Angriffsziels zu erkunden und detailliert grafisch zu dokumentieren.

[11] Windows PowerShell-Remoting muss vom angegriffenen System unterstützt werden. Dies ist in einer zentralen Clientadministrationsumgebung, gerade bei größeren Institutionen, jedoch oft der Fall. Auf dezentralen Windows Clients wird oft die Remoteverwaltung aktiviert und konfiguriert.

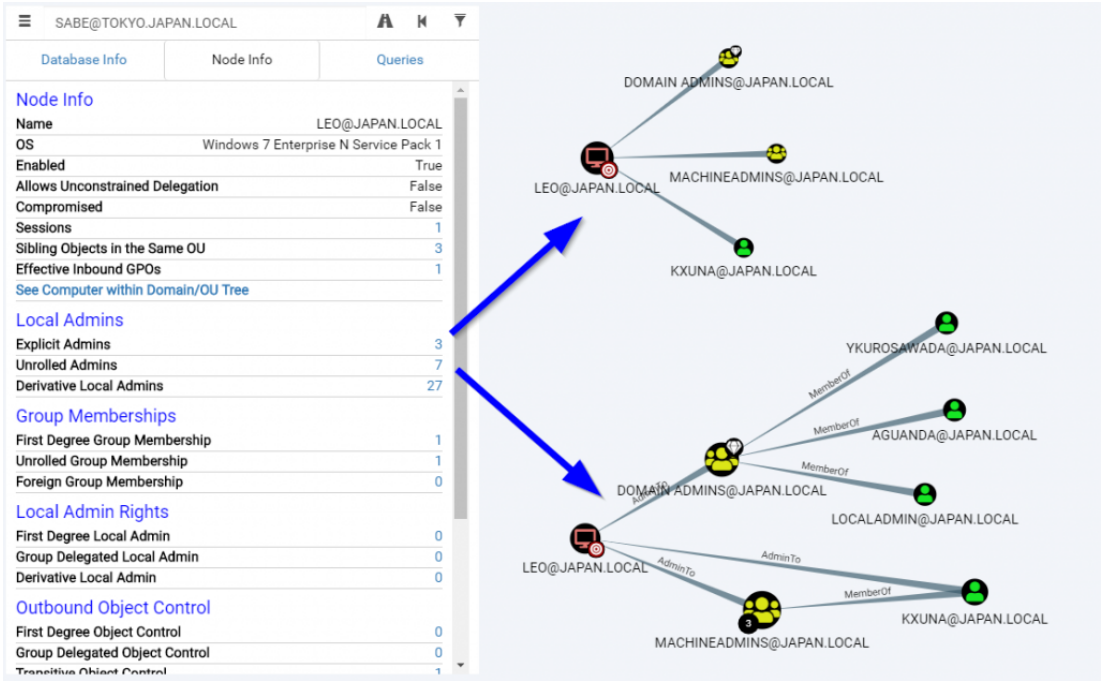
[12] Quelle: `https://github.com/mattifestation/PowerSploit`

[13] Quelle: `https://github.com/BloodHoundAD/BloodHound`

Um die nächsten Angriffsschritte zu planen, ist es für einen Angreifer von großer Bedeutung folgende Fragen zu klären:

- Welcher Benutzer ist in welchen Gruppen?
- Welche Rechte ergeben sich aus den Gruppenzugehörigkeiten?
- Welcher Benutzer ist an welchen Systemen angemeldet?
- Welche weiteren Benutzer sind bzw. waren an diesen Systemen angemeldet?

Die Daten hierzu werden meist in Form eines Verzeichnisses in dem bereits beschriebenen AVD-System der Institution zentral gespeichert. Die Anfragen an den Verzeichnisdienst erfolgen meist mittels Lightweight Directory Access Protocol (LDAP) und werden mit einem PowerShell Commandlet gestartet. Eine Auswertung der vom Verzeichnisdienst bereitgestellten Daten macht es dem Angreifer möglich, seine nächsten Schritte zu planen.



Quelle: Compass-Security Blog

Abbildung 3.5: Grafische Analyse mit BloodHound

BloodHound ist ein speziell entwickeltes webbasiertes Programm, um die oftmals nicht direkt erkennbaren Abhängigkeiten von Benutzern und den zugeordneten Benutzerrechten darzustellen. In diesem Zusammenhang wird oft von *versteckten* Rechten gesprochen, da eine Rechtezuordnung, die über eine Verkettung von Gruppenzugehörigkeiten entsteht, nicht unmittelbar ersichtlich ist. Das Programm wurde ab 2016 basierend auf der Arbeit von Robbins et al. entwickelt. [siehe Robbins et al., 2018] Die grafische Darstellung von Rechtebeziehung zur Ermittlung von Querbewegungen

wird auch von Powell behandelt. [siehe Powell, 2019] Die Erkundung mittels des Programms *BloodHound* erfolgt in zwei Schritten:

1. Ermittlung der benötigten Daten mittels PowerShell Kommando *Get-BloodHoundData*. Die gefundenen Daten werden dabei in einer Datei mit CSV-Format gespeichert.
2. Import der CSV-Daten in ein webbasiertes Programm zur grafischen Darstellung und Analyse.

Das Ergebnis ist eine grafische Darstellung der Benutzer-, Gruppen- und Rechtebeziehungen. Der Angreifer kann damit weitere Analysen durchführen, wie beispielsweise eine Shortest-Path Analyse zu einem Benutzer mit Domänenadministrator-Rechten. Eine beispielhafte Darstellung einer Suche nach Benutzern mit lokalen Administratorrechten für einen Computer *LEO@JAPAN.LOCAL* ist in Abbildung 3.5 dargestellt.

Mimikatz

Das Programm Mimikatz ist wohl das meist benutzte Hacker-Tool des letzten Jahrzehnts. Es wurde von Benjamin Delphy ab 2014 entwickelt, ursprünglich als Übung um sich selbst Programmierkenntnisse in der Programmiersprache C anzueignen. Das Tool nutzt eine Schwachstelle in MS Betriebssystemen der Windows-Familie aus, mit der es unter administrativen Berechtigungen im Debug-Mode möglich ist, an alle zwischengespeicherten Anmeldedaten von aktuell laufenden Sitzungen zu gelangen. Die Software kann von GitHub im Quellcode[14] und in einer frei verfügbaren 32- und 64-Bit Version bezogen werden. Die Software wird nicht nur von Hackern, sondern auch von Sicherheitsexperten im Rahmen von Penetrationstests eingesetzt. Viele Anti-Viren-Systeme detektieren den Start des Programms und verhindern dann dessen Ausführung. Benjamin Delphy hat durch die Programmierung dieses Programms demonstriert, wie einfach es für Angreifer ist, an zwischengespeicherte Anmeldeinformationen auf einem Betriebssystem der Windows-Familie zu kommen. Mithilfe des Programms sind folgende Angriffsvarianten durchführbar, die im Abschnitt 3.4.2 näher erläutert werden:

- Pass-the-Hash
- Pass-the-Ticket
- Over-Pass-the-Hash (Pass-the-Key)
- Kerberos Golden-Ticket
- Kerberos Silver-Ticket
- Pass-the-Cache

Mimikatz basiert auf einer interaktiven Konsole. Um den vollen Funktionsumfang und damit auch den Zugriff auf Anmeldedaten laufender Sitzungen zu erhalten, ist ein Start des Programms mit lokalen Administratorrechten notwendig.

[14] Quelle: `https://github.com/gentilkiwi/mimikatz`

Kontrollserver

Der Kontrollserver (Command and Control Server, C&C-Server) bildet einen zentralen Knoten, von dem aus Angriffe gestartet und koordiniert werden. Der Angreifer selbst greift nur via Remote Verbindung auf den Kontrollserver zu. Der eigentliche Aufenthaltsort des Angreifers wird durch den Kontrollserver verschleiert. Steffens schreibt dazu: [siehe Steffens, 2018, S. 57ff.]

> „Für Täter sind Kontrollserver von immenser Bedeutung. Sie dienen einerseits als Verteidigungswall gegen Analysten und Sicherheitsfirmen, in dem sie eine oder mehrere Anonymisierungsschichten zwischen den Opfern und den Rechnern der Angreifer bilden. Andererseits sind sie oft die einzige Verbindung, um den Zugriff auf bereits kompromittierte Netzwerke zu behalten. Daher ist die Pflege und Verwaltung der C&C-Server ein fester Bestandteil der Aufgaben jeder Tätergruppe. [...] Man kann davon ausgehen, dass es dedizierte Gruppen-Mitglieder gibt, die sich um die Serverinfrastruktur kümmern. Für Angriffe werden Server auf unterschiedlichste Art verwendet. Sie können genutzt werden, um Exploits zu hinterlegen, [...] Angriffsmails können von ihnen verschickt werden. Das Scannen nach verwundbaren Rechnern benötigt Server als Plattform. [...] Die Täter nutzen sie, um gestohlene Daten zwischenzulagern. Und schließlich werden sie gebraucht, um Befehle an Backdoors zu übermitteln."

Steffens schreibt weiterhin, dass die Angreifer derartige Server entweder selbst anmieten oder versuchen, legitime Server, von an der eigentlichen Aktion nicht Beteiligten, zu kompromittieren. Letztere Variante hat den Vorteil, dass ein Angriff nur bis zu dem kompromittierten Server zurückverfolgt werden kann und damit die eigene Identität verschleiert wird.

3.4 Angriffsvektoren im internen Netz

In diesem Abschnitt werden ausgewählte Angriffsvektoren dargestellt, die speziell auf die Kompromittierung von AVD-Systemen zielen. Diese Vektoren sind für den Angreifer im Rahmen der Post-Exploitation-Phase von Relevanz. Sie verdeutlichen im besonderen Maße die Notwendigkeit, ein AVD-System und deren Administrationsumgebung (HSA) gegenüber den restlichen IT-Systemen abzugrenzen und zu schützen.

3.4.1 Man-In-The-Middle-Angriff (MITM)

Ein erster Schritt des Angreifers weg von seinem Brückenkopf, wie in Abschnitt 3.1 beschrieben, ist die Ermittlung weiterer Identitäten, die zu einer Querbewegung in-

nerhalb der Institution führen können. Im internen Netzwerk einer Institution werden ständig Authentifizierungsvorgänge zwischen den zuständigen AVD-Servern und einer Vielzahl von Client-Systemen durchgeführt. Der Angreifer wird versuchen, diese Prozesse netzwerk- und systemseitig zu benutzen, um für sich weitere Identitäten zu erschließen.

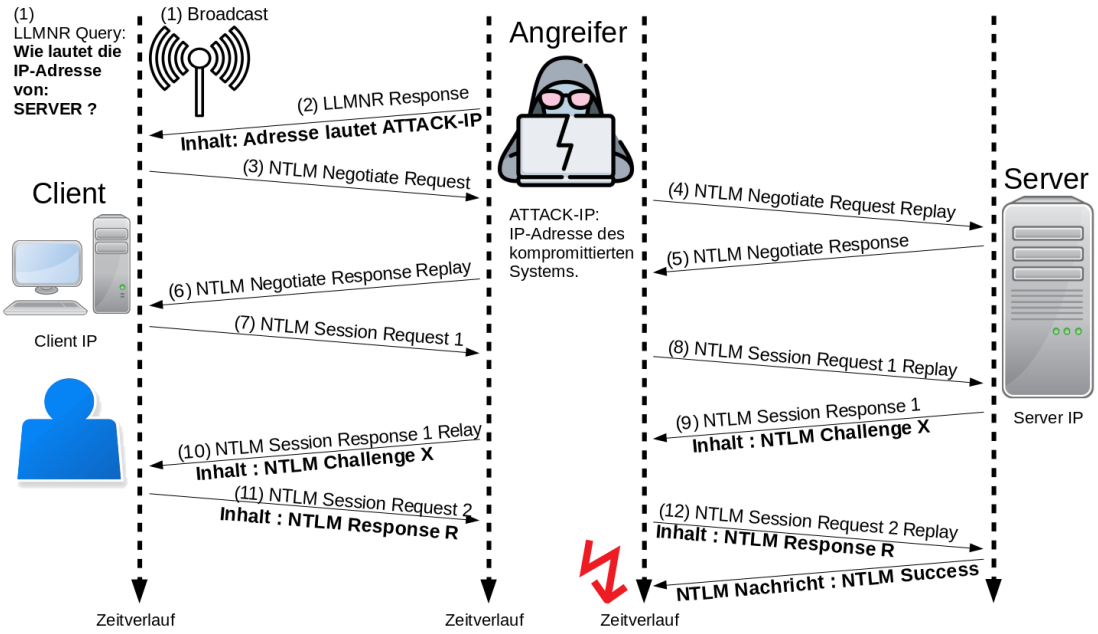
Wie in Abschnitt 2.4.1 beschrieben, werden in heutigen Authentifizierungssystemen, die auf Benutzernamen und Kennwort basieren, nicht mehr die Kennwörter selbst gespeichert und genutzt, sondern ein über eine Einwegfunktion berechneter Hashwert dieser Kennwörter. Diese Maßnahme verhindert zwar den Diebstahl der Kennwörter direkt aus den Kennwort-Datenbanken. Auch werden die Kennwörter dadurch nicht mehr direkt über das Netzwerk übertragen. Da aber bei einigen Authentifizierungsverfahren der Hash eines Kennwortes ohne weitere Informationszugabe – beispielsweise durch Verknüpfung mit einem Salt[15] – behandelt wird, ist er als Kennwort-Äquivalent zu betrachten. Er kann zur Authentifizierung herangezogen werden, ohne das eigentliche Kennwort zu kennen. Eine gängige Angriffsmethode ist daher der Versuch, an Hashwerte von Kennwörtern zu gelangen, die gerade über das Netzwerk einer Institution ausgetauscht werden. Der Angreifer versucht dabei, sich in die Kommunikation zwischen einem Domain Controller und einem Client einzuschalten, während ein Authentifizierungsvorgang läuft. Es handelt sich dabei um eine Form eines Man-in-the-Middle-Angriffs (MITM-Angriff) [siehe Eckert, 2018, S. 419]. Der Angreifer täuscht dabei jedem der beiden Kommunikationspartner vor, dass er das jeweilige Gegenüber sei. Diese Angriffsvariante wird auch als Replay-Angriff bezeichnet.

Ein MITM-Angriff ist in aktuellen Netzwerkstrukturen nicht einfach durchführbar, da die Zugänge auf der Ebene der Clients meist mit Koppelelementen realisiert werden, die eine Stern-Topologie – auf Ebene 2 des ISO/OSI-Referenzmodells, wie in Abbildung 2.1, auf Seite 11 dargestellt – aufweisen. Das bedeutet, dass an jedem Netzzugangspunkt (Port) des Netzwerkes nur Datenpakete übermittelt werden, die genau für den an diesen Port angeschlossenen Client adressiert sind. Ein Angreifer kann also an einem kompromittierten Client – zu Beginn des APT-Angriffs der erste kompromittierte Client (Brückenkopf) – nur Datenpakete sehen, die auch für diesen Client bestimmt sind. Eine MITM-Aktion, also der Eingriff in die Kommunikation, die andere reguläre Clients mit den zentralen AVD-Systemen führen, ist so direkt nicht möglich.

Um auf den Datenverkehr anderer Clients zugreifen zu können, nutzt der Angreifer in dieser Situation systemimmanente Methoden aus, die in der Regel auf Windows-

[15] Eine zufällig gewählte Zeichenfolge, die dem Kennwort vor der Ermittlung des Hashwertes hinzugefügt wird.

basierten Clients zur Verfügung stehen, um automatisch Kommunikationspartner im Netzwerk zu ermitteln. Das Link Local Multicast Name Resolution (LLMNR) Verfahren beispielsweise erlaubt es Systemen, eine Namen-zu-IP-Auflösung unabhängig von eigentlich implementierten DNS-Strukturen[16] durchzuführen. Das Verfahren arbeitet innerhalb des IPv4 Protokollstacks parallel zum im Network Basic Input Output System (NetBIOS) integrierten NetBIOS Name Service (NBNS) und ermöglicht eine Namensauflösung innerhalb einer durch einen Layer 2 Broadcast erreichbaren Netzwerkumgebung.



Quelle: Eigene Darstellung unter Verwendung von Ressourcen von Flaticon.com

Abbildung 3.6: Ablauf eines Man-In-The-Middle-Angriffs am Beispiel einer NTLM Replay Attacke

Ein Angriffswerkzeug, wie zum Beispiel das von Kevin Robertson entwickelte Programm *Inveigh*[17], kann einen LLMNR-Responder oder einen NBNS-Responder immitieren. Das bedeutet, das Programm reagiert auf Broadcast-Aussendungen, die reguläre Clients starten, um beispielsweise die IP-Adresse eines AVD-Servers zu ermitteln, von dem sie aktuell nur den Namen kennen. Empfängt *Inveigh* einen solchen Broadcast, übermittelt es nun aber die IP-Adresse des Systems, auf dem *Inveigh* ausgeführt wird. Wird dies vom regulären Client angenommen, kann sich das Programm in den daran anschließenden Authentifizierungsprozess einschalten. Es empfängt die Anfragen des

[16] Eine grundsätzliche Konfiguration von DNS-Servern auf allen Clients, die mit einer IP-Adresse direkt angesprochen werden, um eine benötigte IP Adresse für einen DNS-Namen zu liefern.

[17] Quelle: `https://github.com/Kevin-Robertson/Inveigh`

Clients, der jetzt fälschlicher Weise den Host des Angreifers für den AVD-Server hält und sendet diese weiter zum echten AVD-Server, gleichzeitig werden die erhaltenen Anmeldedaten abgefangen. Antworten vom AVD-Server werden vom Programm unmittelbar an den wartenden Client weitergeleitet. Der Vorgang ist in Abbildung 3.6 dargestellt. Dieses Beispiel zeigt einen MITM-Angriff, der auf den Anwendungsebenen des ISO/OSI-Referenzmodells abläuft. Er ist möglich, wenn der IP-Datenverkehr zu entsprechenden Serversystemen nicht anderweitig abgesichert wird, beispielsweise durch Internet Protocol Security (IPsec) und / oder dadurch, dass entsprechende temporäre Namensauflösungsmethoden wie LLMNR und NBNS auf Client Ebene nicht deaktiviert sind. Gelangt der Angreifer durch diese Methode an einen neuen oder noch unbekannten Kennworthash, kann er versuchen, damit einen Pass-the-Hash-Angriff durchzuführen.

3.4.2 Pass-the-Hash

Die Pass-the-Hash-Methodik ist ein Angriffsvektor, bei dem der Hashwert eines Benutzerkennwortes vom Benutzer unbemerkt, in unberechtigter Art und Weise, für einen Authentifizierungsvorgang verwendet wird. Der Angreifer kann verschiedene Methoden anwenden, um an den Hashwert eines Kennwort zu gelangen:

1. Auslesen aus einer Benutzer- und Kennwortdatenbank,
2. Mitschneiden der Hash-Übermittlung innerhalb eines regulären Authentifizierungsvorgangs oder
3. Auslesen des Hashwertes aus dem Arbeitsspeicher.

Um Hashwerte beispielsweise mit dem Werkzeug *mimikatz* aus dem Arbeitsspeicher (Credential Cache) auszulesen sind lokale administrative Berechtigungen auf dem System notwendig. Ist der Angreifer mithilfe einer der Methoden an den Hashwert eines Benutzerkennwortes gelangt, so kann er dieses zur Authentifizierung des entsprechenden Benutzers anwenden, ohne das im zentralen AVD-System entsprechende Abwehrsysteme greifen können. Es handelt sich aus Sicht des Authentifizierungsdienstes dabei um einen regulären Authentifizierungsvorgang.

Ein Umstand, der dem Angreifer in dieser Situation sehr weit entgegenkommt, ist der Einsatz von Single Sign-on Verfahren (SSO) innerhalb der Institution. Ziel des Einsatzes von SSO-Verfahren ist es, einem Benutzer mit seiner Identität nur einem einzigen Authentifizierungsprozess innerhalb einer Sitzung (Session) zu unterziehen. Der Begriff Sitzung meint in diesem Zusammenhang den Zeitraum, den der Benutzer an einem Computersystem verbringt, beginnend mit der Systemanmeldung und endend mit der Abmeldung vom Computersystem. Erfolgt die einmalige Authentifizierung des

Benutzers im Rahmen der Systemanmeldung durch die Eingabe eines Kennwortes, so muss bei einigen älteren Authentifizierungsverfahren, wie beispielsweise NTLM, dieses Kennwort beziehungsweise der zugehörige Kennworthash im Computersystem für die gesamte Dauer der Sitzung zwischengespeichert werden. Dies ist in der Regel notwendig, da im Rahmen der Sitzungstätigkeit des Benutzers häufig vom Benutzer unbemerkt Authentifizierungsprozesse durchgeführt werden, beispielsweise beim Zugriff auf eine neu verwendete Ressource, wie eine Dateifreigabe oder einen Netzwerkdrucker. Modernere Authentifizierungsverfahren, wie beispielsweise Kerberos, unterstützen prinzipiell SSO-Verfahren ohne Zwischenspeicherung des Kennwort Hashs. Die in Kapitel 5 dargestellten Konzepte und Verfahren zur Absicherung einer HSA beruhen daher auch auf dem exklusiven Einsatz von Kerberos als Authentifizierungsverfahren. Die Praxis zeigt aber, dass der exklusive Einsatz von Kerberos in großen, heterogenen Systemumgebungen sehr schwer umzusetzen ist. Sobald Anwendungen oder Dienste im internen Netz genutzt werden, die Kerberos nicht unterstützen, ist ein Fall-Back auf beispielsweise NTLM nötig, der wiederum eine Kennwortspeicherung innerhalb der Sitzung bedingt.

Schutz gegen Pass-the-Hash-Angriffe

Die Detektierung eines Pass-the-Hash-Angriffes ist ausgesprochen schwer möglich, da der eigentliche Authentifizierungsvorgang mit einem gestohlenem Hashwert nicht von einem echtem, regulärem Authentifizierungsvorgang zu unterscheiden ist. Auf der Seite des AVD-Serversystems kann mitunter eine erweiterte, kontextbasierte Ereignisprotokollierung von Authentifizierungsvorgängen nützlich sein. Lösungsansätze dazu werden in Abschnitt 4.5 näher beschrieben.

Grundsätzlich gilt, dass Arbeiten an Computersystemen mit administrativen Berechtigungen soweit wie möglich – auch zeitlich – zu beschränken sind. Grundsätzlich sollten Computersysteme nicht im angemeldeten Zustand, also mit laufender Sitzung unbenutzt betrieben werden. Normale Arbeitsstationen sollten zum Ende der Arbeitszeit ausgeschaltet werden. Der ausschließliche Einsatz von Kerberos als Authentifizierungsverfahren und damit der Verzicht auf ältere Verfahren wie NT Lan Manager (NTLM) wird seitens des BSI und seitens der Microsoft Corporation bereits seit mehreren Jahren empfohlen. Diese Empfehlung innerhalb einer Institution umzusetzen, gestaltet sich jedoch schwierig. Ein homogener Einsatz von Kerberos bedingt die konsequente Nutzung eines DNS-Namensraums und eines entsprechenden *Kerberos-Realm*, über den alle Anwendungen und Dienste innerhalb des internen Netzes einer Institution adressiert werden müssen. Der Einsatz von rein IP-adressierten Diensten verbietet sich, da dafür keine Kerberos-Tickets ausgestellt werden können. Diese Anforderung

ist jedoch bei der Mehrheit von Institutionen, mit typischerweise IT-technisch gewachsenen Strukturen, schwer durchzusetzen. Eine erste und eher leicht durchzuführende Stufe der Absicherung ist die Deaktivierung der ersten NTLM Version (NTLMv1) als Authentifizierungsverfahren, wie sie vom BSI empfohlen wird. Die Verwendung und Speicherung von mittlerweile als unsicher zu betrachtenden LAN Manager Hashes (LM-Hashes) bei NTLMv1 wird damit unterdrückt. Eine entsprechende Sicherheitsrichtlinie wird in Abschnitt 2.4.1 in Form der *NTLM-Level* angesprochen.

Clientseitig ist der Einsatz aktueller Betriebssystemversionen zu empfehlen. Innerhalb der MS Windows 10 Produktfamilie ist beispielsweise eine Funktion verfügbar, die als *Credential Guard* bezeichnet wird. Basierend auf dem Einsatz von clientseitiger Virtualisierungstechnologie wird der Speicherbereich, in dem Anmeldeinformationen während einer Sitzung zwischengespeichert werden, zusätzlich geschützt, um den Zugriff durch nicht-autorisierte Programme wie das in Abschnitt 3.3 beschriebene Programm *Mimikatz* zu verhindern.

Varianten von Pass-the-Hash-Angriffen

Im Laufe der letzten Jahre hat sich der Angriffsvektor *Pass-the-Hash* methodisch weiterentwickelt. Es sind mittlerweile mehrere Varianten dieses Angriffsvektors bekannt.

Pass-the-Ticket

Auch wenn Kerberos als Authentifizierungsverfahren eingesetzt wird, bietet das keine absolute Sicherheit vor einem Identitätsdiebstahl. Die Variante Pass-the-Ticket ähnelt dem Pass-the-Hash-Verfahren mit dem Unterschied, dass nicht ein Kennworthash ausgelesen und unberechtigt weiter benutzt wird, sondern ein vom Authentifizierungsdienst im Rahmen des Kerberos Authentifizierungsprozess erstelltes Kerberos-Ticket unberechtigt vom Angreifer ausgelesen und benutzt wird. Der technische Vorgang entspricht dabei dem Pass-the-Hash-Angriff.

Over-Pass-the-Hash (Pass-the-Key)

Die Over-Pass-the-Hash-Methode bezeichnet eine Kombination aus Pass-the-Hash und Pass-the-Ticket. Wenn für das weitere Vorgehen des Angreifers ein Kerberos-Ticket erforderlich ist, aber aktuell nicht auf ein solches zugegriffen werden kann, stattdessen aber auf einen NTLM Kennwort Hash, so kann dieser Hash genutzt werden, um ein Kerberos-Ticket zu erstellen. Die Verknüpfung der beiden Authentifizierungsverfahren NTLM und Kerberos ist seitens der Microsoft Corporation aus Gründen der Rückwärtskompatibilität mit älteren Betriebssystemversionen vorgesehen. Dieser Umstand wird durch diese Angriffsvariante

ausgenutzt, um mit einem vergleichbar unsicheren NTLM Hash des veralteten NTLM-Verfahrens ein gültiges Kerberos-Ticket zu erzeugen.

Pass-the-Cache

Auch unixoide Betriebssysteme wie Mac OS®, UNIX oder Linux-Derivate sind, sofern Kerberos-Authentifizierungsfunktionen implementiert sind, nicht vor Pass-the-Ticket-Angriffen sicher. Auf unixoiden Betriebssystemen werden Kerberos-Tickets in einer temporären Credential Cache (ccache) Datei abgelegt. Mittels eines Pass-the-Cache-Angriffs können Ticket Granting Tickets (TGT) aus dieser Datei beispielsweise durch Programme wie *Mimikatz* ausgelesen werden. Anschließend kann der Microsoft Privilege Attribute Certificate Data Structur (MS-PAC) Anteil des Tickets dahingehend modifiziert werden, dass unrechtmäßige Gruppenzugehörigkeiten, beispielsweise Mitgliedschaft in der Domänenadministratorgruppe hinzugefügt werden.[18] Eine Vertikalbewegung in Form einer Privilege Escalation ist somit möglich.

3.4.3 Golden- und Silver-Ticket-Angriffe

Die beiden als Golden- und Silver-Ticket-Angriffe bekannten Angriffsformen sind eine speziell auf den Kerberos Authentifizierungsdienst gerichtete Variante des Identitätsdiebstahls. Die beiden Angriffsformen richten sich damit direkt gegen das zentrale AVD-System einer Institution. Beiden Varianten gleich ist die Kenntnis des geheimen Schlüssels des Kerberos Authentication Servers (KAS) – in Abbildung 2.8 als K_{TGS} bezeichnet – innerhalb eines zentralen AVD-Systems[19]. Den Zugriff auf diese Daten haben nur Benutzer mit allerhöchster Berechtigungsebene innerhalb einer AVD-Umgebung, wie beispielsweise Domänenadministratoren[20]. Aber auch ein physikalischer Zugriff auf die Daten beziehungsweise Datenspeicher der AVD-Serversysteme und der Datensicherungen gewährt die Kenntnis dieser sensiblen Daten. Sobald ein Angreifer den geheimen Schlüssel K_{TGS} des Kerberos Authentication Server (KAS) kennt, kann er sich beispielsweise mit dem Programm mimikatz selbst Kerberos-Tickets ausstellen. Zur Erstellung der Tickets ist keine Onlinekommunikation mit dem AVD-System notwendig. Da die vom Angreifer erstellten Kerberos-Tickets – durch

[18] Die entsprechende Sicherheitslücke ist 2014 im Microsoft Security Bulletin MS14-068 als Exploit bekannt geworden. Sicherheitsupdates sind verfügbar.

[19] In MS Active Directory® Umgebungen wird in diesem Zusammenhang oft vom Kennwort des *krbtgt*-Kontos gesprochen. Der KDC-Dienst auf dieser Art von Systemen wird mit diesem Systemkonto gestartet.

[20] These: Sobald ein Angreifer ein Konto mit Rechten eines Domänen- oder Enterpriseadministrators kompromittiert hat, kann davon ausgegangen werden, dass auch ein Golden-Ticket-Angriff erfolgreich abgeschlossen wurde.

Kenntnis des Schlüssels K_{TGS} – exakt so verschlüsselt sind, wie sie der KAS selbst verschlüsseln würde, sind sie auch von regulär durch den KAS erstellte Tickets nicht zu unterscheiden. Der genaue Ablauf eines Kerberos Authentifizierungsprozesses wird in Abschnitt 2.4.1 beschrieben.

Kerberos Silver-Ticket

Als Silver-Ticket wird ein unberechtigt vom Angreifer selbst ausgestelltes Kerberos Service Ticket (ST) bezeichnet. Zur Erstellung wird nicht, wie im regulären Kerberos-Authentifizierungsprozess erforderlich, in der Vorstufe ein Ticket Granting Ticket (TGT) zur Authentifizierung benötigt. Der Angreifer kann sich direkt und ohne weitere Kommunikation mit dem AVD-System an einem Dienst oder einer Anwendung innerhalb des Verwaltungsbereichs des AVD-Systems authentifizieren und erhält damit Zugriff entsprechend der im Rahmen dieses Angriffs verwendeten Benutzeridentität.

Kerberos Golden-Ticket

Als Golden-Ticket wird ein Kerberos-Ticket Granting Ticket (TGT) bezeichnet, das, durch Kenntnis des geheimen KAS Schlüssels K_{TGS}, unberechtigter Weise durch den Angreifer erstellt wird. Da das TGT mithilfe des K_{TGS} vom Angreifer selbst erstellt werden kann, ohne mit dem zentralen AVD-System zu kommunizieren[21], ist er nicht an entsprechende Erstellungsrichtlinien des AVD-Systems gebunden, wie beispielsweise Ticket-Gültigkeitszeiträume. Meist erstellen Angreifer daher TGTs mit Gültigkeitszeiträumen von mehreren Jahren im Gegensatz zu regulär erstellten TGTs mit Gültigkeitszeiträumen von etwa 10 Stunden. Auch an gültige Kontenrichtlinien ist der Angreifer nicht gebunden. So ist die Erstellung von Tickets für gesperrte oder gar nicht existente Benutzeridentitäten denkbar.

Wie bereits in der Einleitung zu dieser Arbeit angemerkt wurde, bedeutet die Verwendung von Golden-Tickets innerhalb eines AVD-Systems den kompletten Verlust der Integrität, Vertraulichkeit und Authentizität der Daten, die im Kontrollbereich dieses AVD-Systems – also des Kerberos Realms oder der Domäne – liegen. Dem Angreifer ist es damit möglich, jede denkbare Identität und jede denkbare Berechtigungsstufe innerhalb der angegriffenen Domäne einzunehmen. Das bedeutet im Klartext, er kann auf alle Daten, die innerhalb der Domäne regulär durch eine entsprechende Berechtigungsstruktur geschützt sind, zugreifen, sie nach Belieben ändern oder löschen. Da er dies innerhalb der normalen Berechtigungsprozesse vollzieht, ist der Zugriff auf die Daten

[21] Der Angreifer muss sich lediglich zur Erlangung des geheimen Schlüssels K_{TGS} im Netzwerk des Opfers befinden (online). Die Erstellung des TGT kann anschließend – zeitlich und netzwerktechnisch unabhängig davon – erfolgen (offline).

völlig unauffällig. Dies geht sogar so weit, dass Daten, die durch eine domänenintegrierte PKI mittels Zertifikaten verschlüsselt wurden, im Zugriff des Angreifers stehen. Der Angreifer muss für sich hierzu lediglich in einem zusätzlichen Schritt entsprechende Zertifikate ausstellen, die dann als reguläre Zertifikate entsprechend benutzt werden können.

Schutzmaßnahmen gegen Golden- und Silver-Ticket-Angriffe

Die vom Angreifer selbst erstellten Tickets, die wie oben beschrieben offline erstellt wurden, haben so lange Gültigkeit, bis sich der geheime (private) Schlüssel K_{TGS} des KAS, ändert. In Domänen-Systemen ist in der Regel eine automatische Schlüsseländerung des KDC-Dienstes (KAS) in der Standardinstallation nicht vorgesehen.[22] Aus sicherheitstechnischer Sicht empfiehlt es sich jedoch, den Schlüssel K_{TGS} in regelmäßigen Abständen kontrolliert zu ändern. Ein eventuell bis dato von einem potenziellem Angreifer unbemerkt erstelltes Silver- oder Golden-Ticket verliert dadurch seine Gültigkeit. Der Änderungsvorgang wird als *KRBTGT Key Rollover* bezeichnet. Ein entsprechender Prozess wird von Poeppelman beschrieben. [siehe Poeppelman, 2020] Ein Skript, um die Kennwortänderung automatisch durchzuführen, ist auf Github verfügbar.[23]

Skeleton-Key-Angriff

Eine weitere Methode eines Angriffs auf AVD-Systeme des Herstellers MS bildet der Skeleton-Key-Angriff. Auch hier ist, wie bei den Golden- und Silver-Ticket-Angriffen, eine bereits erfolgte Kompromittierung eines Kontos mit Domänenadministratorberechtigungen nötig. Hat der Angreifer diese Berechtigungsstufe erreicht, kann er mit Tools, wie das in Abschnitt 3.3 vorgestellte Programm *Mimikatz*, in die Laufzeitumgebung des Anmelde- und Authentifizierungsdienstes jedes einzelnen Domain Controllers eine kompromittierte Dynamic Link Library (DLL) einschleusen. Auf MS Active Directory® Domain Controllern ist der LSASS-Prozess für die Beantwortung von Authentifizierungsanfragen zuständig. Dieser Prozess unterstützt meist die beiden Authentifizierungsverfahren NTLM und Kerberos. Für jedes der dazugehörigen Authentifizierungsprotokolle werden die entsprechenden Protokollfunktionen durch je eine DLL zur Verfügung gestellt. Der Angreifer tauscht im Rahmen des Angriffs diese beiden DLLs gegen modifizierte Versionen aus. Diese kompromittierten DLLs sorgen dafür, dass zur Laufzeit des Authentifizierungsdienstes jede weitere clientseitige Authen-

[22] Der Prozess der Schlüsseländerung ist für ein AVD-System als kritisch anzusehen, da auch alle systeminternen Prozesse des AVD-Systems (beispielsweise die DB- und Datensyncronisation) authentifiziert ablaufen und damit eine interne Systemabhängigkeit zu diesem Schlüssel besteht.

[23] Quelle: `https://github.com/microsoft/New-KrbtgtKeys.ps1`

tifizierungsanfrage, alternativ zum regulärem Kennwort, auch durch die Benutzung eines vom Angreifer gewählten Master-Kennwortes als Generalschlüssel (Skeleton-Key) erfolgreich beantwortet wird. Erfolgt die Authentifizierung mittels NTLM wird nunmehr ein eingehender Hash-Wert des Generalsschlüssels nicht mehr gegen die Benutzerkontendatenbank geprüft, sondern es erfolgt ungeprüft eine erfolgreiche Authentifizierung. Der Kerberos-Authentifizierungsprozess wird derart modifiziert, dass bei der TGT-Anforderung des Angreifers auf eine Verschlüssellung mit Salt (RC4_HMAC_-MD5) verzichtet wird und statt auf den Hashwert (basierend auf Kennwörtern der regulären Benutzerkontendatenbank) zuzugreifen, der Hash des Generalschlüssels verwendet wird.

Bisher ist bekannt, dass diese Art des Angriffs nur auf Domain Controller des Herstellers Microsoft Corporation (MS) abzielt, da speziell modifizierte DLLs eingeschleust werden, die auf der Codebasis von MS-Servern beruhen. Eine Kompromittierung von Samba-basierten AVD-Systemen ist mit dieser Methode mit den in Abschnitt 3.3 beschriebenen Werkzeugen bisher nicht bekannt. Weiterhin ist im beschriebenen Szenario der Angriff auf MS-Server nicht persistent. Nach einem Neustart der AVD-Systeme ist der Generalschlüssel des Angreifers nicht länger wirksam. Der Angreifer muss die DLLs erneut auf dem Domain Controller einschleusen. Ein Vorteil gegenüber des Golden-Ticket-Angriffs ist aus Sicht des Angreifers die gleichzeitige Kompromittierung des aus Gründen der Rückwärtskompatibilität meist noch vorhanden NTLM Authentifizierungsprotokolls. Der vom Angreifer eingeschleuste Generalschlüssel erlaubt eine Authentifizierung unabhängig davon, ob das Kerberos oder NTLM-Protokoll verwendet wird.

Schutzmaßnahmen gegen Skeleton-Key-Angriffe

Wie beschrieben, ist der Angriff nicht persistent. Ein Neustart der AVD-Server würde den Angriff beenden. In den meisten Umgebungen ist dieser Neustart nicht einfach und nicht regelmäßig durchführbar, da er unmittelbare Auswirkung auf alle Server- und Client-Systeme einer internen Netzwerkumgebung hat.

DCSync-Angriffe

Bei dieser Art des Angriffs werden Funktionalitäten ausgenutzt, die im regulären Betrieb benötigt werden, wenn die AVD-Umgebung einer Institution aufgrund der Institutionsgröße aus mehr als einem Domain Controller (DC) besteht. Wie in Abschnitt 2.4.3 beschrieben, wird der gemeinsame Datenbestand eines verteilten AVD-Systems auf allen DC mithilfe des Directory Replication Service Remote Protocol (MS-DRSR)-Verfahrens synchronisiert. Der Angreifer nutzt in diesem Szenario diesen Umstand

aus und stellt sein eigenes System als DC dar. Auch für diesen Angriff werden Berechtigungen eines Domänenadministrators benötigt. Wenn der Angreifer erfolgreich einen Replikationsprozess mittels MS-DRSR-Verfahren durchführen konnte, ist er im Besitz einer kompletten Kopie der Benutzer- und Kontendatenbank eines DCs. Die Situation ist vergleichbar mit der Besitzerlangung einer Datensicherung eines DCs oder dem Diebstahl einer Festplatte aus einem DC, auf der die Datenbank ebenfalls enthalten ist. Da sich innerhalb der Datenbank die Hashwerte der Benutzerkennwörter befinden, auch die des Systemkontos *krbtgt*, hat der Angreifer somit auch Kenntnis über den geheimen Schlüssel K_{TGS} des KAS, vergleichbar der am Beginn dieses Abschnitts beschriebenen Methoden. Um diesen Angriff durchzuführen, sind folgende Berechtigungen beziehungsweise Access Control Lists (ACLs) notwendig:

- Replicating Directory Changes,
- Replicating Directory Changes All und
- Replicating Directory Changes In Filtered Set.

Diese Berechtigungen sind in der Regel an die Gruppe der lokalen Administratoren auf Domain Controllern, Domänenadministratoren und Enterpriseadministratoren vergeben. Ein derartiger Angriff verläuft nicht spurlos. Replikationsprozesse werden grundsätzlich protokolliert. Eine entsprechende Überwachung der Ereignisprotokollierung verrät einen Angriff. Dies allerdings erst, nachdem die kritischen Daten abgeflossen sind.

3.4.4 Zusammenfassung der Angriffsvektoren gegen AVD-Systeme

Der größte Teil der oben beschriebenen Angriffsvektoren ist nur mit Berechtigungen der höchsten Berechtigungsebene, als Domänen- oder Enterpriseadministrator durchführbar. Als Schlussfolgerung daraus ergibt sich die besondere Stellung dieser Berechtigungsebene innerhalb des Rollenkonzeptes einer AVD-Umgebung. Zum Schutz von AVD-Systemen und schlussendlich damit auch zum Schutz aller Daten, die durch ein zentrales AVD-System verwaltet werden, ist es unbedingt notwendig, zu verhindern, dass ein Angreifer in diese Berechtigungsebene vordringen kann. Im folgenden Kapitel werden daher Abwehrstrategien vorgestellt, die genau ein Ziel haben, dem Angreifer die Erweiterung seiner Benutzerrechte (Privilege Escalation) bis hin zum Domänenadministrator unmöglich zu machen.

Weiterhin wird aus den oben beschriebenen Methoden der kritische Punkt eines jeden zentralen AVD-Systems deutlich. Das Systemkonto des Kerberos Key Distribution

Center[24] bedarf der besonderen Aufmerksamkeit. Das Kennwort und der entsprechende Kennworthash (der geheime Schlüssel K_{TGS}) dieses Kontos sind der zentrale Angelpunkt der IT-Sicherheit einer Kerberos-basierten Domäne. Der Hersteller Microsoft Corporation und das BSI empfehlen eine regelmäßige Änderung dieses Kennwortes im Rahmen eines *KRBTGT Key Rollover*. [siehe Poeppelman, 2020] Dieser Prozess ist auch ein zentraler Bestandteil eines jeden Bereinigungsprozesses, sobald eine Kompromittierung der AVD-Struktur durch einen Angreifer festgestellt wurde.

Eine Eigenschaft, die alle vorgestellten Methoden aufweisen, ist die extrem schwierige Detektion des Angriffs. Da der Angriff immer auf regulären Prozessen oder Protokollen aufbaut, sind Hinweise über einen gerade laufenden Angriff für die Administratoren einer Institution nur sehr schwer zu erhalten. Angreifer werden eher selten in physischer Präsenz innerhalb der Institution Angriffe durchführen, sondern vielmehr über C&C-Server im Internet die Angriffe steuern. Eine Überwachung der Kommunikation von internen Systemen in Richtung Internet an zentralen Knoten der Institution, in der Regel der Internet-Firewall, ist daher in dieser Hinsicht effizient. Ein mögliches Indiz für einen laufenden Angriff kann hier die Kommunikation zu entsprechend auffälligen IP-Adressbereichen sein.

Im folgenden Kapitel wird im Abschnitt 4.5 auf die Möglichkeiten von intelligenten Analyseverfahren hingewiesen, mit deren Hilfe Ereignisprotokolle von AVD-Systemen nach auffälligen Ereignissen durchsucht werden können, die auf Tätigkeiten eines Angreifers hindeuten.

[24] Auf DC des Herstellers MS das Systemkonto *krbtgt*, mit dem der Dienst gestartet wird.

4 Strategien zur Abwehr von APT-Angriffen

In diesem Kapitel werden Basistechnologien vorgestellt, die als Abwehrstrategien gegen die in Kapitel 3 vorgestellten Angriffe gegen einen zentralen Authentifizierungs- und Verzeichnisdienst eingesetzt werden können. Alle bekannten Abwehrstrategien anzusprechen, würde den Rahmen dieser Arbeit sprengen. Die hier vorgestellten Strategien wurden ausgewählt, weil sie sehr effektiv zur Abwehr eingesetzt und in fast jeder Institution umgesetzt werden können. Grundsätzlich können bei der Entwicklung von Abwehrstrategien folgende Ziele verfolgt werden:

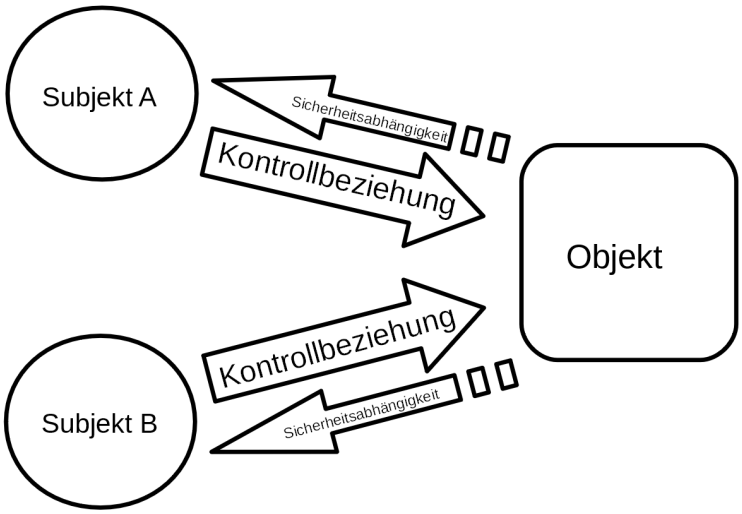
- Reduzierung der Footprints auf Systemen innerhalb einer AVD-Umgebung,
- Absicherung des Authentifizierungsprozesses,
- Schutz der privilegierten Zugangskonten und
- Überwachung der Systemaktivitäten.

Der Großteil der im Folgenden dargestellten Strategien und Methoden ist unabhängig von bestimmten Implementierungen anwendbar. Sie betreffen vielmehr grundlegende, strukturelle Aspekte in Bezug auf den Aufbau zentraler Authentifizierungs- und Verzeichnisdienst (AVD)-Systeme.

4.1 Grundprinzip der vertrauenswürdigen Quelle

Das Grundprinzip der vertrauenswürdigen Quelle, auch bekannt als Clean Source Prinzip (CSP), besagt, in abstrakter Form, dass für ein abzusicherndes Objekt jedes dazu in einer Sicherheitsabhängigkeit stehende Subjekt ebenso abzusichern ist, wie das Objekt selbst. [siehe Microsoft, 2019b] In Abbildung 4.1 ist zu erkennen, dass jedes Subjekt, das ein Objekt kontrolliert, eine Sicherheitsabhängigkeit dieses Objektes darstellt. Hat ein Angreifer eine Möglichkeit gefunden, effektive Kontrolle auf ein sicherheitsabhängiges Subjekt zu erlangen, hat er damit gleichzeitig auch die Kontrolle über das Zielobjekt erlangt. Als Schlussfolgerung ist es daher ein Grundsatz bei der Absicherung von Objekten, alle Sicherheitsabhängigkeiten im Rahmen einer Anforderungsanalyse zu ermitteln und anschließend sicherzustellen, dass die Sicherheitsstufe der entsprechenden Subjekte der Sicherheitsstufe des Zielobjektes selbst entspricht. Die dargestellte Kontrollbeziehung ist transitiv, wie in Abbildung 4.2 dargestellt, jedoch nicht grundsätzlich kumulativ. Daraus folgt, dass Subjekt A nicht automatisch die Kontrolle über

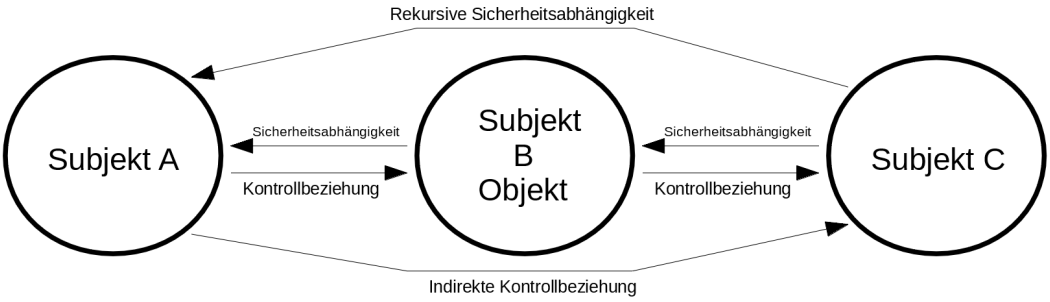
Subjekt B hat, bedingt dadurch, dass beide die Kontrolle über das gleiche Objekt haben, wie in Abbildung 4.1 dargestellt. Dieses Prinzip ist allgemeingültig, kann also auf alle Arten von Objekten angewandt werden, wie Hardware- und Systeminstallation, Softwareentwicklung und -verteilung, Architektur oder Konfiguration von Systemen.



Quelle: In Anlehnung an [Microsoft, 2019b]

Abbildung 4.1: Sicherheitsabhängigkeit zwischen Subjekten und einem Objekt

Die in Abbildung 4.2 dargestellte Verkettung von Subjekten und Objekten wird im Bereich der Cybersecurity mitunter als Supply-Chain bezeichnet und sollte in diesem Rahmen nicht mit dem gleichlautenden Begriff der Lieferkette aus dem Wirtschaftssektor verwechselt werden. Entsprechende Angriffe auf diese Kette werden demnach als Supply-Chain-Attack[1] beschrieben.



Quelle: In Anlehnung an [Microsoft, 2019b]

Abbildung 4.2: Transitivität zwischen mehreren Subjekten und Objekten

Angriffe auf die Supply-Chain sind nicht selten erfolgreich, wie der NotPetya Outbreak als Beispiel für einen Angriff auf eine Software-Supply-Chain zeigt. [siehe

[1] https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks

Quelle: Eigene Darstellung

Abbildung 4.3: Sicherheitsabhängigkeiten beim Aufbau von AVS- und HSA-Systemen

Maynor et al., 2017] In diesem Fall wurde der Software-Update-Mechanismus eines ukrainischen Entwicklers für Buchhaltungs- und Steuersoftware initial angegriffen, um Schadsoftware einzuschleusen, die sich dann über die normale Vertriebskette der Software weiter verteilen konnte.

Um das Prinzip der vertrauenswürdigen Quelle auf den Bereich des Aufbaus einer hochsichere Administrationsumgebung (HSA) zu übertragen, kann Abbildung 4.3 herangezogen werden. Aus der Darstellung wird deutlich, dass eine letztendlich installierte HSA, ebenso wie das eigentliche AVD-System, grundlegend sicherheitstechnisch von der Vertrauenswürdigkeit der verwendeten Hardware und Software abhängt. Dabei sind bei der Hard- und Softwareinstallation unterschiedliche Schwerpunkte zu setzen.

Hardwareinstallation

Hier können folgende Schritte zur Absicherung der Supply-Chain empfohlen werden:

- Absicherung der Vertriebskette für Hardware-Produkte. Wird auch wirklich ein Originalprodukt und nicht ein Nachbau als günstigeres Angebot bezogen?
- Sicherheitsprüfung der Originalverpackung bzw. Versiegelung der Komponenten und Lieferteile.
- Firmware-Reset bzw. (UEFI)-BIOS-Update bei der Erstinbetriebnahme.
- Installation und Inbetriebnahme in einer abgesicherten Installationsstraße.

Softwareinstallation

Bei dem Bezug von Software muss sichergestellt werden, dass Installationsdaten und -medien nach der Herausgabe beziehungsweise Veröffentlichung durch den Hersteller nicht manipuliert wurden. Im Grundmodell aus Abbildung 4.1 stellt die Installationssoftware das Ursprungssubjekt dar, welches im Rahmen der Installation (Kontrollbeziehung) als Ergebnis das installierte System als Objekt erzeugt. Die Softwareintegrität

muss dabei während des gesamten Zyklus, also vom Bezug über die Aufbewahrung bis hin zur Verwendung der Software gewahrt bleiben. Gleichzeitig ist eine entsprechende Dokumentation des Zyklus sinnvoll. Beim Erwerb der Software sollte die Quelle über eine der folgenden Methoden überprüft werden: [siehe Microsoft, 2019b]

- Die Software wird auf einem physischen Medium erworben, das vom Hersteller oder einer seriösen Quelle stammt (üblicherweise werden diese Medien von einem Anbieter ausgeliefert).
- Die Software wird aus dem Internet bezogen und mittels der vom Softwareanbieter bereitgestellten Datei-Hashes überprüft.
- Die Software wird aus dem Internet bezogen und es werden zwei unabhängig sowie unterschiedlich heruntergeladenen Kopien durch Vergleich der Datei-Hashes überprüft.
- Die Software wird im Quellcode bezogen (Open Source), einem Review unterzogen und anschließend selbst kompiliert.

Wenn möglich, sollte Anwendungssoftware wie Anwendungsinstallationsprogramme und -tools immer digital signiert werden. Weiterhin sollte die Software innerhalb der Institution in der Art gespeichert werden, dass sie nicht von Unbefugten bearbeitet oder verändert werden kann. Eine Speicherung mit gleichzeitiger Dokumentation des Datei-Hashes ist sinnvoll, da idealerweise direkt vor der Verwendung – dem Start des Installationsprozesses – eine Integritätsüberprüfung in Form einer nochmaligen Überprüfung der Datei-Hashes vorgenommen werden kann.

4.2 Prinzip der Berechtigungsebenen (Schichtenmodell)

Die Einführung eines Schichtenmodells ist die konsequente Umsetzung des Grundprinzips der vertrauenswürdigen Quelle in Bezug auf die Architektur und den Entwurf eines zentralen AVD-Systems. Es bedeutet eine schematische Einteilung in Sicherheitsschichten und die Modellierung eines grundlegenden sicherheitsbezogenen Schichtenmodells.

Begriffsdefinition: Sicherheitsschicht

Im Bereich des BSI-Grundschutzes werden die Begriffe *Informationsverbund* [siehe BSI, 2017b, S. 29ff] und *Schutzbedarf* [siehe BSI, 2017a, S. 77ff] häufig gebraucht. Diese werden im Rahmen des IT-Grundschutzes verwendet, um eine Schutzbedarfsanalyse durchzuführen. Der Informationsverbund bezeichnet die Menge an Objekten

und / oder Systemen, für die eine Bewertung erfolgt. Das Ergebnis einer Risikobeurteilung für den Informationsverbund wird als Schutzbedarf klassifiziert. Die im Folgenden vorgestellte Strategie ähnelt einem solchen Prozess, bezieht sich aber nur auf die Objekte im Verwaltungsbereich eines zentralen AVD-Systems, der hier entsprechend als Informationsverbund betrachtet werden kann. Eine Einstufung nach den BSI-Schutzbedarfskategorien ist hier mithin nicht sinnvoll, da sie zu grob klassifiziert. Daher wird im Folgenden der Begriff der Sicherheitsschicht eingeführt. Er steht synonym für die Begriffe Vertrauensebene, Zugriffsebene, Level- oder Sicherheitslevel (Tier), wenn sie vom Bedeutungsumfang her die Einstufung von Kontroll- und Zugriffsregeln spezifizieren, die einem Subjekt im Bereich eines zentralen AVD-Systems in Bezug auf ein Objekt zugeschrieben werden. Exemplarisch sei in Tabelle 4.1 noch eine sehr grobe, aber dafür leicht verständliche Einteilung einer Systemarchitektur in fünf Sicherheitsebenen für Benutzer dargestellt:

Tabelle 4.1: Denkbare Rollenverteilung auf einem System

Rolle	Funktionsbeschreibung
Gast	Nutzer mit eingeschränkten Rechten an einem lokalen System
Benutzer	Nutzer können keine Änderungen am System durchführen, dürfen jedoch Anwendungen ausführen.
lokaler Administrator	Nutzer haben uneingeschränkte Rechte an einem lokalen System
Systemadministrator	Nutzer haben uneingeschränkte Rechte an einem Serversystem
Domänenadministrator	Nutzer haben uneingeschränkte Rechte an einem AVD-System

Quelle: In Anlehnung an Rechteeinteilung eines Windows Betriebssystems

In Tabelle 4.1 sind Rollen dargestellt, deren Schutzbedarf nach unten ansteigend ist. Dies folgt direkt aus der Beurteilung des möglichen Schadens bei einer eventuellen Kompromittierung der Rollengruppe und der Annahme einer gleichbleibenden Häufigkeit der Kompromittierung.

Meist sind in einem zentralen AVD-System erheblich mehr Rollen- und Berechtigungen vorhanden, als in Tabelle 4.1 dargestellt. Auch müssen bei der Betrachtung von Sicherheitsschichten nicht nur Benutzer und Benutzergruppen herangezogen werden, sondern auch Computersysteme, die innerhalb einer AVD-Umgebung als Objekte mit entsprechenden Berechtigungen existieren. In einer üblichen AVD-Umgebung gibt es

mehrere tausend einzelne Berechtigungs- und Zugriffseinstellungen, die in diesem Zusammenhang auch als Access Control List (ACL) bezeichnet werden. Eine Sicherheitsschicht in einem zentralen AVD-System entspricht einer Gruppe von Objekten genau gleichen Funktions- und Rechteumfangs innerhalb des Gültigkeitsbereiches des AVD-Systems. Sicherheitsschichten besitzen bezüglich des Schutzbedarfs eine unterschiedliche Gewichtung, die abhängig ist vom möglichen Schaden, der bei einer Kompromittierung entstehen könnte.

Anwendung des Prinzips der vertrauenswürdigen Quelle auf Sicherheitsschichten

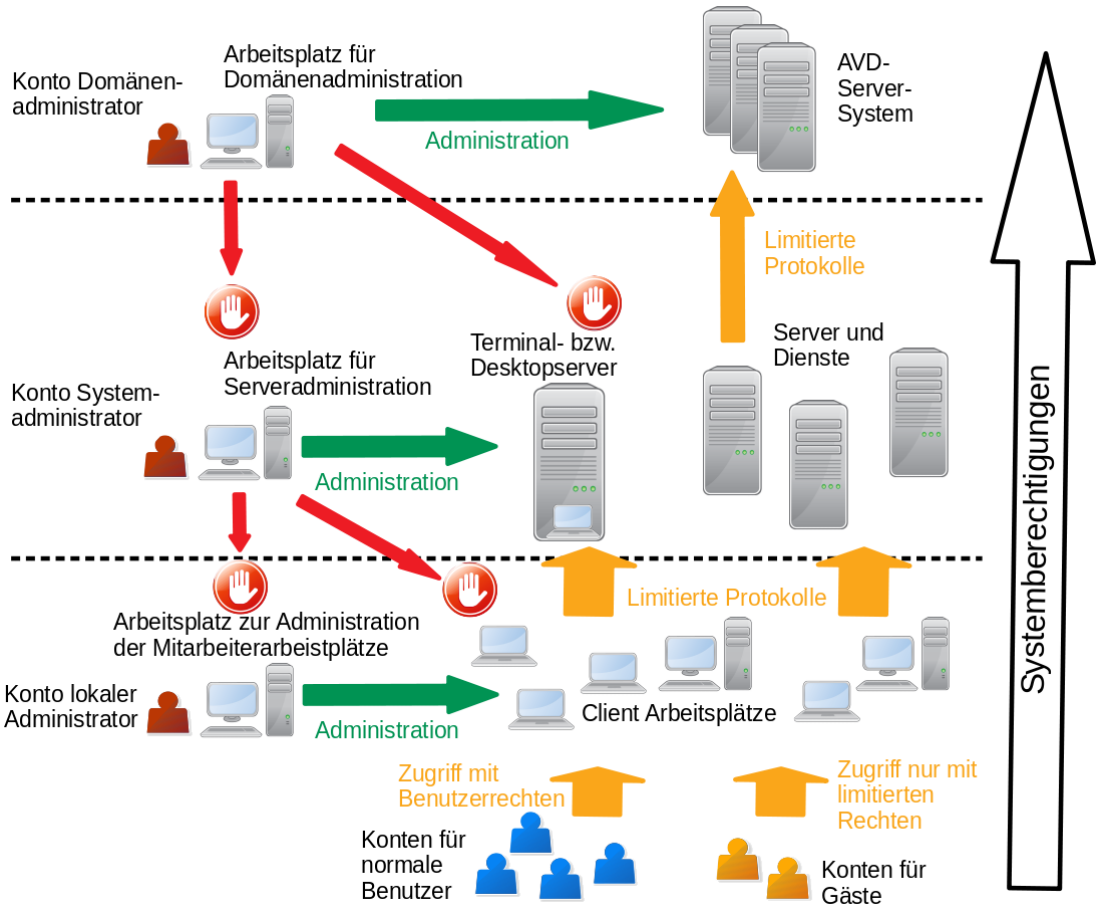
Wendet man das im Abschnitt 4.1 vorgestellte Prinzip der vertrauenswürdigen Quelle auf eine AVD-Systemarchitektur mit implementierter Rollen- und Berechtigungsstruktur an, so ergibt sich in Anlehnung an die Supply-Chain aus Abschnitt 4.1 und das Bell-LaPadula-Modell aus Abschnitt 2.5.1 folgende Beziehungskette:

- Ein Objekt einer Sicherheitsschicht darf nicht von einem Subjekt einer Sicherheitsschicht mit niedrigerem Schutzbedarf abhängig sein.
- Ein Objekt darf nur eine Abhängigkeit von einem Subjekt der gleichen Sicherheitsschicht oder einer Sicherheitsschicht mit höherem Schutzbedarf haben.

Die möglichen Abhängigkeiten werden in Abbildung 4.4 mit den beispielhaft in Tabelle 4.1 dargestellten Sicherheitsschichten wiedergegeben. Zur Erläuterung sei nochmals Tabelle 4.1 herangezogen. Es wäre beispielsweise zulässig, dass ein Nutzer, der als AVD-Systemadministrator tätig ist, ein AVD-System administriert und steuert, da dies einer Sicherheitsschicht mit gleichem Schutzbedarf entspricht. Es wäre aber nicht zulässig, dass ein Nutzer, der an einem einzelnen Arbeitsplatz-Computersystem lokale Administratorrechte besitzt, damit steuernden Zugriff auf ein Serversystem erhält, es sei denn, er ist lokaler Administrator an genau diesem Serversystem, da ein Serversystem einer höheren Sicherheitsschicht entspricht als ein Arbeitsplatz-Computersystem.

Vor dem Hintergrund, dass in einem Windows System Anmeldeinformationen zwischengespeichert werden (Footprint), die im Falle einer Kompromittierung des Computersystems ebenfalls kompromittiert sind, wie in Abschnitt 3.4.2 Pass-the-Hash beschrieben, ist es von elementarer Bedeutung, die Computersysteme selbst in die Betrachtung der Sicherheitsschichten als Subjekt und Objekt mit einzubeziehen. Meldet sich beispielsweise ein AVD-Administrator[2] an einer Arbeitsstation an, entsteht folgende Abhängigkeitskette: Jeder Benutzer, der über lokale Administrationsrechte an dieser Arbeitsstation verfügt, kann auf die Anmeldeinformationen des AVD-

[2] Im Kontext eines MS Active Directory® beispielsweise ein Domänenadministrator.



Quelle: Eigene Darstellung

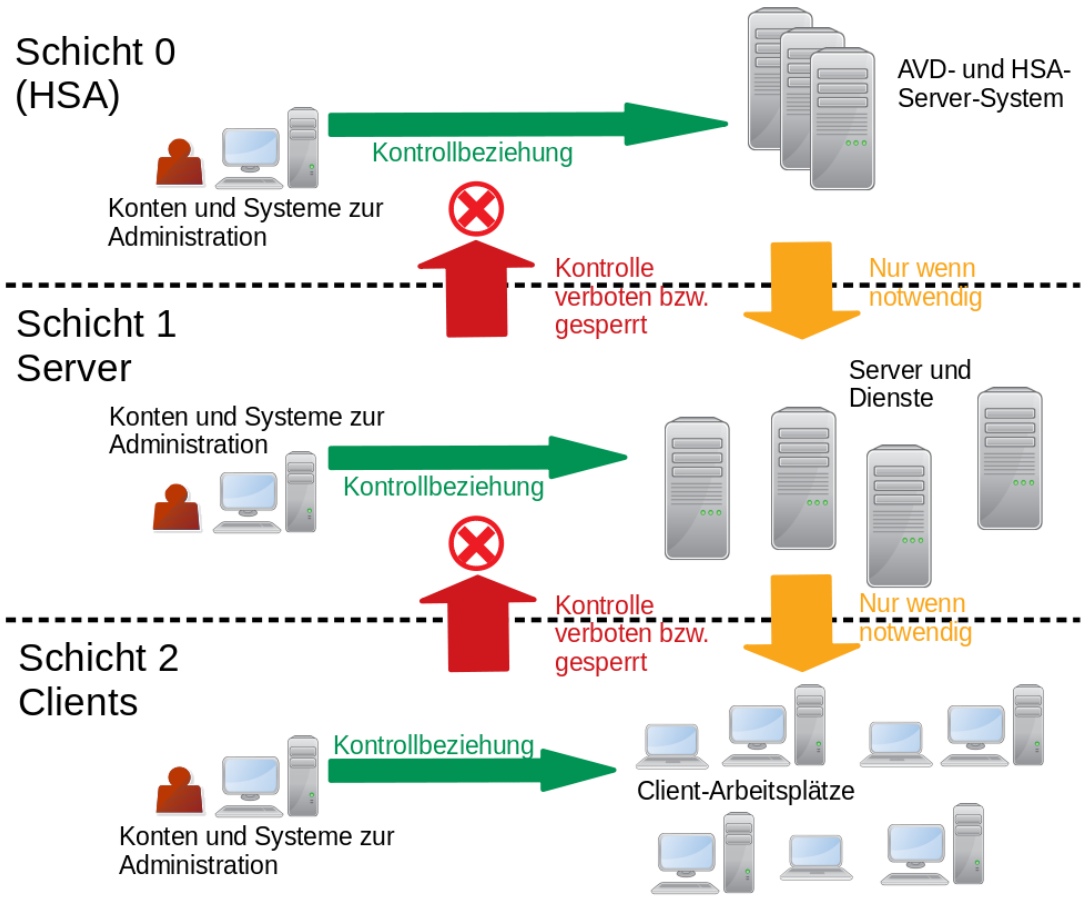
Abbildung 4.4: Mögliche Abhängigkeiten der Sicherheitsschichten

Administrators zugreifen und erhält damit indirekt Zugriff auf das AVD-System und somit auch indirekt, aufgrund der Rechte eines AVD-Administrators, Zugriff auf alle Objekte, die von diesem AVD-System kontrolliert werden. Dieses Beispiel zeigt, dass es von grundlegender Bedeutung ist, die Elemente, die Sicherheitsabhängigkeiten mit dem zentralen AVD-System besitzen, abzugrenzen und deren Anzahl möglichst zu beschränken.

Abbildung 4.4 verdeutlicht bereits die Abstraktion der einzelnen Systemkomponenten in separate Bereiche. Dabei gilt, die Zugriffe in aufsteigender Richtung werden durch definierte Protokolle limitiert. Die Kontrolle von Systemen unterhalb einer Schicht ist eingeschränkt möglich. Eine Anmeldung an Systemen in absteigender Richtung wird jedoch durch technische und organisatorische Maßnahmen verhindert. Lediglich die Zugriffe innerhalb eines Bereichs bleiben unbeschränkt.

Einführung eines 3-Schichten-Modells

Seit einigen Jahren empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) ebenso wie die Microsoft Corporation (MS) die Einführung einer hierarchischen Struktur für den Betrieb von Domänen. Das BSI bezeichnet die Strukturierung einer Domäne als Schichtenmodell[3]. Die Verwendung eines Schichtenmodells mit struktureller Trennung in drei Bereiche ist für eine hochsichere Administrationsumgebung Voraussetzung. Die HSA bildet die Administrationsumgebung der Serversysteme (u. a. Domain Controller), die in Schicht 0 des Strukturmodells angeordnet sind (siehe Abbildung 4.5, oberste Schicht). Eine Präzisierung der Komponenten, die in Schicht 0 einzuordnen sind, erfolgt in Abschnitt 5.3 auf Seite 109. Alle anderen Serverdienste und deren Administrationsumgebung werden in Schicht 1 zusammengefasst. Die Menge aller normalen Arbeitsstationen mit Internetzugang (PCs, Laptops, Tablets usw.) und die entsprechenden Anmeldekonten bilden die Schicht 2.



Quelle: In Anlehnung an [Microsoft, 2019b, Kontrollbereiche]

Abbildung 4.5: Kommunikations- und Kontrollbeziehungen zwischen den Schichten

[3]MS Synonym hierfür: Tier-Modell. Die Bedeutung / Struktur ist identisch.

Zugriffsregeln – basierend auf der Implementierung von TOM – sorgen dafür, dass die Kommunikation innerhalb einer Schicht (horizontal) und zwischen den Schichten (vertikal) auf das unbedingt Notwendige begrenzt ist. Diese Beziehungen werden in Abbildung 4.5 verdeutlicht. Eine Kernforderung hierbei ist: Ein administrativer Zugriff vertikal über die Schichtgrenzen hinweg ist **nicht** möglich.

Äquivalenz zur Schicht 0

Grundsätzlich sollten in der Schicht 0, neben den primär als kritisch anzusehenden Domain Controllern, alle dazu in einer direkten Sicherheitsabhängigkeit stehenden Objekte angesiedelt werden. Gemäß dem in Abschnitt 4.1 erläuterten Prinzip der vertrauenswürdigen Quelle, betrifft dies insbesondere die technischen Systeme und logischen Komponenten, die zur Administration dieser Serversysteme notwendig sind. Hier müssen auch alle Abhängigkeiten, die sich aus dem Betrieb moderner Rechenzentren ergeben – wie in Abschnitt 2.3 dargestellt – berücksichtigt werden.
Zu beachten sind hier grundlegend folgende Serversysteme und Adminstrationskomponenten: [siehe Microsoft, 2019b]

- PKI-Systeme, insofern sie Zertifikate für Domain Controller ausstellen,
- Datensicherungssysteme, wenn sie Datensicherungen für Domain Controller speichern,
- allgemeine Zugangssysteme, wenn dadurch ein Zugang zu Domain Controllern – auch in physischer Art und Weise – ermöglicht wird,
- Update Systeme für Schicht-0-Systeme,
- eine eventuell vorhandene Virtualisierungsumgebung für Serversysteme der Schicht 0 sowie
- Arbeitsstationen und Benutzerkonten, die zur Administration der Schicht-0-Systeme benutzt werden.

Die Microsoft Corporation stellt hierzu fest, dass Institutionen an dieser Stelle oft übersehen, dass eine Vielzahl von Berechtigungsgruppen innerhalb einer typischen AVD-Umgebung auch indirekt über Berechtigungen verfügt, die ein äquivalent zur Schicht 0 darstellen. Diese Gruppen bieten einen recht einfachen Eskalationspfad für Angreifer, um über verschiedene Angriffsmethoden auf dieselben expliziten Berechtigungen der Schicht 0 zuzugreifen. [Microsoft, 2019b] Ein Serveroperator könnte z. B. Zugang zum Sicherungsmedium eines Domain Controllers erhalten und alle Anmeldeinformationen aus den Dateien auf diesem Medium abrufen, um diese zur Ausweitung von Berechtigungen zu nutzen. Institutionen sollten die Mitgliedschaft in allen Gruppen der Schicht 0 (einschließlich geschachtelter Mitgliedschaften) daher kontrollieren und überwachen.

Die Gruppen, die indirekt, teils über weitere Schachtelung, diese Art von Zugriff erlauben, werden als Schicht 0 äquivalente Gruppen bezeichnet (Tier-0-Äquivalenz) und sind in Tabelle 4.2 dargestellt.

Tabelle 4.2: Schicht 0 äquivalente Gruppen

Gruppenname	Gruppentyp	Beschreibung
Organisations-Admins	Universal	Admins der Organisation
Domänen-Admins	Global	Admins der Domäne
Schema-Admin	Universal	Admins des Schemas
BUILTIN\Administrators	Local (in Domäne)	Vollzugriff auf dem DC
BUILTIN\Konten-Operatoren	Local (in Domäne)	Verwaltung von Domänenbenutzern und -gruppen
BUILTIN\Sicherungs-operatoren	Local (in Domäne)	Vollzugriff auf DC Sicherungen
BUILTIN\Druck-Operatoren	Local (in Domäne)	Verwalten auf DC installierte Drucker
BUILTIN\Server-Operatoren	Local (in Domäne)	Verwalten DC
Domänencontroller	Global	Alle DC der Domäne
Schreibgeschütze Domänencontroller	Global	Alle schreibgeschützen DC der Domäne
Richtlinien-Ersteller-Besitzer	Global	Können GPO in der Domäne ändern
BUILTIN\Kryptografie-Operatoren	Local (in Domäne)	Können kryptographische Vorgänge ausführen

Quelle: In Anlehnung an [Microsoft, 2019b]

Die Administrationsumgebung der Schicht 0 (HSA)

Die System-Umgebung, mit der die Administration der in der Schicht 0 befindlichen Server-Systeme erfolgt, wird aufgrund der Kritikalität der betrachteten Systeme in dieser Arbeit als hochsichere Administrationsumgebung (HSA) bezeichnet. Sie besteht unter Einbeziehung der im vorigen Abschnitt gemachten Überlegungen aus folgenden Systembestandteilen:

- Dedizierte, gehärtete Arbeitsstationen zur Administration von Schicht-0-Systemen,
- Benutzerkonten, die ausschließlich zur Administration genutzt werden,

- ggf. gesonderte Virtualisierungsumgebung für Server-Systeme der Schicht 0,
- gesonderte Datensicherungssysteme für Schicht-0-Systeme,
- ggf. Zugangssysteme für Server und Arbeitsstationen der Schicht 0,
- gesonderte Updateserver für Schicht-0-Systeme und
- spezielle Gruppenrichtlinien für Benutzerkonten und Arbeitsstationen der Schicht 0.

Die Arbeitsplatz-PCs, die zur Administration der Schicht-0-Server-Systeme benutzt werden, müssen mit speziellen Richtlinien versehen sein, da auf diesen Systemen mit Berechtigungen der höchsten Sicherheitsebene gearbeitet wird.[4]

4.3 Strategien der Berechtigungsminimierung (Credential Partitioning)

Ein Berechtigungsnachweis (credential) stellt innerhalb einer AVD-Umgebung ein zentrales Datenobjekt dar. Er besteht aus einer logischen Identität, wie in Abschnitt 2.4 beschrieben, und einem dazugehörigem Identitätsnachweis, in AVD-Systemen meist ein Kennwort. Ein Berechtigungsnachweis dient der Authentifizierung und Autorisierung an einem IT-System. Dieser Prozess wird als Benutzerlogon bezeichnet. Der Berechtigungsnachweis wird dementsprechend meist als Benutzerlogin bezeichnet, der im Rahmen der Authentifizierung einem Benutzerkonto zugeordnet wird. In der Praxis wird bzw. sollte in einer Institution grundsätzlich jedem Mitarbeiter ein Benutzerkonto innerhalb einer AVD-Umgebung zugeordnet sein. Da Aktivitäten innerhalb von IT-Systemen meist mit Bezug auf ein Benutzerkonto in Ereignisprotokolle (Logs) geschrieben werden, ist es aus Gründen der sicherheitstechnischen Nachvollziehbarkeit für Institutionen ratsam, grundsätzlich personalisierte Benutzerkonten zu verwenden. Dadurch können IT-Vorgänge möglichst eindeutig einer realen Person zugeordnet werden.[5] In einem AVD-System existieren in der Praxis jedoch auch Konten – hier zu nennen sind vor allem Dienstkonten (Service Accounts) – die genau diesem Grundsatz widersprechen. Diese Art von Konten ist technisch notwendig, deren Anzahl sollte jedoch auf ein Minimum beschränkt werden.

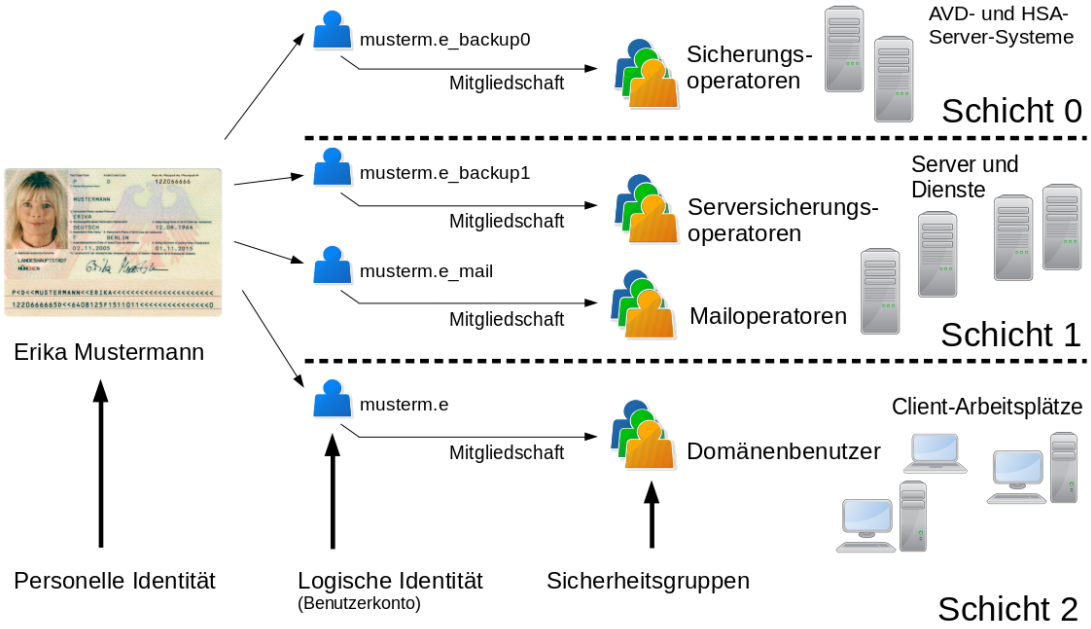
[4] MS bezeichnet diese Arbeitsstationen mit privilegiertem Zugriff als *Privileged Access Workstations* (PAW). Eine entsprechende Konfiguration wird seitens MS empfohlen. [siehe Microsoft, 2019c]

[5] Das BSI empfiehlt die Implementierung eines Identitätsmanagements, mit dessen Hilfe Zugriffe und Berechtigungen geregelt werden. Darin sollten Benutzer und IT-Komponenten zweifelsfrei identifiziert und authentisiert werden. [siehe BSI, 2019b, Modul ORP.5]

Berechtigungsaufteilung

Grundsätzlich wäre es möglich, alle Arbeiten an einem IT-System mit einem einzigen Benutzerkonto durchzuführen, wenn dieses mit allen nötigen Berechtigungen für die zu bewältigenden Aufgaben versehen ist. Ein Beispiel hierfür ist das grundsätzlich existierende Administratorkonto einer MS Domäne (der BUILTIN\Administrator auf den DC-Systemen). Wenn bei der Installation / Konfiguration nicht manuell geändert, verfügt dieses Benutzerkonto über alle denkbaren Berechtigungen innerhalb der gesamten AVD-Struktur, auf allen Computersystemen innerhalb dieser Struktur, mit Zugriff auf alle gespeicherten Daten.

Gerade vor dem Hintergrund der in Kapitel 3 beschriebenen Angriffsverfahren, wie beispielsweise Pass-the-Hash, ist diese Art der Berechtigungsvergabe prinzipiell ungeeignet. Ein wirkungsvolles Vorgehen gegenüber jeder Art von Identitätsübernahme ist die Aufteilung der Berechtigungen auf verschiedene Anmeldekonten, die jeweils nur für einen konkreten Zweck eingesetzt werden. Die Aufteilung möglicher oder notwendiger Berechtigungen auf mehrere Identitäten wird als Berechtigungsaufteilung (engl. Credential Partitioning) bezeichnet.



Quelle: Eigene Darstellung

Abbildung 4.6: Beispiel einer Berechtigungsaufteilung auf mehrere Konten

Ein Beispiel für eine wirksame Berechtigungsaufteilung ist in Abbildung 4.6 dargestellt. In diesem Beispiel hat eine Mitarbeiterin einer Institution mehrere Aufgaben innerhalb der IT-Umgebung zu bewältigen, die teils in unterschiedlichen Schichten des im vorherhigen Abschnitt vorgestellten Schichtenmodells anzusiedeln sind. Um

eine Rechte-Eskalation während eines APT-Angriffs wirksam zu verhindern, sind die Aufgaben möglichst granular aufgeteilt. Im konkreten Beispiel übernimmt die Mitarbeiterin Frau Mustermann die Aufgabe der System-Datensicherung und der E-Mail-Administration. Wie der Tabelle 4.2 zu entnehmen ist, ist die Gruppe Sicherungsoperatoren[6] eine Schicht 0 äquivalente Gruppe. Da Frau Mustermann, ihrer Aufgabe entsprechend, gleichzeitig auch für die Datensicherung von weiteren Servern zuständig ist, ist sie zusätzlich mit einer weiteren Identität Mitglied in einer Gruppe mit Berechtigung für die Server-Datensicherung. Für die Aufgabe der E-Mail-Administration, die funktional eindeutig von der Datensicherung zu trennen ist, benutzt Frau Mustermann eine weitere Identität, die durch die Mitgliedschaft in der Gruppe der E-Mail-Administratoren auf den E-Mail-Servern über entsprechende Rechte verfügt. Ihre weiteren IT-Tätigkeiten, die eventuell mit Internetaktivitäten verbunden sind, erledigt sie mit einer grundlegenden, personifizierten Benutzeridentität ohne weitere Systemrechte.

Aufteilung von Berechtigungen auf verschiedene Arbeitsstationen

Generell ist auch eine Aufteilung der Berechtigungen auf unterschiedliche Arbeitsstationen sinnvoll. Innerhalb der Abgrenzung von Aufgaben seitens der Mitarbeiter in unterschiedlichen Schichten des Schichtenmodells ist die Aufteilung der Arbeit an unterschiedlichen Arbeitsstationen sogar ein Muss. Die Aufteilung der Arbeiten, die innerhalb einer Sicherheitsschicht stattfinden, auf unterschiedliche Arbeitsstationen bleibt abzuwägen. Nach bisherigen Einschätzungen – auch seitens des BSI[7] und der Microsoft Corporation – kann eine Aufteilung auf verschiedene Arbeitstationen in Form einer Virtualisierung erfolgen. Damit wäre es möglich, auf einer Host-Arbeitsstation unterschiedliche virtualisierte Arbeitstationen zu betreiben, um dadurch Ressourcen in Form von Kosten und Platz zu sparen. Bei der Betrachtung sind die unterschiedlichen Sicherheitsschichten der Arbeitsstationen relevant. Die Sicherheitsschicht der realen Host-Arbeitsstation muss der höchsten Sicherheitsschicht der darauf virtualisierten Arbeitsstationen entsprechen. Eine Arbeitsstation der Schicht-0-Sicherheitsebene sollte jedoch ausnahmslos separat betrieben werden. Grundsätzlich sind bei Überlegungen zur Virtualisierung von Systemen unterschiedlicher Sicherheitsschichten auf einem Host-System aktuelle Sicherheitsprobleme, wie Meltdown und Spectre [siehe Lipp et al., 2018] zu beachten. Gegebenenfalls ist hier in der Zukunft eine neue Einordnung der sicherheitstechnischen Abgrenzung von Virtualisierung nötig.

[6] In einer MS-Domäne sind die in Tabelle 4.2 angegebenen Gruppen grundsätzlich immer vorhanden, es sei denn, sie wurden bewusst gelöscht.

[7] Unter Beachtung der Grundschutzkomponente B 3.304 Virtualisierung [siehe BSI, 2011a].

4.4 Authentifizierungsabsicherung

Wie in Abschnitt 3.4 erläutert, bieten Authentifizierungsverfahren Schwachstellen, die von Angreifern im Rahmen eines APT-Angriffs ausgenutzt werden. In Abschnitt 3.4.2 werden Pass-the-Hash-Angriffe beschrieben, mit denen ein Angreifer diese Schwächen ausnutzen kann, um sich im internen Netz einer Institution unbemerkt zu bewegen. Um diesem Sachverhalt entgegenzuwirken, ist es sinnvoll, die Authentifizierungsvorgänge innerhalb der AVD-Umgebung weiter abzusichern. So kann eine Authentifizierungsabsicherung durch die Einführung einer Multi-Faktor-Authentifizierung (MFA) erfolgen. In diesem Bereich sind eine Vielzahl von technischen Lösungen verfügbar. Einige davon wurden im Kapitel Grundlagen in Abschnitt 2.4.1 dargestellt. Auf alle Verfahren einzugehen, würde den Rahmen dieser Arbeit sprengen.[8]

Zwei-Faktor-Authentifizierung (2FA) mittels Smartcard

Eine Smartcard-Anmeldung wird in die Kategorie der Zwei-Faktor-Authentifizierung (2FA) eingeordnet, da es zum einen den Besitz einer Smartcard und zum anderen die Kenntnis einer PIN verlangt. Grundsätzlich verlangt ein Authentifizierungsverfahren mittels Smartcard gleichzeitig den Einsatz einer PKI-Infrastruktur (Public Key Infrastruktur) innerhalb der AVD-Umgebung, da zur Authentifizierung mit einer Smartcard X.509v3 Zertifikate [siehe Gutmann, 2000] benötigt werden. Der private Schlüssel eines der Smartcard zugeordneten Zertifikats wird dabei im geschützen Schlüsselspeicher auf der Smartcard abgespeichert. Zur Authentifizierung wird der private Schlüssel auf der Smartcard ausgelesen. Dies geschieht unter der Voraussetzung, dass beim Abruf des Zertifikats die korrekte PIN eingegeben wurde. In diesem Anwendungsgebiet empfiehlt sich der Einsatz von Smartcards mit kryptografischen Fähigkeiten, die meist mit eigenem Prozessor, geschütztem Speicher und eigenem Betriebssystem ausgestattet sind.

Authentication mechanism assurance (AMA)

Grundsätzlich beschreibt eine Authentifizierungsabsicherung mittels AMA-Verfahren eine Funktionalität innerhalb des Kerberos Authentifizierungsprozesses. Das Kerberos Key Distribution Center (KDC) bietet in diesem Szenario die Möglichkeit, eine Authentifizierung unterschiedlich zu handhaben, basierend auf dem Typ des präsentierten Authentikators. Der Einsatz dieser Technologie ist nur in Verbindung mit zertifikatsbasierter Anmeldung sinnvoll umsetzbar. Bisher bietet nur die Microsoft Corporation

[8] MS empfiehlt für den Bereich der Schicht-0-Absicherung und im Rahmen des Aufbaus einer hochsicheren Administrationsumgebung (HSA) eine Authentifizierungsabsicherung durch Einführung eines smartcardbasierten Authentifizierungsverfahrens.

(MS) im Rahmen des Produktes Active Directory® eine konkrete Umsetzung dieses Verfahrens an.

Microsoft AMA-Implementierung

Wird das Anmeldeverfahren mittels Smartcard im Rahmen einer Kerberos-Authentifizierung an einem MS Kerberos Key Distribution Center (KDC) benutzt, ist eine Authentifizierungsabsicherung (AMA) möglich. MS hat hierzu ein spezielles Absicherungsverfahren entwickelt, das ab MS Windows Server® 2008 R2 als *Authentication Mechanism Assurance for AD DS (MS-AMA)* bekannt ist. [siehe Microsoft, 2012] Gerade im Hinblick auf die Absicherung einer hochsicheren Umgebung als Form einer Schicht-0-Administrationsumgebung ist die Implementierung dieses Verfahrens mit einem hohen Grad der Absicherung gegen Pass-the-Hash-Angriffe verbunden. Bei diesem Verfahren prüft das KDC bei einer Authentifizierungsanfrage zusätzlich die Art des Authentikators, der bei der Anfrage verwendet wird: Erfolgt eine Anfrage mit Benutzername/Kennwort (kennwortbasiert) oder erfolgt eine Anfrage durch Präsentation eines Zertifikats mit gültigem Schlüssel (smartcardbasiert). Je nach Art der Authentifizierungsanfrage wird ein gesondertes Kerberos Ticket Granting Ticket (TGT) erzeugt, das jetzt nicht nur zur Authentifizierung genutzt werden kann, sondern gleichzeitig auch Autorisierungsinformationen enthält, die in Abhängigkeit vom Authentikator gesetzt werden. Die proprietäre Lösung von MS benutzt dabei ein spezielles Datenfeld des Kerberos TGT, welches als *Microsoft Privilege Attribute Certificate Data Structur* (MS-PAC)[9] bezeichnet wird. Innerhalb dieses Datenbereichs eines TGTs, das von einem MS Domain Controller erzeugt wird, befinden sich zusätzliche Daten zu Gruppenzugehörigkeiten des erfolgreich authentifizierten Benutzers.

Im Rahmen des MS-AMA-Verfahrens können vom Domain Controller unterschiedliche Gruppenzugehörigkeiten innerhalb des TGT an den Client zurückgemeldet werden. Die genaue Zuordnung von Gruppen, die bei einer smartcardbasierten Anmeldung übergeben werden, wird im Verzeichnis (in diesem Fall Active Directory®), in der Systempartition festgelegt. Dort werden Object Identifiers (OIDs) definiert, die mit entsprechenden Zertifikatsvorlagen und indirekt mit entsprechenden Sicherheitsgruppen verknüpft sind. Im Auslieferungszustand eines Microsoft Corporation (MS) Active Directory® existieren hierfür die in Tabelle 4.3 angegeben Richtlinien und entsprechende Sicherheitsgruppen. Dieses Zuordnungssystem ist mit eigenen OID-Koordinaten und Gruppen beliebig erweiterungsfähig.

[9] Die proprietäre Protokollerweiterung des standardisierten Kerberos Protokolls wurde von MS im Rahmen der *Open Specifications* Initiative veröffentlicht.
Quelle: `https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-pac/`

Tabelle 4.3: Richtliniensystem für das MS-AMA-Verfahren

OID Bezeichner	Richtlinienbezeichner
OID 1.3.6.1.4.1.311.21.8.-DomainSID-.400	niedrige Zusicherung
OID 1.3.6.1.4.1.311.21.8.-DomainSID-.401	mittlere Zusicherung
OID 1.3.6.1.4.1.311.21.8.-DomainSID-.402	hohe Zusicherung

Quelle: Microsoft Corporation Active Directory®

Die Konfiguration erfolgt dabei in der Konfigurations-Partition des Verzeichnisdienstes. Dort wird eine entsprechende Zertifikatsvorlage generiert, für die eine Zertifikatsrichtlinie mit passendem OID-Bezeichner (nach Tabelle 4.3) konfiguriert ist. In dieser Konfiguration verweist das Objekt-Attribut *msDS-OIDToGroupLink* auf eine entsprechende Sicherheitsgruppe, die letztendlich mit den Rechten ausgestattet ist, die für die vorgesehene Sicherheitsschicht benötigt werden.

Grundsätzlich ist es mithilfe des MS-AMA-Verfahrens möglich, einer Benutzeranmeldung unterschiedliche Berechtigungen, dynamisch – das bedeutet, in Abhängigkeit des präsentierten Authentikators und bei jedem einzelnen Anmeldeprozess neu geprüft – zuzuordnen. Dieser Prozess kann dazu genutzt werden, ein mit hoher Berechtigung versehenes Benutzerkonto zusätzlich abzusichern, indem die eigentliche, kritische Berechtigung beispielsweise mit einer der in Tabelle 4.3 dargestellten Gruppen verknüpft wird. In der angemeldeten Sitzung ist diese Berechtigung dann nur verfügbar, wenn die Authentifizierung mit einer zugeordneten Smartcard, auf der ein Zertifikat gespeichert ist, welches den entsprechenden OID-Schlüssel enthält, durchgeführt wurde. Erfolgt die Anmeldung am System lediglich mit Benutzername und Kennwort, ist die Berechtigung nicht vorhanden. Dieses Verfahren ist damit grundsätzlich gut geeignet, wirksam gegen Pass-The-Hash-Angriffe eingesetzt zu werden, da die Berechtigung für kritische Systeme, wie Systeme der Schicht 0, an den Besitz der Smartcard gekoppelt werden kann.

Einschränkungen der Authentifizierungsabsicherung

Da das beschriebene Verfahren an die Autorisierungsinformation im MS-PAC-Datenfeld eines Kerberos TGT gebunden ist, müssen entsprechende Berechtigungen und Rollenfunktionen diese Information auch auswerten. Autorisierungsprozesse, die Berechtigungen durch statische Gruppenzuordnung im Verzeichnisdienst ermitteln, können durch das MS-AMA-Verfahren nicht abgesichert werden.

Die oben beschriebenen Verfahren basieren grundsätzlich auf dem Kerberos Authentifizierungsprotokoll. Innerhalb einer MS-basierten AVD-Struktur wird aus Gründen der

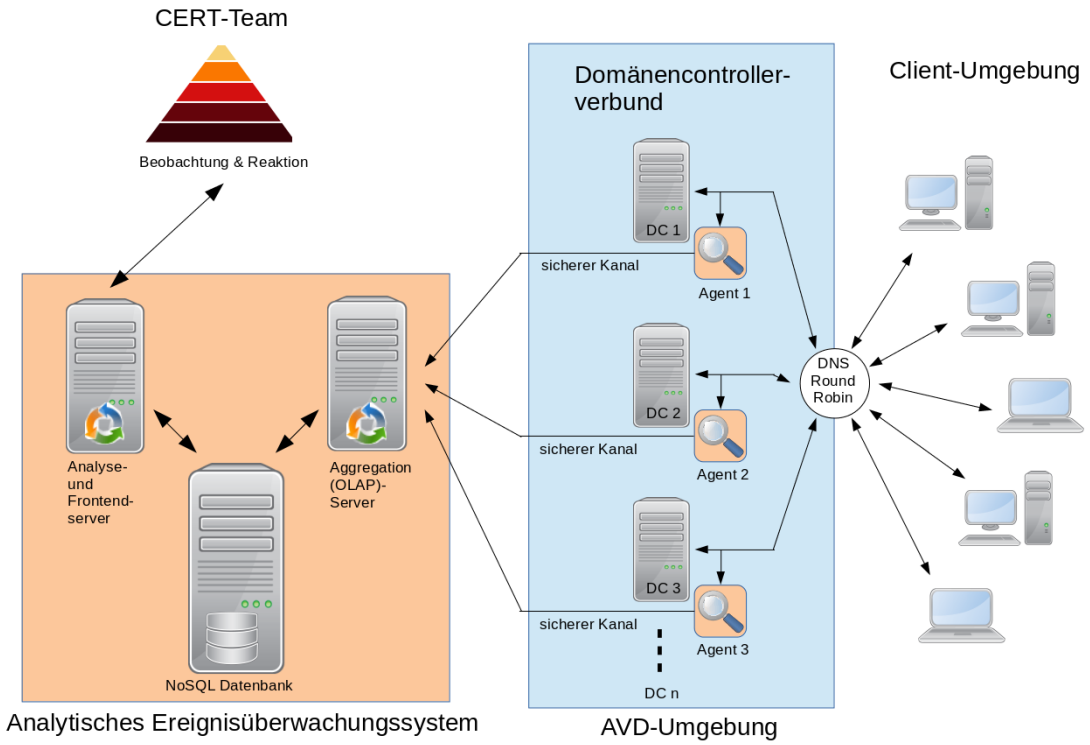
Abwärtskompatibilität – und wenn nicht anders konfiguriert – weiterhin auf ein funktionsfähiges NTLM-Authentifizierungsverfahren gesetzt. Dies bedingt, dass in einer laufenden Session ein Kennwort-Hash verfügbar sein muss, um alle Anforderungen im Sinne des Single Sign-on (SSO) Verfahrens zu erfüllen. Wäre dies nicht der Fall, müsste der Benutzer bei jedem einzelnen – auch im Hintergrund des Arbeitsprozesses ablaufenden – Authentifizierungsprozess mittels NTLM, sein Kennwort neu eingeben. Aus diesem Grund wird bei einer Anmeldung, die eigentlich mithilfe des Kerberos Protokolls erfolgte, selbst wenn diese wie oben beschrieben abgesichert wird, im normalen Betrieb der Kennwort-Hash im Rahmen der TGT-Übermittlung an den Client übertragen. Er liegt also weiterhin für den Angreifer verfügbar, im Speicher des Clients, von dem die Anmeldung erfolgte. Die Microsoft Corporation bietet für diese Problematik eine Lösung in Form einer speziellen Sicherheitsgruppe (Protected User Group). Ist ein Benutzerkonto Mitglied dieser Gruppe, wird die oben beschriebene Kennwort-Hash-Übermittlung nicht durchgeführt. Die Benutzung dieser Gruppe wird für sicherheitskritische Berechtigungen seitens MS dringend empfohlen. Gleichzeitig ist seitens der Institution zu prüfen, ob bei Benutzung dieser Gruppe noch alle erforderlichen Tätigkeiten durchführbar sind, da das NTLM-Authentifizierungsverfahren – wie oben beschrieben – nicht mehr verfügbar ist, wenn ein Benutzer Mitglied dieser Gruppe ist.

4.5 Analytische Ereignisüberwachung

In diesem Abschnitt wird eine Strategie vorgestellt, die nicht direkt mit der Absicherung einer in der Schicht 0 befindlichen, hochsicheren Administrationsumgebung verbunden wird. Die Strategie der analytischen Ereignisüberwachung kann jedoch durch frühzeitige Erkennung von Vorgängen, die auf einen APT-Angriff hindeuten, zur indirekten Absicherung der Schicht-0-Systeme beitragen, indem ein möglicher Angriff bereits in der Exploitation Phase detektiert werden kann und entsprechende Gegenmaßnahmen, wie Abschottung, Deaktivierung oder Neuinstallationen von kompromittierten Systemen eingeleitet werden können. Im speziellen Fokus stehen hier alle Datenflüsse, die seitens der Client- und Serversysteme an die AVD-Systeme gerichtet werden und von ihrer Art und Weise her nicht den Standardabfragen entsprechen. Man spricht in diesem Bereich daher auch von verhaltensorientierter Ereignisüberwachung. Ein entsprechendes, lernfähiges System wird von Ghafir et al. als Machine-Learning APT Correlation Analysis (MLAPT) bezeichnet und grundlegend beschrieben. [siehe Ghafir et al., 2018]

Strukturaufbau einer AVD-Ereignisüberwachung

Um die entsprechenden Ereignisse erfolgreich und unverfälscht aufzeichnen zu können, ist ein mehrstufiges Verfahren notwendig, wie in Abbildung 4.7 dargestellt und im Folgenden kurz erläutert.



Quelle: Eigene Darstellung unter Verwendung von Ressourcen von smashicons.com

Abbildung 4.7: Beispiel der Struktur eines Ereignisüberwachungssystems

Ein AVD-System besteht, gerade bei größeren Institutionen, aus mehreren Domain Controllern. Sie bilden ein verteiltes System, wie in Abschnitt 2.4.3 grundlegend erläutert. Die gleichmäßige Verteilung der Authentifizierungs- und Verzeichnisdienstanfragen seitens der Clients erfolgt meist durch ein DNS-Round-Robin-Verfahren. Um alle Vorgänge erfolgreich zu registrieren, sind in der ersten Stufe Agenten notwendig, die auf allen an dem Round-Robin-Verfahren beteiligten Systemen die entsprechenden Netzwerkschnittstellen abhören. Die Agenten können hostseitig auf den jeweiligen Domain Controllern installiert werden. Aus sicherheitstechnischer Sicht empfiehlt sich jedoch der Einsatz von sogenannten *Netzwerksonden* (network probes), physikalisch eigenständig realisierte Agenten, die über einen netzwerkseitigen Spiegelport auf Schicht 2 des ISO/OSI Modells den Datenverkehr vom und zum DC aufzeichnen. Diese Variante hat den Vorteil, dass sie physikalisch unabhängig von Domain Controllern arbeitet. Netzwerksonden können nicht im Zusammenhang mit einem DC kompromittiert werden. Sie sind auch für einen Angreifer in dieser Form nicht sichtbar. Es

empfiehlt sich bei Einsatz von Netzwerksonden, diese einer gesonderten Sicherheitsebene zuzuordnen. Nachteilig an, physikalisch von DCs separierten, Agenten ist der Umstand, dass in der Regel der gesamte Datenverkehr von und zu einem DC verschlüsselt abläuft. Ein auf dem DC-Host installierter Agent zeichnet den Datenverkehr mit, in dem er sich in den IP-Protokollstack oberhalb der Verschlüsselung, in der Anwendungsebene des ISO/OSI Modells einbringt. Ein als Netzwerksonde aufgebauter, vom DC getrennt arbeitender, Agent muss den verschlüsselten Datenverkehr entschlüsseln können.

In der zweiten Stufe müssen die gesammelten Daten einer Aggregation unterzogen werden. AVD-Systeme, gerade bei größeren Institutionen, müssen teils mehrere hundert Anfragen pro Sekunde verarbeiten. Die Aufzeichnung des gesamten Datenverkehrs würde ein Ereignisspeichersystem bezüglich der Speicherfähigkeit überlasten. Im Rahmen der Aggregation werden aus den aufgezeichneten Prozessdaten der Authentifizierungs- und Verzeichnisdienstanfragen daher Metadaten gebildet, die nur die für die verhaltensorientierte Ereignisanalyse notwendigen Daten beinhalten. Die Aggregation kann bereits im Agenten erfolgen oder in einer gesonderten Kollektor-Instanz.

In der dritten Stufe werden die Metadaten in einer zentralen Datenbank gespeichert. Zum Einsatz kommen in diesem Bereich aufgrund der hohen Datenmengen typischerweise strukturierte Datenspeicher, die horizontal skalieren und einen nicht-relationalen Ansatz verfolgen[10]. Verbunden mit dem Datenbankspeicher ist in dieser Stufe auch die „zentrale Intelligenz“. Diese verwendet ein umfangreiches Regelwerk, um Auffälligkeiten in den gespeicherten Metadaten zu finden.

Überwachungsprinzipien bei APT-Angriffen

Die Überwachung der Authentifizierungsvorgänge erfolgt im Hinblick auf die Art und Weise der Anmeldung. Dabei sind folgende Fragestellungen signifikant:

- Welche Arbeitsstation wird zur Anmeldung verwendet?
- Wann erfolgt die Anmeldung?
- Anmeldung eventuell in Zeiträumen der Abwesenheit des Mitarbeiters (Urlaub, Krankheit)?
- Welches Authentifizierungsverfahren und welche Verschlüsselungsart wird verwendet?

[10] Typische NoSQL Datenbanken, wie Mongo-DB oder ein ELK-Stack, bestehend aus Elasticsearch, Logstash und Kibana

Um eine analytische Ereignisüberwachung aufzubauen, die diese Fragestellungen beantworten kann, ist in der Regel ein Lernprozess notwendig. In einer Trainingsphase muss „erlernt“ werden, welche Art von Ereignissen zum Normalzustand gehören. Es wird dadurch der sogenannte Grundzustand (Baseline) ermittelt. Im Bereich des Verzeichnisdienstes werden ebenfalls die Art und Weise der Anfragen analysiert. Der Prozess der Bildung des Grundzustandes kann mitunter mehrere Monate andauern. Nach erfolgreicher Feststellung des Grundzustandes können Ereignisse detektiert werden. Mögliche Ereignisse sind in Tabelle 4.4 beispielhaft zusammen mit einer Ereignissklassifizierung dargestellt (Auszug).

Tabelle 4.4: Beispielereignisse eines analytischen Überwachungssystems

Ereigniss	Klassifizierung
Ungewöhnliche Modifizierung von sensiblen Gruppen	Kritisch
Aktivität zur Herabstufung der Verschlüsselung	Warnung
Umfangreiche Objektlöschungen	Warnung
Reconnaissance mithilfe von Verzeichnisdienstabfragen	Warnung
Identitätsdiebstahl mithilfe eines Pass-the-Hash-Angriffs	Kritisch
Berechtigungsausweitung mithilfe von gefälschten Autorisierungsdaten	Kritisch
Reconnaissance über DNS	Warnung
Ungewöhnliche Protokollimplementierung	Warnung
Offengelegte Anmeldeinformationen (keine Verschlüsselung)	Warnung
Verdächtige Authentifizierungsfehler	Warnung
Verdacht des Identitätsdiebstahls aufgrund ungewöhnlichem Verhaltens	Warnung
Reconnaissance mithilfe von Kontoenumeration	Warnung

Quelle: MS Advanced Threat Analytics Handbuch [Microsoft, 2019a]

Die von einem analytischen Überwachungssystem festgestellten Ereignisse sollten von einem Computer Emergency Response Team (CERT) schnellstmöglich überprüft werden. Folgende Klassifikation sind nach einer ordnungsgemäßen Untersuchung der Ereignisse denkbar: [siehe Microsoft, 2019a]

- Richtig positiv: Eine böswillige, vom Überwachungssystem erkannte Aktion ist erfolgt.
- Unbedenklich richtig positiv: Eine vom Überwachungssystem erkannte Aktion, die tatsächlich durchgeführt wurde, aber nicht böswillig ist, wie z. B. ein Penetrationstest.

- Falsch positiv: Ein falscher Alarm, das heißt, die Aktivität wurde nicht ausgeführt.

Überwachung von Köderkomponenten

Im Zusammenhang mit einer analytischen Überwachung können auch speziell für AVD-Systeme eingerichtete Köderobjekte (Honeypot Object) erstellt werden. Beispielweise ist es mitunter sinnvoll, ein gesondertes Konto mit höchster Berechtigungsebene anzulegen[11] und dieses wie vergleichbare Konten zu personifizieren, jedoch nicht zu benutzen. In entsprechenden Ereignisüberwachungssystemen kann ein derartiges Konto speziell nominiert werden. Wird eine Aktion unter Benutzung dieses Köderkontos detektiert, sollte dies unverzüglich von einem CERT überprüft werden.

Datenschutzrechtliche Betrachtung

Die in diesem Abschnitt beschriebenen Maßnahmen stehen teils in direktem Widerspruch zu bestehenden Datenschutzprinzipien. Der Einsatz entsprechend geeigneter Software muss daher bezüglich datenschutzrechtlicher Aspekte innerhalb der Institution abgewogen werden. Hilfreiche Techniken, um den Anforderungen des Datenschutzes beim Einsatz von Ereignisüberwachungssystemen entgegenzukommen, sind in diesem Fall:

- Einsatz des Vier-Augen-Prinzips, beim Zugriff auf personenbezogene Daten,
- frühzeitige Anonymisierung bei der Speicherung der Daten,
- Befristung der Datenspeicherung von personenbezogenen Daten oder
- arbeitsvertragliche Regelungen bezüglich der Ereignisüberwachung.

Seit dem 25. Mai 2018 gelten hierzu folgende Rechtsgrundlagen:

- Die europäischen Datenschutzrichtlinie 95/46/EG,
- vorrangig die Datenschutz-Grundverordnung (DSGVO) in der aktuellen Fassung von 2016 und
- nachrangig das deutsche Bundesdatenschutzgesetzes (BDSG)-neu in der Fassung von 2018.

[11] Dies würde beispielsweise eine Gruppenmitgliedschaft in der Gruppe der Domänenadministratoren erreichen.

5 Detailkonzeption einer hochsicheren Administrationsumgebung (HSA)

Aus Gründen des in Abschnitt 4.1 dargestellten Prinzips der vertrauenswürdigen Quelle ist es angebracht, die Komponenten der HSA zusammen mit den Komponenten der AVD-Umgebung innerhalb des Netzwerk einer Institution von anderen Systemen und Komponenten zu separieren. Das zugrundeliegende Schichtenmodell wurde im Abschnitt 4.2 erläutert. Innerhalb des Schichtenmodells werden diese explizit schützenswerten Objekte[1] in der Schicht 0 (Tier 0) angesiedelt. Wendet man das in Abschnitt 4.1 vorgestellte Prinzip der vertrauenswürdigen Quelle auf alle Sicherheitsabhängigkeiten an, die letztendlich – auch rekursiv / indirekt – zu einem administrativen Zugriff auf Domain Controller führen könnten, erhält man alle Objekte, die in die Schicht 0 verlagert werden müssen. In Abschnitt 5.3 werden die Komponenten einer HSA detailliert vorgestellt. Der Zugriff auf diese Objekte muss durch den Aufbau einer eigenen logischen und mitunter auch physikalischen Struktur innerhalb der IT-Umgebung der Institution abgekoppelt werden.

5.1 Netzwerktopologischer Aufbau

Eine HSA lässt sich netzwerktopologisch auf verschiedene Weise realisieren:

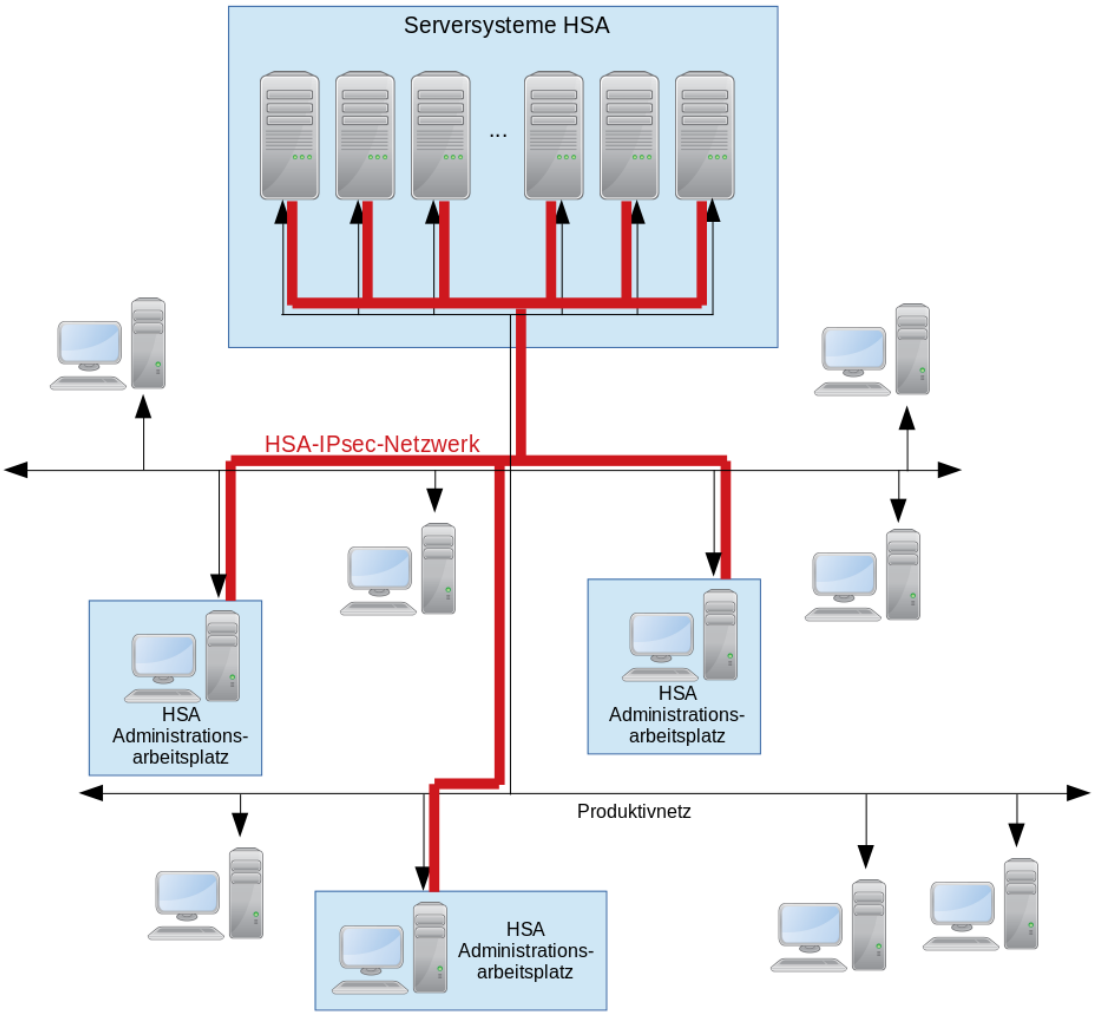
- Im Produktivnetz integriert und mittels IPSEC abgesichert,
- in einer gesonderten Firewall-Zone vom Produktivnetz getrennt oder
- in Form eines eigenen Netzwerkes (VLAN), möglichst getrennt vom Produktivnetz.

Alle drei Varianten werden im Folgenden mit ihren Vor- und Nachteilen kurz vorgestellt. Gleichermaßen gilt bei allen Varianten, die Netzwerkkommunikation zwischen den HSA-Servern und den zur Administration nötigen Arbeitsstationen strikt auf das Nötigste einzuschränken. Datenverkehr von und zum Internet ist generell zu unterbinden. Eine Lösung für Updateprozesse und gewollten Datenimport wird später in diesem Kapitel vorgestellt.

[1] Der Hersteller Microsoft Corporation spricht in seinen Publikationen in diesem Zusammenhang von *assets* (deutsch: in etwa Gegenstand oder Gut.)

HSA mittels IPsec im Produktivnetz

In dieser Variante werden die Server und Arbeitsstationen einer HSA direkt im Produktivnetz eingebunden. Um die nötige Kontrolle über den Netzwerkverkehr innerhalb der HSA zu gewährleisten, wird Internet Protocol Security (IPsec) als Protokoll-Suite zur Absicherung der Kommunikation eingesetzt. Eine schematische Darstellung dieser Variante ist in Abbildung 5.1 erkennbar.



Quelle: Eigene Darstellung

Abbildung 5.1: Struktur einer mittels IPsec abgesicherten HSA im Produktivnetz

Vorteile dieser Variante sind:

- In homogenen Umgebungen mit Betriebssystemen des Herstellers Microsoft Corporation kann IPsec über Gruppenrichtlinienobjekte (GPO) zentral gesteuert werden. Dies mindert den Administrationsaufwand erheblich.
- Die Variante eignet sich besonders für kleinere, homogene Netzwerkumgebungen.

- Wenn IPsec-Regeln implementiert werden können, ist der weitere Aufwand der netzwerktechnischen Realisierung gering, da im bestehenden Produktivnetzwerk gearbeitet wird.
- Die Variante ist gut geeignet bei einem kompletten Neuaufbau einer HSA.

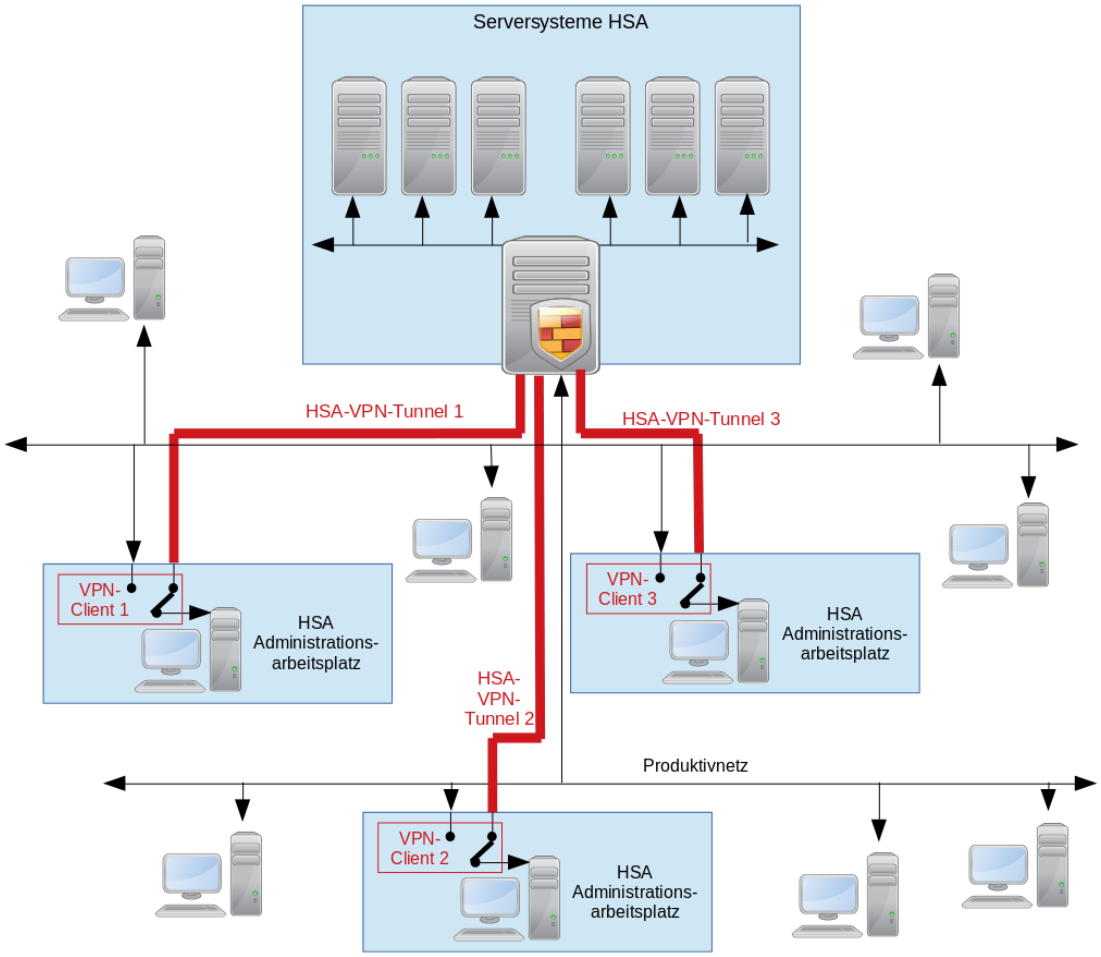
Nachteile dieser Variante sind:

- Sehr komplexe IPsec-Konfiguration in größeren Umgebungen.
- Sie ist in heterogenen Netzwerkumgebungen schwer umsetzbar, da alle direkt beteiligten Kommunikationspartner angepasst werden müssen, um IPsec zu unterstützen.
- Das Produktivnetz verfügt meist über eine Internetkonnektivität. Die Maxime des Offline-Betriebs für alle HSA-Komponenten ist in dieser Umgebung schwer durchzusetzen. Technische und organisatorische Maßnahmen (TOM) sind an einer Vielzahl von Elementen nötig, um die Maxime umzusetzen.

HSA innerhalb einer abgeschotteten Firewall-Zone

In dieser Konzeptvariante werden die Systeme der HSA in einer abgegrenzten Firewall-Zone betrieben, wie in Abbildung 5.2 dargestellt. Die Firewall bildet dabei das zentrale netzwerktechnische Gateway zum restlichen Netzwerk der Institution. Eine derartige Abschottung mittels einer Hardware-Firewall bietet einen zusätzlichen Vorteil: Heutige Hardware Firewalls bieten meist gleichzeitig mit der Fähigkeit, Netzwerkverkehr nach Regeln zu Filtern, zusätzlich eine VPN-Funktionalität. Dabei fungiert die Firewall als das zentrale Tunnelende eines VPN-Tunnels und ein entsprechender Software-VPN-Client auf den entfernten Arbeitsstationen zur Administration als das andere Tunnelende. Diese Funktionalität ermöglicht es, die Serversysteme der HSA in der Firewall-Zone zu betreiben, die zugeordneten Administrationsarbeitsplätze aber im normalen Produktivnetz zu belassen. Diese werden dann mittels eines VPN-Tunnels fest mit der Netzwerkzone der HSA verbunden.[2]

[2]Der Software-VPN-Client sollte dabei derart konfiguriert werden, dass Netzwerkverkehr nicht mehr über die normale physikalische Schnittstelle übermittelt wird, sondern exklusiv über die logische Schnittstelle des VPN-Tunnels.



Quelle: Eigene Darstellung

Abbildung 5.2: Struktur einer HSA in gesonderter Firewall-Zone.

Vorteile dieser Variante:

- Hohe Flexibilität bei der Anbindung der Administrationsarbeitsplätze durch VPN-Technologie.
- Die Lösung bietet erhöhte Sicherheit, wenn die VPN-Technologie mit Smartcard-Authentifizierung verbunden wird.

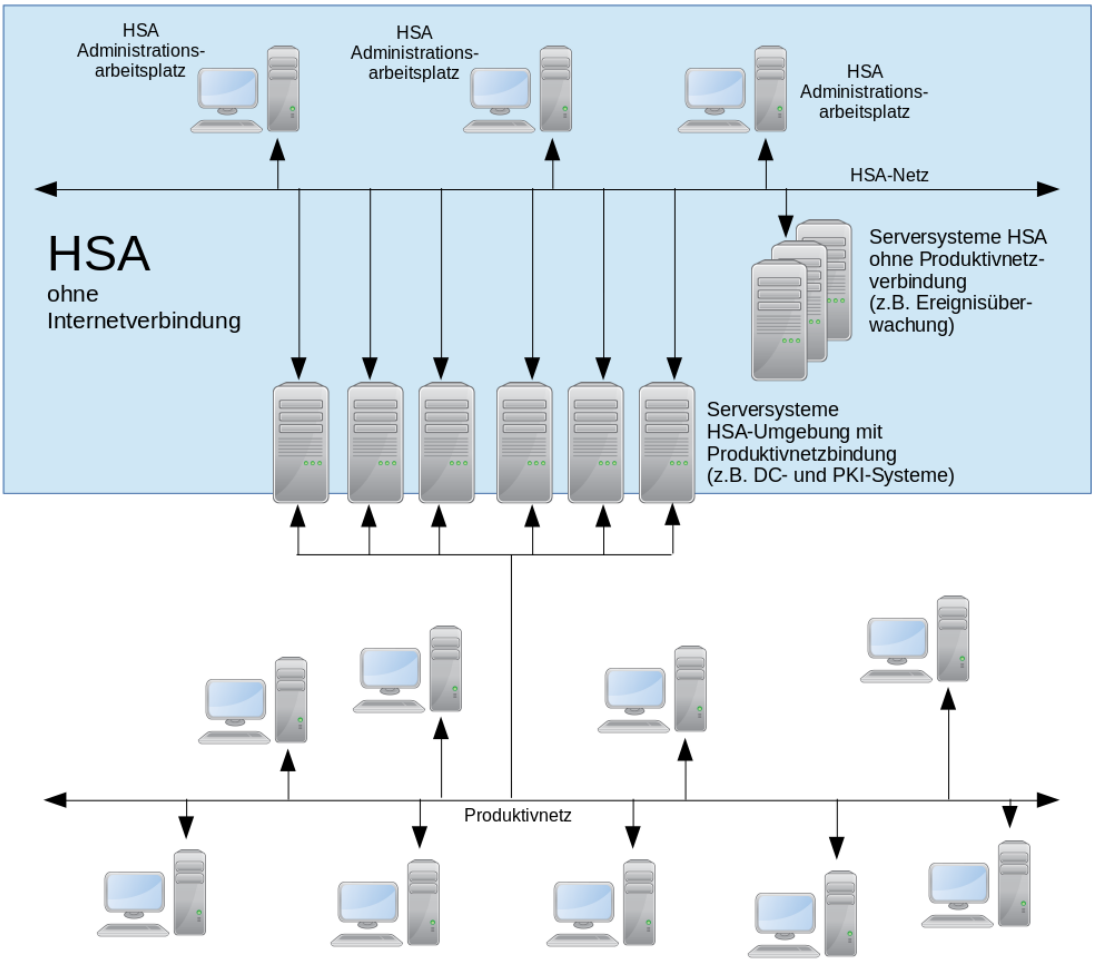
Nachteile dieser Variante:

- Ein erhöhter Administrationsaufwand bei der Konfiguration und Pflege der Firewall-Installation.
- Zusätzliche Firewall-Technologie ist erforderlich.

HSA in einem eigenem LAN oder VLAN

Unter der Annahme, dass VLAN-Zonen bezüglich der Rolle der Netzwerkadministration als sicher gelten, kann in dieser Variante entweder ein physikalisch (LAN) oder logisch getrenntes (VLAN) Netzwerk verwendet werden. Diese Konzeptvariante ähnelt

der vorherigen Variante insofern, als eine eigene Netzwerkzone für die Komponenten und Systeme der HSA existiert. Jedoch wird keine zentrale Firewall zur Netzwerkkopplung mit dem Produktivsystem verwendet. Alle Systeme, die eine Anbindung an das Produktivsystem benötigen, sind mit zwei Netzwerkschnittstellen ausgestattet. Die Systeme, die nur der Administration der HSA selbst dienen, befinden sich netzwerktechnisch exklusiv in der gesonderten LAN oder VLAN Zone. Die Struktur ist in Abbildung 5.3 dargestellt.



Quelle: Eigene Darstellung

Abbildung 5.3: Struktur einer HSA in eigenem LAN/VLAN

Vorteile dieser Variante:

- Leichte Umsetzung bei Einsatz eines VLANs.
- Alle Komponenten ohne Produktivkopplung sind grundsätzlich von dem restlichen IT-Netzwerk physikalisch entkoppelt.

Nachteile dieser Variante:

- Eine komplexere Konfiguration bei Systemen, die in beiden Netzwerken eingebunden sind (multihomed).[3]
- Es besteht ein Sicherheitsrisiko durch einen möglichen Zonensprung, sobald es einem Angreifer gelingt, einen der mit zwei Netzwerkkarten ausgestatteten Server zu kompromittieren.

Sicherheitsbetrachtung der Netzwerktopologie bezüglich eines APT-Angriffes

Bei der Betrachtung der Netzwerktopologien bezüglich ihrer Sicherheit ist ein grundsätzlicher Aspekt erkennbar. Wendet man das Prinzip der vertrauenswürdigen Quelle aus Abschnitt 4.1 auf den Betrieb und die Konfiguration der Netzwerkkomponenten an, rückt die in Abschnitt 2.3 definierte Rolle der Netzwerkadministration in den Fokus. Hier existiert bei allen drei Konzeptvarianten eine Sicherheitsabhängigkeit, wie folgendes Beispiel verdeutlicht: Es ist vorstellbar, dass ein Angreifer einen Administrationsplatz der Netzwerkadministratoren mittels Pass-the-Hash-Angriff kompromittiert und sich dadurch einen Zugang in den sicheren Netzwerkbereich der AVD-Umgebung bzw. der HSA schalten kann. Dieses Beispiel weist darauf hin, dass es Administrationsbereiche innerhalb der IT gibt, die weder direkt noch indirekt – in Form einer Schicht-0-Äquivalenz, wie in Abschnitt 4.2 beschrieben – mit der Sicherheit von AVD-Systemen zusammenhängen, aber dennoch ob ihrer Sicherheitsabhängigkeit kritisch betrachtet werden müssen.

5.2 Logische Struktur einer HSA

Auch in der logisch / strukturellen Einordnung einer HSA in eine existierende Netzwerkumgebung gibt es verschiedene Lösungsansätze. Grundsätzlich kann man strukturell folgende Möglichkeiten des Aufbaus unterscheiden:

- Aufbau der HSA innerhalb einer Domänenstruktur oder
- Aufbau als gesonderte HSA-Domänenstruktur (Administrationsforest) bzw.
- Aufbau als gesonderte HSA-Domänenstruktur zur Verwaltung mehrerer Institutionsdomänenstrukturen.

Domänenintegrierte HSA

Wird die HSA logisch direkt in der Zielstruktur der Institution implementiert, resultiert daraus der geringste Aufwand in der Umsetzung. Grundvorraussetzung ist das

[3] Datenflüsse und Adressierungen bedürfen in Multihomed-Server-Umgebungen einer besonderen Betrachtung.

Vorhandensein einer singulären Domänenstruktur in der Institution. Alle Objekte der HSA sind folglich auch Bestandteil dieser Domänenstruktur.

Vorteil dieser Variante:

- Eine domänenintegrierte HSA lässt sich einfach und schnell realisieren. Es sind lediglich zusätzliche Administrationsarbeitsplätze zur Administration der Schicht-0-Systeme notwendig.

Nachteil dieser Variante:

- Privilegierte Administrationskonten können nicht durch weiterführende Maßnahmen (Authentifizierungsfirewall, Trust Boundary) geschützt werden, da dies nur durch die Einführung einer separaten Domänenstruktur möglich ist, wie im folgenden Abschnitt beschrieben.

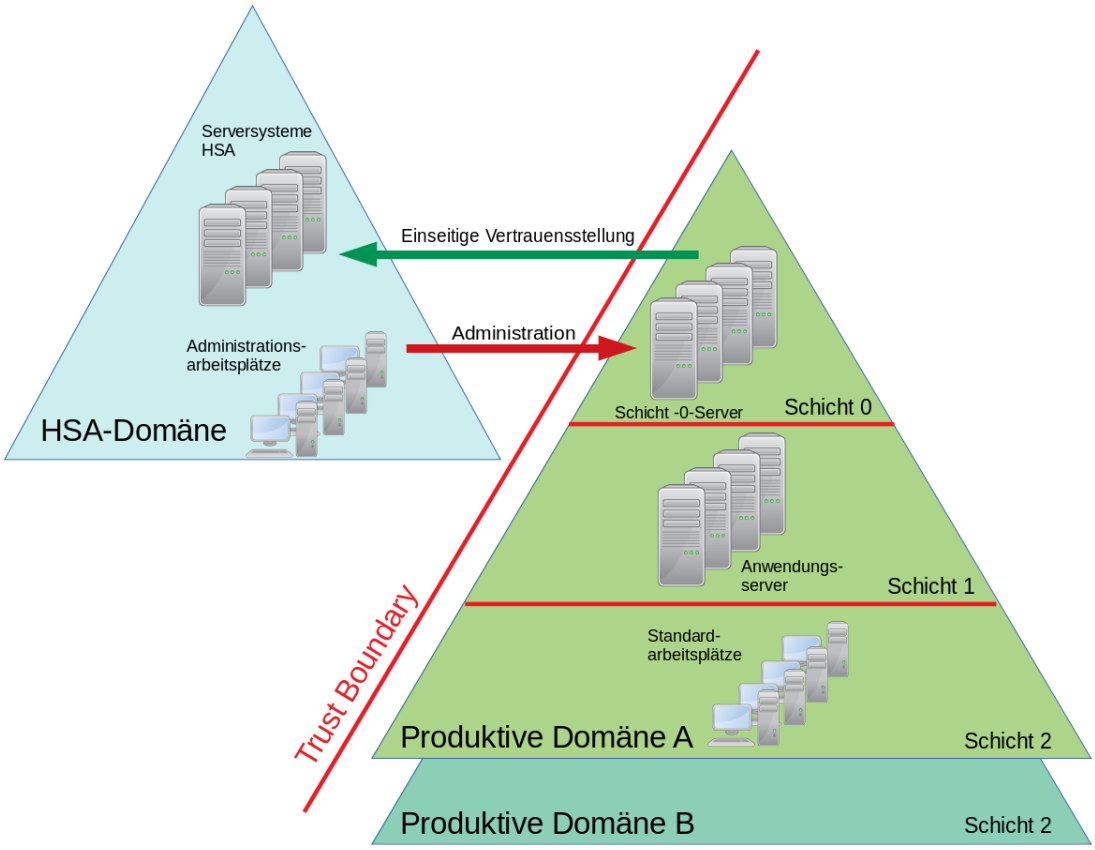
HSA in einer gesonderten Domänenstruktur

Die Ausprägung einer HSA in einer gesonderten Domänenstruktur ist insbesondere bei größeren Institutionen weit verbreitet. Existieren in einer Institution organisationsbedingt mehrere zentrale AVD-Umgebungen, ergeben sich durch eine in einer eigenen Struktur eingebundene Administrationsumgebung Synergiepotenziale bezüglich Ressourcen und Personal. Eine gesonderte HSA-Domänenstruktur wird auch als administrativer Forest[4] bezeichnet. Ein Administrationsforest besteht nicht nur aus einem oder mehreren Domain Controllern. Alle Komponenten, die für einen eigenständigen und unabhängigen Betrieb erforderlich sind, müssen in diesem Forest vorhanden sein. Dazu zählen beispielsweise folgende Systeme:

- Softwareverteilungssystem für Zielsysteme innerhalb der HSA-Struktur,
- Updateserver für Systeme der HSA-Struktur,
- PKI-Systeme für die HSA-Struktur,
- Domain Controller der HSA-Domäne und
- Administrationsarbeitsplätze.

Zur Einhaltung des Schichtenmodells ist an dieser Stelle auf eine entschiedene Trennung zwischen der Administration der HSA-Domäne und der produktiven Domäne und deren Betrieb zu achten. Aus der HSA-Struktur heraus erfolgt lediglich die Administration. Unter Anwendung des Prinzips der vertrauenswürdigen Quelle (siehe Abschnitt 4.1) darf es keine Sicherheitsabhängigkeit von Systemen der Produktivumgebung zu Systemen der HSA-Struktur geben. In Abbildung 5.4 wird die Struktur einer Produktivumgebung mit gesondertem Administrationsforest deutlich.

[4] In Dokumentationen des Herstellers Microsoft Corporation wird bei einer gesonderte Domänestruktur zur Administration der Schicht-0-Systeme von einem Red-Forest gesprochen.



Quelle: Eigene Darstellung

Abbildung 5.4: HSA als Administrationsforest

Innerhalb der HSA-Struktur werden nicht-privilegierte Benutzerkonten angelegt, die zur Administration der Produktivumgebung herangezogen werden (AP-Konten). Unter Anwendung der in Abschnitt 4.4 vorgestellten Authentifizierungsabsicherungsstrategien ist auch eine Zwei-Faktor-Authentifizierung mittels Smartcard für diese Konten zu empfehlen. Wie in Abbildung 5.4 dargestellt, ist der Administrationsforest mittels einer Vertrauensstellung mit der oder den produktiven Domäne(n) verbunden[5]. In den produktiven Umgebungen werden die benötigten Rechte für AP-Konten mittels Role Based Access Control (RBAC) durch Mitgliedschaft in den entsprechend privilegierten Gruppen zugewiesen. Die Vertrauensstellung zu den produktiven Domänen kann zusätzlich mit einer Authentifizierungsfirewall ausgestattet werden. In Form einer Whitelist wird hierzu in jeder produktiven Domäne separat festgelegt, an welchen Computersystemen grundsätzlich eine Authentifizierung mit einem AP-Konto erfolgen darf. Durch diese Maßnahme wird ein Identitätsdiebstahl, wie in Abschnitt 3.1 beschrieben, grundlegend erschwert, da ein Angreifer ein AP-Konto nicht an einem System zur Authentifizierung benutzen kann, das nicht in der entsprechenden Whitelist konfiguriert ist.

[5] In der Art einer einseitigen, nicht transitiven Vertrauensstellung

Vorteile dieser Variante:

- Eine in dieser Form umgesetzte HSA isoliert die in der produktiven Umgebung verwendeten privilegierten Konten effektiv gegenüber einem Pass-the-Hash-Angriff (siehe Abschnitt 3.4.2), da eine physikalische Vertrauensgrenze (Trust Boundary) eingeführt wird.
- Besteht der Bedarf an einer HSA in mehreren produktiven Domänen innerhalb einer Institution, kann ein gesonderter Administrationsforest die gesamte Schicht-0-Administration übernehmen. Dabei entstehen keine zusätzlichen Sicherheitsabhängigkeiten zwischen den einzelnen produktiven Domänen, da die jeweiligen Vertrauensstellungen nicht transitiv sind.

Nachteile dieser Variante:

- Der Ressourcenbedarf einer gesonderten HSA-Struktur ist im Vergleich zur domänenintegrierten HSA-Struktur erheblich höher.
- Es sind weitere Lizenzen für zusätzliche Systeme erforderlich.
- Aus Gründen der Sicherheitsabhängigkeiten darf nicht auf eine produktive Virtualisierungsumgebung mit entsprechenden Storagesystemen zurückgegriffen werden. Die Systeme sind in dieser Ebene komplett separiert aufzubauen.
- Eine entsprechende personelle Trennung der Zuständigkeiten ist empfehlenswert, erfordert jedoch zusätzliches Personal.

5.3 Komponenten und Systeme einer HSA

Basierend auf der Ermittlung der rekursiven Sicherheitsabhängigkeiten auf Schicht-0-Systemen und deren Äquivalenzen lassen sich alle Komponenten (Assets) ermitteln, die innerhalb der HSA anzusiedeln sind. Dies betrifft neben den privilegierten Zugangskonten insbesondere folgende Komponenten:

- Administrationsarbeitsplätze für die Administration,
- AVD-Serversysteme (Domain Controller),
- PKI-Serversysteme (sofern eine PKI-Struktur in die Domäne integriert ist),
- Updateserver (für Domain Controller),
- Servervirtualisierungssysteme für HSA- und AVD-Systeme,
- Speichersubsysteme für HSA- und AVD-Systeme,
- Ereignisüberwachungsysteme sowie
- sonstige Managementsysteme, die auf Systemen der Schicht 0 privilegierten Zugriff haben.

Auf die Konfiguration der oben gelisteten Server- und Speichersysteme kann nicht detailiert eingegangen werden, ohne den Rahmen dieser Arbeit zu sprengen. Technische Maßnahmen zur Konfiguration dieser mitunter bereits bestehenden Systeme einer Institution, werden im Abschnitt 5.4 dargestellt.

5.3.1 Administrationsarbeitsplatz in der HSA

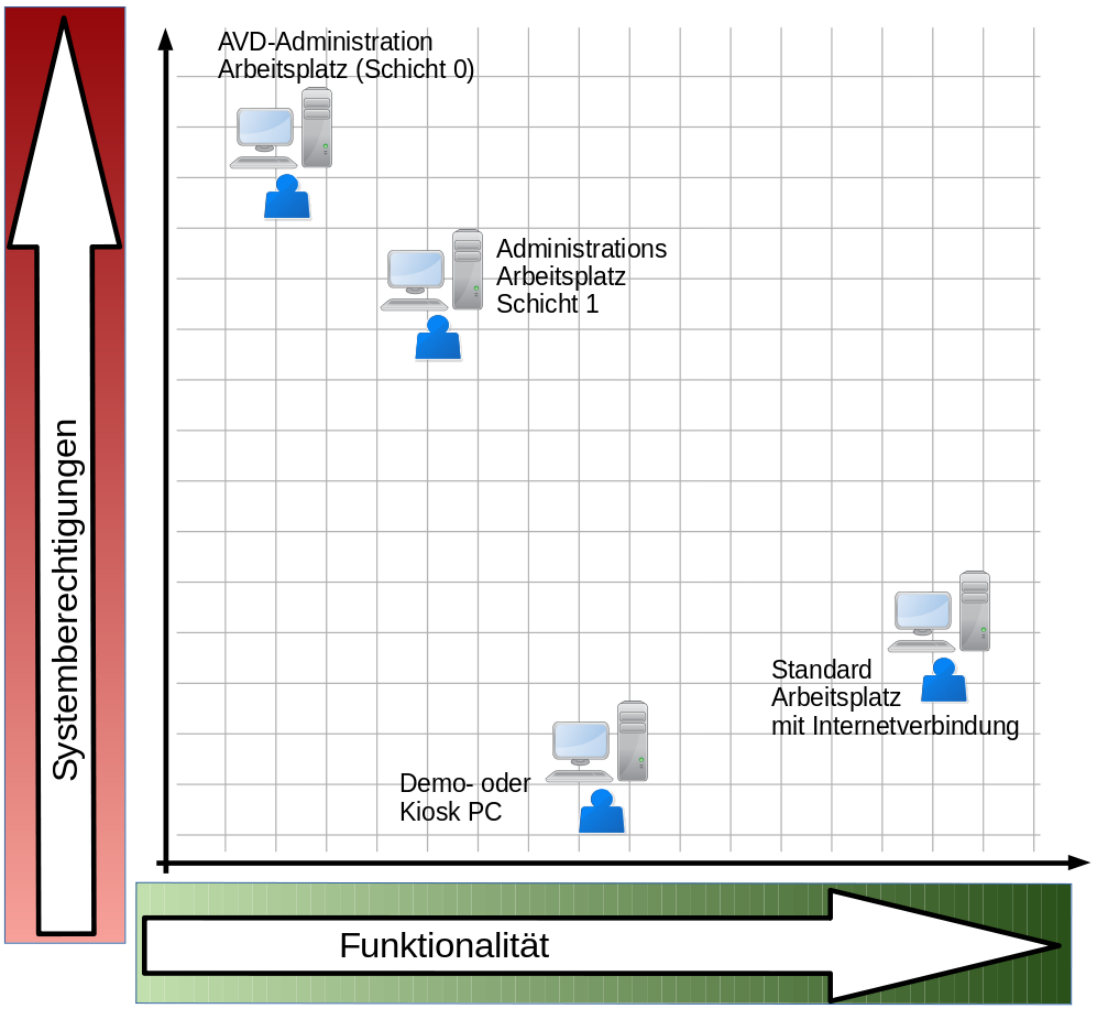
Administrationsarbeitsplätze innerhalb einer hochsicheren Administrationsumgebung unterliegen besonderen Anforderungen. Aus dem BSI-Schutzstufenkonzept können hierzu die Maßnahmen für erhöhten Schutzbedarf herangezogen werden. [siehe BSI, 2019b, INF.1.A S. 22ff] Separierte, abgeschlossene Räume, die Unbefugten den physischen Zugriff auf die Arbeitsplätze verwehren, sind mitunter sinnvoll. Grundsätzlich sollte auf eine Systemverwaltung der HSA-Serversysteme aus unsicheren Netzen heraus oder von anderen Standorten bzw. aus dem Homeoffice mittels VPN-Techniken verzichtet werden.

Installation

Bei der Installation von Administrationsarbeitsplätzen ist die Beachtung des Grundprinzips der vertrauenswürdigen Quelle, wie in Abschnitt 4.1 vorgestellt, in allen Phasen des Installationsprozesses von größter Bedeutung. Von der Hardwarebeschaffung, über die physische Bereitstellung, bis hin zur Betriebssysteminstallation sollten die entsprechenden Prozesswege mit Bedacht gewählt und dokumentiert werden. Sicherheitsabhängigkeiten zu einer möglicherweise bereits kompromittierten Produktivumgebung gilt es dabei zu vermeiden.

Betrieb

Grundsätzlich gilt für den Betrieb eines Administrationsarbeitsplatzes das Prinzip des Minimalismus. Dies widerspricht einem bei IT-Administratoren weit verbreiteten Grundverständis von Administration, wonach ein Administrator über erweiterte Rechte verfügt, damit beliebig und nach Bedarf Software installiert und getestet werden kann. Diese Aufgaben sollten generell getrennt von einem Entwicklungs- und Testsystem aus durchgeführt werden. Auf Administrationsarbeitsplätzen sollte grundsätzlich nicht mit lokalen Administratorrechten gearbeitet werden. Wenn möglich sollten Zugriffsrechte und Netzwerkkommunikation auf die eigentliche Administrationstätigkeit beschränkt werden. Eine generelle Einordung eines Administrationsarbeitsplatzes im Spannungsfeld zwischen Systemberechtigung und Funktionalität wird in Abbildung 5.5 dargestellt.



Quelle: Eigene Darstellung

Abbildung 5.5: Einordnung von PC-Arbeitsplatztypen im Spannungsfeld zwischen Systemberechtigungen und Funktionalität

Zur sicherheitstechnischen Konfiguration Windows-basierter Administrationsarbeitsplätze gibt der Softwarehersteller Microsoft Corporation detaillierte Informationen. [siehe Microsoft, 2019c] Betriebssystemunabhängig sollten folgende technischen Maßnahmen zur Einschränkung des Administrationsbetriebs erfolgen:

- Einsatz von aktuellen Versionen des gewählten Betriebssystems,
- Umsetzung von herstellerseitigen, betriebssystemabhängigen Sicherheitsrichtlinien (Security Baselines),
- Aktivierung von Secure Boot und Verschlüsselung des lokalen Datenträgers,
- Sperrung eingehender Netzwerkverbindungen (Betriebssystemfirewall),
- Blockierung des Zugangs zum Internet (technisch),
- Whitelisting von lokal installierten Anwendungen und Programmen,
- Einspielung von Sicherheitsupdates (proaktiv und unmittelbar),

- Begrenzung des Zugangs für mobile Datenträger (Whitelisting) und
- Einschränkung der lokalen Anmeldung auf die zugelassen Identitäten.

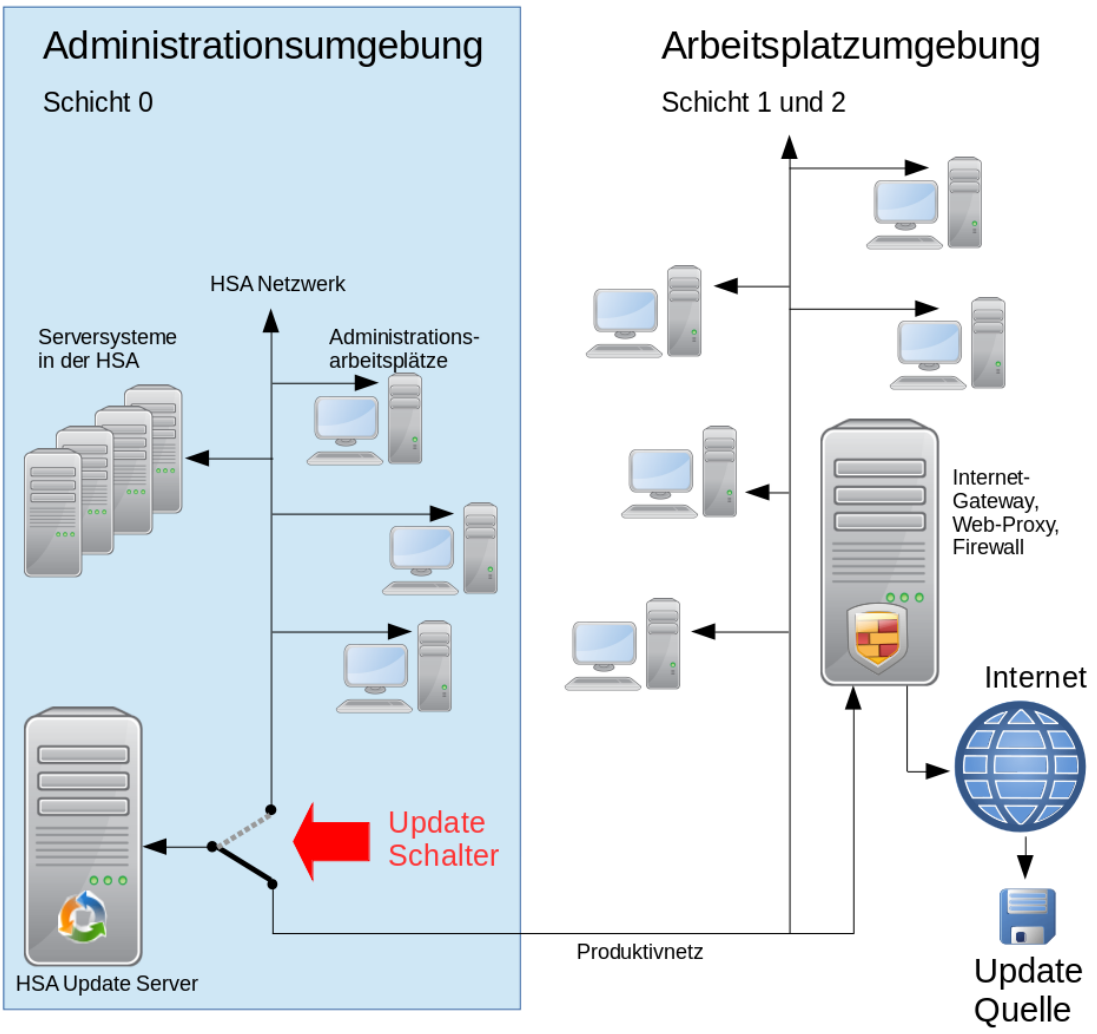
5.3.2 Updateprozesse und Datenimport in einer HSA

Ausgesprochen sensible Umgebungen, wie die hier beschriebene HSA, benötigen ein Höchstmaß an Sicherheit. Zwei Faktoren sind in diesem Zusammenhang von besonderer Relevanz:

- Die Aktualität der Systeme und
- der Datenfluss der Updatedaten.

Grundsätzlich gilt für den Updateprozess innerhalb einer HSA eine Prämisse, die in dieser Form in produktiven Umgebungen eher nachteilige Konsequenzen hat: Sicherheitsupdates sind unverzüglich und ohne vorherige Testphase einzuspielen. Hinter dieser Prämisse steht die Abwägung der Gefahr, entweder einem Angreifer eine noch nicht geschlossene Sicherheitslücke für seinen Angriff zu bieten, oder durch ein nicht getestetes Update einen Systemausfall der Administrationsumgebung zu riskieren. Da jedoch bei einem Ausfall der Administrationsumgebung der Betrieb der Serversysteme nicht unmittelbar betroffen ist, sondern nur das administrative Änderungsmanagement eben dieser Serversysteme, überwiegt in dieser Abwägung die Gefahr einer zu lange offen gehaltenen Sicherheitslücke. Der normale Produktivbetrieb bleibt in der Regel von einem Ausfall eines Administrationsarbeitsplatzes unberührt.

Das Einspielen von Updates und anderen Daten in eine HSA bedarf einer speziellen Betrachtung, da der Updateprozess in der Regel mit direkter Datenverbindung zu Onlinequellen im Internet einhergeht und damit dem generellen Prinzip einer HSA, die grundsätzlich keine Internetanbindung haben sollte, im höchsten Maße widerspricht.



Quelle: Eigene Darstellung

Abbildung 5.6: Einbindung eines Updateservers in die HSA

Eine mögliche Ankopplung eines HSA-Updateservers mit Internetquellen ist in Abbildung 5.6 dargestellt. Grundsätzlich sollte eine Kopplung mit dem Internet nur zeitlich befristet zum Zwecke des Datentransfers mit den Online-Update-Quellen erfolgen. Durch die dargestellte schematische Umschaltung der Netzwerkanbindung des internen Updateservers ist sichergestellt, dass während des Online-Updateprozesses des Servers keine generelle Internetverbindung von und zu anderen Hostsystemen der HSA besteht. Weiterhin kann durch zusätzliche Einbindung eines Internet-Gateways (HTTP-Proxyserver), das in vielen Institutionen auch grundsätzlich die Internetkonnektivität für normale Client-Arbeitsstationen bereitstellt, die Sicherheit noch weiter erhöht werden. Auf diesem Gateway können Verbindungsregeln speziell für den Updateserver zu den nötigen vertrauenswürdigen Updatequellen als Whitelist definiert werden. Ist der Online-Update-Prozess des Updateservers abgeschlossen, wird die netzwerktechnische Anbindung vom Internet getrennt und der Updateserver wieder

in das Netzwerk der HSA eingekoppelt. Die empfangenen Updates können dann den weiteren Systemen der HSA zur Verfügung gestellt werden. Dieser Zyklus wird in der Regel periodisch wiederholt. Dieses technisch sehr aufwendige Konstrukt eines Online-Update-Prozesses ist nur notwendig, wenn die Updatedaten nicht auf einem Offline-Weg in die HSA importiert werden können.

Einsatz von Datenschleusen

Wenn technisch möglich, sollte ein sensibler IT-Bereich wie die HSA physikalisch und logisch derart isoliert werden (Air Gap), dass der Datenaustausch mit anderen Computern und Netzwerken ausschließlich über mobile Datenträger erfolgt. Der hier beschriebene Offline-Weg sollte immer bevorzugt werden, da damit unerkannter Datenverkehr eines potenziellen Angreifers grundsätzlich unterbunden wird. Da aber der Umgang mit mobilen Datenträgern wie USB-Sticks in Bezug auf Schadsoftware ein hohes Risiko darstellt, hat sich zum Zwecke des Offline-Datenimports der Betrieb einer Datenschleuse als zweckdienlich erwiesen. Datenschleusen überprüfen mobile Datenträger auf Malware und Änderungen bevor Schaden entstehen kann. Sie bestehen meist aus einem gehärteten unixoiden Betriebssystem, das von einem Nur-Lese-Speicher (CD-ROM) gestartet wird. Mobile Datenträger werden intensiv, meist mit mehreren Anti-Viren-Scannern überprüft. Dabei können riskante Dateitypen wie Office-Dokumente in sichere Dateiformate umgewandelt und ausführbare Dateien geblockt werden. Schadhafte Daten können von derartigen Systemen sicher gelöscht werden, bevor sie auf Zielsystemen Schaden anrichten können.

Die zu transferierenden Daten werden bewusst auf einem mobilen Datenträger, wie zum Beispiel einem sicheren USB-Speicher[6] gespeichert. Die auf dem USB-Speicher abgelegten Daten werden in der Datenschleuse überprüft, bevor diese dann in der HSA eingespielt werden. Diese Überprüfungen sind regelmäßig durchzuführen und werden von der Datenschleuse automatisch dokumentiert. Im Anschluss können die durchsuchten und als einwandfrei befundenen Dateien z. B. auf einen von der Institution bereitgestellten / zugelassenen USB-Stick, kopiert, über ein isoliertes Air-Gapped-Netzwerk auf einen Netzwerkpfad kopiert oder per Secure File Transfer in das sichere Netzwerk übertragen und gespeichert werden.

[6] FIPS- und / oder BSI-Zertifikat, Common Criteria Stufe EAL2+, wenn möglich.

5.4 Weitere technische und organisatorische Maßnahmen

Zusätzlich zu denen in dieser Arbeit vorgestellten Konzepten, über den topologischen Aufbau und die einbezogenen Komponenten einer HSA, ergeben sich darüber hinaus eine Vielzahl von sicherheitstechnisch empfohlenen Maßnamen. Metcalf hat hierzu eine umfassende Empfehlung (Security Best Practices) aufgelistet. [siehe Metcalf, 2016, S. 43ff] Gleichzeitig sind Empfehlungen für technische und organisatorische Maßnahmen seitens des Softwareherstelles MS [siehe Microsoft, 2019c; Microsoft, 2019b] und unabhängiger Sicherheitsfirmen [siehe Trust, 2016] verfügbar. Zusammenfassend ergeben sich aus diesen Quellen folgende Empfehlungen:

Generelle technische Maßnahmen und Empfehlungen zur Absicherung kritischer Systeme:

- Einführung eines Sicherheitsmechanismus für lokale System- und Administratorkennwörter, Local Administrator Password Solution (LAPS) [siehe Microsoft, 2015] und
- damit verbunden, die Abschaffung möglichst aller lokalen Administratorkonten.
- Keine Verwendung generischer Konten mit identischen Kennwörtern auf den Systemen.
- Die Implementierung des *Restricted Admin mode* für das Remote Desktop Protocol (RDP).
- Die strikte Einhaltung der herstellerseitigen Sicherheitsempfehlungen für eingesetzte Hard- und Softwarekomponenten.
- Betriebssysteme, für die kein Herstellersupport verfügbar ist, möglichst abschalten.
- Einsatz einer Anwendungskontrolle (Application Whitelisting) auf den lokalen Systemen.
- Einsatz einer hostbasierten Firewall mit einem möglichst restriktiven Regelwerk.
- Intensive Ereignisaufzeichnung, unter Einbeziehung eines zentralen Security Information and Event Management (SIEM)-Systems.
- Dateitransfer möglichst nur über aktuelle Protokolle, wie Server Message Block (SMB) Version 2 / 3+, durchführen.
- Die Kennwörter des Standard-Domänenadministrators und des KAS-Schlüssels K_{TGS} jährlich ändern. Eine sofortige Änderung ist ratsam, wenn ein Mitarbeiter mit Domänenadministratorenrechten die Institution verlässt.
- Eine Vertrauensstellung, die nicht mehr benötigt wird, sollte unverzüglich gelöscht werden.

- Das NTLM-Authentifizierungsverfahren sollte, wenn nötig, nur noch in der Version NTLMv2 verwendet werden. Alle älteren Protokollvarianten sollten deaktiviert werden.
- Für alle kritischen Systeme sollte die direkte Verbindung zum Internet unterbunden werden.
- Das Protokoll *NetBIOS over TCPIP* sollte nicht mehr benutzt werden.
- Auf Windows-basierten Systemen sollte das Protokoll LLMNR deaktiviert werden.
- Alle privilegierten Konten, die nicht aktiv benutzt werden, sollten deaktiviert und aus entsprechenden Rollengruppen entfernt werden.
- Mitgliedschaften in hochsensible Rollengruppen, wie Schema-, Organisations- und Domänenadministratoren sollten möglichst begrenzt werden. Eine Mitgliedschaft sollte nur bei einer konkreten Anforderung zugewiesen werden.
- Die Anmeldung mit Konten, die in hochsensiblen Rollengruppen Mitglied sind, sollte nur auf Administrationsarbeitsplätzen (HSA) möglich sein.
- Wenn möglich, sollten interaktive Logon-Verfahren vermieden werden, um die unnötige Verteilung von sensiblen Credentials zu vermeiden.
- Die Implementierung eines Intrusion Detection System (IDS) wird empfohlen.

Neben der Sensibilisierung der Mitarbeiter sind folgende Denkansätze für organisatorische Maßnahmen von Relevanz: [siehe Trust, 2016]

- Jede Institution sollte sich auf den Eintrittsfall eines APT-Angriffs vorbereiten.
- Die Angreifer wählen die Waffen, den Zeitpunkt und das Schlachtfeld. Sie haben die freie Wahl der Angriffswerkzeuge und entscheiden, wann sie welchen Server angreifen. Diese Situation bringt ihnen einen Vorteil gegenüber der Verteidigung. Die Vorteile des Verteidigungsteams sind die bessere Kenntnis der Infrastruktur und die weitreichenderen Handlungsmöglichkeiten in der internen IT.

Ein Prozessmodell für ein prototypenhaftes Vorgehen zur Konzeption und für den Aufbau einer HSA werden in Form von Prozess-Ablaufdiagrammen im Anhang A dieser Arbeit gegeben.

6 Aufwand und Wirkung einer Administrationsumgebung (HSA)

Im Folgenden wird zunächst eine Einschätzung des Risikos eines APT-Angriffs gegeben, gefolgt von Orientierungshilfen für die Abschätzung der Aufwendungen für die Einführung einer HSA. Anschließend werden Methoden der Evaluation einer HSA-Implementierung vorgestellt. Abschließend erfolgt eine kurze Gegenüberstellung der Faktoren Risiko und Aufwand.

6.1 Risikoeinschätzung

Das Verfahren zur Abschätzung von Sicherheitsgefährdungen und die Gegenüberstellung zu deren Auswirkungen wird als *Risikoanalyse* bezeichnet. Da der Fokus dieser Arbeit auf den technischen Hintergründen eines APT-Angriffs liegt und die Betrachtung von möglichen Schäden aufgrund eines erfolgreichen Angriffs im Hintergrund steht, wird in diesem Zusammenhang in dieser Arbeit der Begriff Risikobewertung verwendet.

Begriffsdefinition eines Risikos

Geschonneck definiert ein Risiko in folgender Form:

> „Ein Risiko lässt sich durch die Wahrscheinlichkeit eines gefährdenden Ereignisses und die zu erwartende Schadenshöhe beschreiben. Diese beiden Parameter, Schadenshöhe und Eintrittswahrscheinlichkeit, sind für die Bewertung der eigenen Risiken heranzuziehen. Bei der im Vorfeld für ein Sicherheitskonzept durchzuführenden Risikoanalyse geht es genau darum herauszufinden, welche Unternehmenswerte bedroht werden könnten, welcher Schaden an den Unternehmenswerten im Einzelnen und für das Unternehmen im Ganzen im Schadensfall entsteht, wie hoch die Wahrscheinlichkeit eines Schadens ist und welche Schwachstellen existieren. Erst auf Basis dieser Erkenntnisse ist es in den meisten Fällen sinnvoll, organisatorische, technische, personelle oder infrastrukturelle Sicherheitsmaßnahmen umzusetzen.“ [Geschonneck, 2014, S. 12]

Wie die Kapitel 4 und 5 zeigen, gibt es verschiedene Realisierungsformen und Ausprägungen bei der Umsetzung der Strategien und Implementation einer HSA. Dies

bietet den Vorteil, für jede institutionelle Situation eine entsprechende Realisierungsform wählen zu können, je nach möglichen Ressourcen. Der Aufwand für den Aufbau einer HSA lässt sich skalieren.

Denkbare Schadenshöhe bei einem erfolgreichem APT-Angriff

Wie bereits in Abschnitt 3.4.3 erläutert, bedeutet eine erfolgreich durchgeführte Golden-Ticket-Attacke den kompletten Verlust der Integrität, Vertraulichkeit und Authentizität aller Daten, die durch das betroffene AVD-System verwaltet werden. Das bedeutet, für einen Großteil aller Institutionen auch gleichzeitig den Verlust eben dieser Schutzziele für alle relevanten und existenziellen Daten, da ein zentrales AVD-System dem Zweck dieser Datenspeicherung und -verwaltung dient. Derart existenzielle Daten werden im Umfeld der IT-Sicherheit als Kronjuwelen bezeichnet. [siehe BSI, 2017a, S. 28] Es ist denkbar, dass eine von einem derartigen Angriff betroffene Institution durch den entstandenen Schaden in ihrer gesamten Existenz bedroht ist.

Tabelle 6.1: Schutzbedarfskategorien

Schutzbedarfskategorie	Auswirkungen des Schadens
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Quelle: BSI-Standard 200-2, Definition der Schutzbedarfskategorien [siehe BSI, 2017a, S. 104]

In der vom BSI vorgeschlagenen Schutzbedarfskategorisierung, die in Tabelle 6.1 dargestellt ist, entspricht eine Schadenshöhe mit existenziell bedrohlichem Ausmaß der Schutzbedarfskategorie *sehr hoch*. [siehe BSI, 2017a, S. 104]

Eintrittswahrscheinlichkeit eines APT-Angriffs

Wie bereits an mehreren Stellen in dieser Arbeit beschrieben, handelt es sich bei APT-Angriffen um gezielte Angriffe mit hochspezialisierten Werkzeugen, die meist von einer Gruppe von Tätern ausgeführt werden, die im Auftrag Dritter handeln. Im Umkehrschluss ist davon auszugehen, dass die Wahrscheinlichkeit, dass eine Institution angegriffen wird, mit dem potenziellen Interesse an den Daten, die dort gespeichert werden, stark ansteigt. Steffens benutzt in diesem Zusammenhang den Begriff *Auftragsvergabe*. Man könne davon ausgehen, dass eine APT-Gruppe im Auftrag handelt. [siehe Steffens, 2018, S. 81] Er schreibt dazu:

> „Wie die Auftraggeber ihre Interessenlage in konkrete Aufträge für APT-Gruppen abbilden, ist öffentlich kaum bekannt. Selbst in den wenigen Fällen, in denen eine sichere Zuordnung von APT-Angriffen auf eine Organisation möglich war, fehlen Erkenntnisse über die interne Auftragssteuerung. Eine Ausnahme bildet die Operation Olympic Games, die den Trojaner Stuxnet entwickelt und eingesetzt haben soll. David E. Sanger stützt sich [...] auf Aussagen aktiver und ehemaliger Nachrichtendienst-Mitarbeiter [siehe Sanger, 2012].“ [Steffens, 2018, S. 81]

Dies lässt im ersten Blick vermuten, dass primär staatliche Institutionen wie Polizeibehörden, Ämter und Ministerien im Fokus von APT-Angriffen stehen, da eher strategische oder taktische Ziele verfolgt werden. Für Institutionen in diesen Bereichen ist die Wahrscheinlichkeit eines Angriffs daher als hoch einzuschätzen. Weiterhin ist davon auszugehen, dass mittlerweile auch wirtschaftliche Interessen zu Aufträgen an APT-Gruppen führen. Damit kommen auch Wirtschaftsunternehmen in den Fokus eines Angriffs. Das BSI äußert sich dazu im Lagebericht zur IT-Sicherheit wie folgt: „Als Trend bei APTs [...] sind folgende Phänomene festzustellen: mehr öffentlich verfügbare APT-Werkzeuge, eine wachsende Zahl internationaler APT-Dienstleister, die Nutzung legitimer Dienste zur Verschleierung, das Erschweren von Schadsoftware-Analysen sowie die Übernahme von APT-Techniken in kriminellen Kampagnen.“ [BSI, 2019a, S. 7]

Grundsätzlich kann zusammenfassend davon ausgegangen werden, dass, sobald es für eine Institution eine den eigenen Interessen entgegenstehende Partei mit einem wirtschaftlichen oder politischen Motiv für einen Angriff und ausreichend finanziellen Mitteln gibt, die Wahrscheinlichkeit einer Kompromittierung stark ansteigt. In diesem Zusammenhang wurde der Begriff des *Assume-Breach-Paradigma* geprägt. Es bezeichnet die These, dass obwohl im Bereich der IT aufwendige Sicherheitsvorkehrungen getroffen werden, jede Institution davon ausgehen muss, einmal Opfer einer Cyber-Attacke zu werden. Das BSI schreibt hierzu:

> **„Assume the Breach: Verantwortung für Prävention, Detektion und Reaktion in der Wirtschaft**
>
> In der Wirtschaft muss sich durchsetzen, dass IT-Sicherheit Teil des Risikomanagements und damit eine Managementaufgabe ist, die in der Unternehmensleitung verankert ist. Eine mangelnde Entschlossenheit der Unternehmensführung führt somit zu mangelhafter IT-Sicherheit. Dabei kann IT-Sicherheit nach dem Pareto-Prinzip wirtschaftlich umgesetzt werden:

> Die Investition in bewährte Basismaßnahmen in den Bereichen Technik, Personal und Organisation lässt sich wirtschaftlich vertreten und schützt bereits gegen eine Vielzahl heutiger Angriffe.“ [BSI, 2015, S. 49]

6.2 Aufwand für den Aufbau einer HSA

Der Aufwand, den eine Institution betreiben muss, um die vorgestellten Strategien und Konzepte umzusetzen, lässt sich nicht pauschal quantifizieren, da er von vielen institutionsbezogenen Faktoren (Größe, Struktur, Schutzbedarf etc.) abhängig ist. Um Institutionen eine Basis für eine individuelle Einschätzung des jeweiligen Aufwands zu geben, wird in den folgenden Abschnitten kurz auf die verschiedenen Bereiche eingegangen, in denen mit Aufwendungen zu rechnen ist.

Strukturaufwand

Die Neuimplementierung eines Schichtenmodells und der Aufbau einer Schicht-0-HSA kann mit einem erheblichen Planungs- und Konzeptionsaufwand verbunden sein. In der Regel ist es für Institutionen in dieser Situation sinnvoll, sich entsprechende Dienstleistungen für Beratung und Aufbau der Struktur an die Seite zu holen. Diese Leistungen sind von Softwareherstellern, wie der Microsoft Corporation, aber auch von Dritt-Unternehmen und Sicherheitsfirmen im Rahmen von Beratungsdienstleistungen abrufbar.

Sachkosten

Der Aufbau einer von der restlichen IT getrennten Schicht-0-Systemschicht kann mit erheblichen Kosten verbunden sein. Wird an dieser Stelle auf eine strikte Trennung der Systeme geachtet, muss eine eventuell vorhandene Virtualisierungsschicht ebenso wie eine vielleicht vorhandene Speicherinfrastruktur gesondert aufgebaut werden, da sonst die Prinzipien der vertrauenswürdigen Quelle im Rahmen der Schichten-Abstraktion verletzt werden. Weiterhin sind zusätzliche Administrationsarbeitsplätze für die Administration der Schicht-0-Systeme erforderlich. Mit entsprechenden Kosten für zusätzliche Hard- und Software muss gerechnet werden.

Schulungen

Ein nicht zu unterschätzender Punkt ist die Sensibilisierung der Mitarbeiter, speziell der Administratoren, für die Existenz eines Schichtenmodells und die damit verbundenen organisatorischen Maßnahmen. Viele Handlungen, die aufgrund ihrer Einordnung eine Verletzung des Schichtenmodells darstellen, wie in Abschnitt 4.2 beschrieben,

können nicht oder nur mit sehr großem Aufwand technisch verboten oder gesperrt werden. Daher ist es in diesem Bereich von besonderer Bedeutung, Mitarbeiter über organisatorische Maßnahmen zu informieren und diesbezüglich zu schulen.

Ein Beispiel ist die Benutzung eines privilegierten Anmeldekontos, beispielsweise aus der Schicht 0, an einem normalen Arbeitsplatz-PC. Versucht ein Mitarbeiter eine Anmeldung mit einem derartigen Konto an einem Arbeitsplatz-PC, wird diese bei entsprechender Systemkonfiguration und korrekter Implementierung des Schichtenmodells zu einer Fehlermeldung führen. Eine Anmeldung selbst ist also nicht möglich. Handelte es sich jedoch bei dem PC, an dem die Anmeldung versucht wurde, um eine kompromittierte Arbeitsstation, kann selbst der initiale Schritt, die Eingabe des Kennwortes, dazu führen, dass ein Angreifer in Besitz sensibler Anmeldeinformationen kommt. Mit diesen Anmeldeinformationen ist er unmittelbar, in Sekundenschnelle in der Lage, einen Golden-Ticket-Angriff durchzuführen, wie in Abschnitt 3.4.3 beschrieben. Dieses Beispiel zeigt, dass technische Maßnahmen allein nicht ausreichend sind. Gerade Mitarbeiter, die als Administratoren tätig und dementsprechend mit erweiterten Rechten ausgestattet sind, müssen mit diesen Berechtigungen ausgesprochen sensibel umgehen und dahingehend geschult werden.

In dem beschriebenen Szenario zeigt sich zudem ein weiterer Effekt: Der Bitkom e. V. bezeichnet die Situation des oben dargestellten Beispiels als Asynchronität zwischen Angriff und Verteidigung. „Der Angreifer muss nur ein Schlupfloch finden, die Sicherheitsverantwortlichen aber eine Vielzahl von Systemen mit noch mehr potenziellen Schwachstellen absichern“. [siehe Bitkom e.V., 2015, S. 45] Die Implementierung des Schichtenmodells innerhalb einer Institution kann noch so gründlich und aufwendig durchgeführt worden sein, eine kleine Unzulänglichkeit oder eine unbedachte Handlung kann alle diese Maßnahmen auf einen Schlag zunichte machen.

Personalaufwand

In kleineren Institutionen ist durchaus denkbar, dass die Administration der Schicht 0 durch einen Administrator, der sonst Aufgaben und Tätigkeiten in anderen Schichten des Schichtenmodells erfüllt, in Personalunion durchgeführt wird. Bedingung ist hier aber eine strikte Trennung der verwendeten IT-Ressourcen. Das bedeutet den Einsatz eines gesonderten Administrationsarbeitsplatzes und die Verwendung getrennter Anmeldekonten. Grundlegend ist an dieser Stelle das Bewusstsein der Mitarbeiter für die Existenz des Schichtenmodells und die Bereitschaft, die entsprechenden Handlungen und Tätigkeiten auf die unterschiedlichen Schichten des Modells abzustimmen.

Bei größeren Institutionen, in denen die Abtrennung der Schicht 0 durch alle

Systembereiche der IT klar durchgesetzt wird, ist der Einsatz von dedizierten Schicht-0-Administratoren mithin sinnvoll. Wird eine HSA nach allen Maßgaben und Prinzipien aufgebaut und betrieben, die in den vorangegangenen Kapiteln dieser Arbeit erläutert wurden, wie eine separierte Virtualisierungsumgebung, dedizierte Softwareverteilungs- und Updateprozesse sowie gesonderte Speichersubsysteme, fallen entsprechende Aufgaben gemäß den in Abschnitt 2.3 dargestellten Rollenkonzepten in doppeltem Maße an. Institutionen sollten in dieser Situation entsprechende Mitarbeiterteams mit Vertretungsfunktion für die Administration der Umgebung einplanen.

Bei Institutionen in Konzerngröße ist der Einsatz einer gemäß Abschnitt 5.2 logisch abgetrennten HSA in Form einer eigenen Administrationsdomäne sinnvoll. In Institutionen dieser Größenkategorie existieren bisweilen mehrere zentrale AVD-Systeme, die durch Anbindung an eine zentrale HSA-Struktur in Form einer Schicht-0-Domäne verwaltet werden können. Der Betrieb dieser Struktur erfordert entsprechend große personelle Ressourcen.

6.3 Schutzfunktion gegen APT-Angriffe

Die Autoren der Bitcom e. V. fordern ein Umdenken bei der Informationssicherheit. Sie schreiben Folgendes: „Da die Bedrohungen immer vielfältiger und die IT-Infrastrukturen immer komplexer werden, reicht ein rein präventiver Ansatz zum Schutz der Unternehmensinformationen nicht mehr aus: Ein Unternehmen muss lernen, mit Sicherheitsvorfällen professionell umzugehen und den entstandenen Schaden zu minimieren. Das sogenannte *Incident Management* bzw. IT-Störungsmanagement ergänzt die bisherigen Schutzkonzepte.“ [Bitkom e.V., 2015, S. 36] Die Bildung eines Computer Emergency Response Team (CERT) ist für eine schnelle Reaktion in dieser Situation ein sehr wesentlicher Schritt, um eine sofortige Reaktion auf einen auftretenden Sicherheitsvorfall zu ermöglichen.Im Rahmen eines Computer Emergency Response Team (CERT) ist auch die in Abschnitt 4.5 vorgestellte verhaltensorientierte Ereignisanalyse einzuordnen, die eine frühzeitige Detektierung eines laufenden Angriffs ermöglicht.

Die Umsetzung der in Kapitel 4 und 5 vorgestellten Verfahren verspricht an dieser Stelle einen systematischen Schutz vor einer möglichen Rechte-Eskalation, mit der der Angreifer die Kontrolle über zentrale AVD-Strukturen erlangen könnte. Es schützt jedoch nicht vor Querbewegungen, die der Angreifer innerhalb einer Sicherheitsschicht, wie der Schicht 2 – der Bereich der normalen Arbeitsstationen – eventuell durchführen könnte, um an Daten zu gelangen. An dieser Stelle ist es erforderlich, die

beschriebenen Konzepte innerhalb einer Institution mit weiteren Sicherheitskonzepten zu verzahnen und in einem stetigen Zyklus zu überprüfen.[1]

6.4 Überprüfbarkeit der vorgestellten Konzepte (Evaluation)

Im Bereich des IT-Sicherheitsmanagements sind unterschiedlichste Testverfahren und -prozesse etabliert, wie beispielsweise eine IT-Revision oder ein Code-Review. Mit Bezug auf das Thema dieser Arbeit sollen jedoch drei spezielle Testprozesse näher betrachtet werden, die nach Umsetzung der vorgestellten Strategien und Konzepte über die Wirksamkeit der Maßnahmen Aufschluss geben:

- IT-Sicherheitsbeurteilung (Security Assessment),
- Penetrationstests und
- Red Teaming.

Sicherheitsbeurteilung im Rahmen eines Security Assessment

Im Vorfeld einer aktuellen Bedrohung kann eine Beurteilung der Sicherheitsarchitektur wertvolle Informationen zur Verbesserung der Absicherung bringen. Bei der Untersuchung des Status quo können vorbereitete Schwachstellenscanner zum Einsatz kommen. Gleichzeitig kann aber auch ein Audit / Interview von IT-Sicherheitsverantwortlichen durchgeführt werden. Das BSI schreibt hierzu: „Ein Weg, vorhandene Schwachstellen nachzuweisen, ist, mit so genannten technischen Sicherheitsaudits stichprobenartig sicherheitsrelevante Konfigurationen und Regelwerke der eingesetzten IT-Systeme zu untersuchen und anhand der Versionen und Patchstände Rückschlüsse auf Schwachstellen zu ziehen.“ [BSI, 2016, S. 6] Entsprechende Assessments werden von Softwareherstellern, aber auch von unabhängigen Sicherheitsfirmen angeboten.

Sicherheitsüberprüfung durch Penetrationstests

Im Gegensatz zum Security Assessment wird bei einem Penetrationstest nicht die sicherheitstechnische Einrichtung als Ganzes beurteilt. In der Regel wird bei einem derartigen Test ein konkretes Auftragsziel vereinbart. Im Laufe des Tests werden direkte Angriffsversuche gestartet. Ein Penetrationstest in dieser Form bedeutet die Suche

[1] Vergleichbar einem PDCA-Zyklus (Plan, Do, Check, Act) [siehe Moen et al., 2009], auch bekannt als Demingkreis [siehe Deming, 1982, S. 88].

nach einer Kette von Schwachstellen im Gesamtsystem, die letztendlich zum Zielobjekt, dem Auftragsziel, führt. In der Regel ist der Test erfolgreich abgeschlossen, wenn ein Schwachstellenpfad gefunden wurde. Weitere, mitunter gleichzeitig existierende Schwachstellen, werden meist außer Acht gelassen. Das BSI schreibt hierzu: „Ein IS-Penetrationstest ist ein erprobtes und geeignetes Vorgehen, um das Angriffspotenzial auf ein IT-Netz, ein einzelnes IT-System oder eine (Web-)Anwendung festzustellen. Hierzu werden die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System eingeschätzt und daraus notwendige ergänzende Sicherheitsmaßnahmen abgeleitet beziehungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen überprüft.“ [BSI, 2016, S. 5] Ein unmittelbares Angriffsziel für die in dieser Arbeit relevanten APT-Angriffe ist der administrative Zugriff auf die AVD-Serversysteme einer Institution und die daraus resultierende Aktion der Erstellung eines Golden Tickets.

Red Teaming

Mansfield-Devine beschreibt, dass einer der besten Wege für die Untersuchung der Wirksamkeit von Abwehrmaßnahmen das Erleben eines echten Angriffs sei [siehe Mansfield-Devine, 2018]. Schwachstellen können demnach am besten von gut ausgebildeten Hackern aufgedeckt werden. IT-Verantwortliche einer Institution werden dabei mit einer Situation konfrontiert, die einem echten Angriff sehr ähnlich ist. Als Red Team wird dabei eine – grundsätzlich von der Institution unabhängige – Gruppe bezeichnet, die als Angreifer auftritt. Ziel des Red Teaming ist es, Schwachstellen aufzuspüren und auszunutzen. Im Gegensatz zum IT-Penetrationstest wird üblicherweise kein konkretes Angriffsziel vereinbahrt. Das generische Ziel des Einsatzes ist es, Sicherheitslücken aufzuspüren und das Gesamtsystem so weit wie möglich zu kompromittieren, bevor dies einem echten Angreifer gelingen könnte und tatsächlich Schaden entsteht. In Bezug auf APT-Angriffe wird ein Red Team versuchen, den Modus Operandi möglichst genau nachzustellen. Dabei werden die in Abschnitt 3.2.2 dargestellten Angriffsphasen detailliert durchlaufen und die in Abschnitt 3.3 vorgestellten Werkzeuge verwendet.

In diesem Testszenario sind folgende Gruppen / Rollen definiert:

- Das Red Team bildet die Gruppe der Angreifer, die ihr Ziel und die Art und Weise des Angriffs relativ frei wählen kann, soweit es der Testauftrag zulässt.
- Das Blue Team bildet die Gruppe der Verteidiger, die in der Regel aus den IT-Verantwortlichen der Institution besteht. Ihre Aufgabe ist es, den Angriff zu detektieren, einzudämmen und Schwachstellen zu schließen.

- Das Purple Team bildet eine Gruppe außerhalb des eigentlichen Angriffsszenarios. Sie hat eine moderierende Funktion. Ihre Aufgabe ist es, durch Informationsaustausch mit dem Red- und Blue Team einen Verstärkungsfaktor auf beiden Seiten herbeizuführen, um sowohl den Angriff als auch die Verteidigung effektiver gestalten zu können [siehe Miessler, 2019].

Die Aufgabe aller Rollen im Red Teaming Prozess ist es, die Effektivität der Abwehrmaßnahmen einer getesteten Institution zu steigern. Die Vorteile eines Red Teaming Prozesses sind: [siehe Core Security, 2020]

- Das Aufdecken aller Angriffsvektoren, die die Angreifer ausnutzen könnten.
- It-Verantwortlichen wird demonstriert, wie sich Angreifer bei einem APT-Angriff im Netzwerk bewegen.
- Vermittlung der Fähigkeiten, die nötig sind, um einen echten APT-Angriff abzuwehren.

6.5 Risikofaktor versus Aufwand

Den in Abschnitt 6.2 dargestellten möglichen Aufwänden steht der in Abschnitt 6.1 beschriebene Risikofaktor, bestehend aus der möglichen Schadenshöhe und der Eintrittswahrscheinlichkeit, entgegen. Eine generelle Empfehlung für oder gegen die Implementierung einer HSA kann an dieser Stelle nicht erfolgen, da die Entscheidung von vielen individuellen Faktoren einer Institution abhängig ist, und sich in ihr die Risikobereitschaft der jeweiligen Institution ausdrückt. Das BSI bezeichnet die Risikobereitschaft auch als *Risikoappetit* und benennt u. a. folgende Einflussfaktoren: [siehe BSI, 2017c, S. 42]

- Interne Faktoren (wie Organisationskultur, Einstellung des Managements),
- Marktumfeld (z. B. konservatives oder innovatives Umfeld) und
- Risikotragfähigkeit (Finanzierung der Institution, Haftung, Kapitaldecke usw.).

Die Entscheidung zur Einrichtung einer HSA ist eine Abwägungsentscheidung und sollte grundsätzlich in der Leitungsebene einer Institution getroffen werden und nicht in einer IT-Fachabteilung, die die genannten Faktoren mitunter nicht vollumfänglich beurteilen kann.

7 Zusammenfassung und Ausblick

In diesem Kapitel werden einige Schlussfolgerungen aus den Ergebnissen der strategischen Überlegungen zur Einführung eines Schichtenmodells und Absicherung der Schicht 0 und deren Administration angestellt. Diese werden dann in Relation zur in der Einleitung dargestellten Problemstellung gesetzt. Das Kapitel schließt diese Arbeit mit einem Ausblick auf aktuelle Trends und aufkommende Technologien der Perimeter Absicherung ab.

In der jetzigen Situation ist davon auszugehen, dass in der Schicht der normalen PC Arbeitsstationen mit Officefunktionalität und Internetzugang (Schicht 2) eine ständige Kompromittierungslage existiert. Dies wird auch als Assume-Breach-Paradigma bezeichnet, wonach jede Institution davon ausgehen muss, einmal Opfer eines Cyber-Angriffs zu werden, obwohl alle denkbaren Sicherheitsvorkehrungen getroffen wurden. Ist es Angreifern möglich, sich in dieser Sicherheitsschicht ohne großen Aufwand festzusetzten, ist es für Institution mitunter unerlässlich, ein Schichtenmodell einzuführen und die kritischen Systeme gegenüber anderen Systemen abzuschotten, um eine Rechte-Eskalation zu verhindern.

Konklusion

Das Assume-Breach-Paradigma beschreibt eine Situation, die es unumgänglich macht, sich mit der Absicherung einer zentralen AVD-Umgebung zu befassen. Ein erster, aber sehr essenzieller Schritt für die IT-Mitarbeiter einer Institution ist dabei die Auseinandersetzung mit den Möglichkeiten und Werkzeugen, die ein APT-Angreifer hat. Nur durch das Verständnis der Vorgänge während eines APT-Angriffs ist es möglich, das Schadenrisiko im Vorfeld zu reduzieren, den Angriff zu detektieren und zumindest in seinem Ablauf abzuschwächen.

> „Wer die Position des anderen versteht und nachvollziehen kann, ist in der Lage, umso fester eine Gegenposition einzunehmen."
>
> Quelle: Mündliches Zitat von F. Schroeder[1], in Anlehnung an G. W. F. Hegel

Institutionen, ganz gleich welcher Größe, sollten beispielsweise das in Abschnitt 3.2.3 beschriebene MITRE ATT&CK™ Portal nutzen, um sich Wissen über Verhaltensweisen von cyberkriminellen Gruppierungen anzueignen. So können Sicherheitsmechanismen und Verteidigungssysteme effektiv angepasst werden.

[1] Interview mit Jan Sternberg, Reporter des Redaktionsnetzwerk Deutschland, RND vom 11.8.2020

Durch Anwendung der in Kapitel 4 vorgestellten Strategien und der in Kapitel 5 vorgestellten Konzepte, ist nach heutigem Stand des Wissens und der Technik die Resilienz der AVD-Systeme einer Institution gegenüber einem APT-Angriff signifikant zu erhöhen. Die Ausbildung einer hochsicheren Administrationsumgebung (HSA) gemäß der in Kapitel 5 angesprochenen technischen und organisatorischen Maßnahmen ist in diesem Zusammenhang ein elementarer Bestandteil der Absicherung. Eine in dieser Form ausgeprägte HSA zur Administration aller Schicht-0-Serversysteme kann den kompletten Verlust der Integrität, Vertraulichkeit und Authentizität der Daten, die innerhalb der Domäne abgelegt werden, verhindern.

7.1 Fazit

In Kapitel 3 wurde dargelegt, dass APT-Angriffe in den meisten Fällen mit Identitätsdiebstahl und Versuchen der Rechteerweiterungen innerhalb einer gemeinsamen, zentralen Authentifizierungsumgebung einhergehen. Betrachtet man die aktuelle Situation im Hinblick auf die Verfügbarkeit der entsprechenden APT-Angriffswerkzeuge und die Beurteilung der aktuellen Gefährdungslage, ist eine Absicherung zentraler Authentifizierungs- und Verzeichnisdienst Systeme, wie sie in dieser Arbeit beschrieben wurde, nicht nur sinnvoll, sondern mitunter sogar notwendig. Die konsequente Absicherung des IT-Netzwerkes einer Institution im Hinblick auf APT-Angriffe bedeutet auch die Umsetzung der in Kapitel 4 vorgestellten Strategien in den Bereichen der Schicht 1 (Serversysteme) und Schicht 2 (Clients).

Gerade im Hinblick auf kleinere Institutionen, sind folgende Punkte schnell umzusetzen, haben aber gleichzeitig eine große Wirkung auf die Absicherung im Bezug auf Identitätsdiebstahl und Rechte-Eskalation:

- Aufteilung von Berechtigungen,
- Trennung der Systeme für Office-Arbeit und Administration,
- Beobachtung der Systemumgebung (Ereignisaufzeichnung) und
- Ermittlung eines Normalzustandes, um „Auffälligkeiten“ feststellen zu können.

Diese Maßnahmen sind bereits bei einer minimalen Institutionsgröße technisch und organisatorisch ohne größeren Aufwand umsetzbar.

In der Arbeit wurde aufgezeigt, dass ältere Authentifizierungsprotokolle, wie NTLMv1 und NTLMv2, ausgesprochen anfällig für Pass-the-Hash-Angriffe sind. Auf die Anwendung dieser Protokolle sollte verzichtet werden.

Bei der Umsetzung eines Schichtenmodells, speziell der Abgrenzung zwischen den Schichten, bleibt die Einschätzung der Abgrenzungsmöglichkeiten von Virtualisierungen ein noch offen diskutierter Punkt. Es bleibt beispielsweise ungeklärt, ob nach Offenlegung der Schwachstellen Meltown und Spectre [siehe Lipp et al., 2018], eine Virtualisierung einer normalen Arbeitsstation und einer Administrationsstation auf dem gleichen Virtualisierungshost eine sicherheitstechnisch vertretbare Lösung ist. Weiterhin ist die Abschottung der Netzwerkschichten durch virtuelle LAN Strukturen (VLAN), wie in Kapitel 5 beschrieben, hinsichtlich der Resilienz gegen APT-Angriffen ein noch nicht abschließend aufgeklärter Punkt.

7.2 Ausblick

Am Ende dieser Arbeit soll ein Ausblick auf aktuelle Entwicklungen innerhalb der Informationstechnologie gegeben werden, die in Zukunft höchstwahrscheinlich für viele Institutionen zu einem Wandel der angewendeten Authentifizierungsverfahren führen werden.

AVD-Systeme in der Cloud

Cloudbasierte Architekturen bieten einen immer populäreren Ansatz, IT-Leistungen zu virtualisieren und bei externen Anbietern betreiben zu lassen. Dies würde nach Borchers alle cloudbasierten Architekturen betreffen, [siehe Borchers et al., 2016, S. 1] die von der NIST und darauf basierend vom BSI wie folgt definiert wurden: [siehe Mell et al., 2020, S. 2ff]

- Infrastructure as a Service (IaaS),
- Platform as a Service (PaaS) und
- Software as a Service (SaaS).

Alle Arten der cloudbasierten Architekturen sind nach Borchers von Anbietern (Providern) in der Regel als exklusive („private“) oder auf Basis einer mit anderen Kunden geteilten Infrastruktur („public“) verfügbar. Zunehmende Tendenz haben in diesem Bereich auch immer mehr SaaS-Anwendungen, wie Kollaborationsanwendungen[2] und andere mitunter geschäftskritische Systeme, die von Kunden – in diesem Fall Institutionen – gerne benutzt werden, da sie eine schnelle und vermeintlich unkomplizierte Integration in hausinterne Prozesse bieten. [siehe Borchers et al., 2016, S. 1]

[2] Als Kollaborationsanwendung (auch kollaborative Software) wird Groupware bezeichnet, die die Zusammenarbeit einer Gruppe über zeitliche und / oder räumliche Distanz hinweg unterstützt. Darunter fallen E-Mail-, Kalender- und Messagingsysteme aber auch moderne Audio- und Videokonferenzsystem, wenn sie derartige Funktionen in Kombination anbieten.

Vielen Institutionen ist dabei nicht bewusst, dass Kollaborationsanwendungen meist über eine zentrale Benutzerverwaltung verfügen, deren technischer Aufbau im Backend-Bereich, dem eines zentralen Authentifizierungs- und Verzeichnisdienstes gleicht. [siehe Kaffel-Ben Ayed, 2016] Der initiale, administrative Benutzer einer derartigen SaaS-Anwendung entspricht dem initialen Domänenadministrator eines zentralen AVD-Systems. Lediglich der Geltungsbereich ist ein anderer. Werden innerhalb einer SaaS-Anwendung seitens der Institution Daten gespeichert, sind für diesen Geltungsbereich alle datensicherheitstechnischen Überlegungen, die in dieser Arbeit präsentiert wurden, ebenso relevant wie für institutionsinterne Datenspeicherungen. Problematisch ist dabei nur, dass bei vielen Institutionen derartige SaaS-Anwendung nicht von zentralen IT-Abteilungen beschafft und betrieben werden, sondern vermehrt direkt von Fachabteilungen, denen der in dieser Arbeit vermittelte Wissensstand eventuell nicht bekannt ist. Der hier beschriebene Effekt wird durch die aktuelle Corona-Situation noch verstärkt, da viele SaaS-Anbieter auf Grund der vermehrten Homeoffice-Situation im Sommer 2020 ihre Kollaborationsanwendungen zeitlich befristet kostenlos anbieten. Der Umstand, dass vermehrt AVD-Systeme cloudbasiert und von der IT-Fachabteilung unkontrolliert in der Institution auftreten, wird in dieser Form als Bildung von „IT-Schattensystemen“ bezeichnet und bedarf in naher Zukunft vermehrter Aufmerksamkeit.

Zero-Trust-Netzwerkarchitektur

Bisherige Netzwerkarchitekturen basieren meist auf dem hierarchischem Internetworking Netzwerkmodell, welches bereits 2002 vom Hersteller Cisco als Architekturmodell eingeführt wurde. In diesem Modell besteht ein physikalisches Netzwerk aus folgenden Ebenen: [siehe Raza et al., 2002]

- Die Kernschicht (core layer),
- die Verteilungsschicht (distribution layer) und
- die Zugriffsschicht (access layer).

Kindervagwith fügt diesem Modell noch eine Grenzschicht (edge layer) hinzu [Kindervagwith et al., 2010, vgl.S.4], die für die Anbindung eines Netzwerks an das Internet zuständig ist. Bisherige Authentifizierungsmodelle gehen davon aus, dass im gesamten, derartig definierten Netzwerkraum eine vollumfängliche Vertrauensstruktur herrscht. Jedes Objekt kann jedem anderen Objekt vertrauen, da es sich nur in der beschriebenen Netzwerkstruktur befinden kann, wenn es erfolgreich authentifiziert wurde. Gilman spricht in diesem Zusammenhang von einer *Common Sense Security* [siehe Gilman, 2016, S. 9], die Sicherheitsüberprüfung erfolgt demnach an der Außen-

grenze des definierten Netzwerkraums. Dies wird daher auch als Perimeterabsicherung bezeichnet.

Dagegen ist die Idee hinter der Zero-Trust-Architektur, die Paradigmen der Perimeterabsicherung komplett fallen zu lassen und jedes Objekt, egal wo es sich befindet, grundsätzlich aufgrund der Objekteigenschaften zu authentifizieren. Gilman spricht in diesem Zusammenhang von: „Internet Security Everywhere." [Gilman, 2016, S.13] Dieser Ansatz entspricht einer Verlagerung der Authentifizierung von der Netz- auf die Anwendungsebene unter Verwendung von Nutzer-, Assets- und Ressourceneigenschaften. Die Zero-Trust-Paradigmen in dieser Form können mitunter in Zukunft eine ergänzende Möglichkeit liefern, über die in dieser Arbeit vorgestellten Strategien hinaus, das Risiko und die Schadensauswirkung eines möglichen APT-Angriffs auf die interne Infrastruktur zu reduzieren. Im Fokus steht hierbei der kontrollierte Zugriff auf Unternehmensressourcen bei gleichzeitig steigender Anzahl von mobilen Endgeräten und tendenziell stärkerer Cloud-Nutzungen seitens der Institutionen.

2019 hat das NIST einen ersten Entwurf zur technischen Standardisierung der *Zero Trust Architecture* als NIST Special Publication 800-207 veröffentlicht. [siehe Rose et al., 2020] Für größere Institutionen mit entsprechend weitläufigen Infrastrukturen wird in den kommenden Jahren von Interesse sein, inwiefern Zero-Trust Paradigmen die bisherigen architekturellen Sicherheitsprinzipien unter Verwendung von modernen Authentisierungsverfahren sinnvoll ergänzen können.

Verzeichnisse

Abbildungsverzeichnis

1.1 Drei-Säulen-Modell zur Informationssicherheit 5

2.1 Datenfluss im OSI-7-Schichten-Modell 11
2.2 Beispielhafte Darstellung einer auf mehreren Servern verteilten Anwendung (Identitätsmanagementsystem) 14
2.3 Schematische Darstellung der Client-Server-Architektur 15
2.4 Struktur und Aufgaben eines Rechenzentrums 19
2.5 Ebenen der Kopplung mehrerer Rechenzentren 19
2.6 Zusammenhang der personellen, kontextuellen und technischen Identität 25
2.7 Darstellung des NTLM Authentifizierungsprozesses 29
2.8 Darstellung des Kerberos Authentifizierungsprozesses 32
2.9 Darstellung der Kerberos-Vertrauensstellung 34
2.10 Darstellung der Kerberos-VS-Struktur und -Transitivität 34
2.11 Beispielhafte Darstellung eines Directory Information Tree 37
2.12 Darstellung eines verteilten AVD-Systems 39
2.13 Prinzip einer Zugriffskontrolle 41
2.14 Beispielhaftes Bell-LaPadula-Sicherheitsmodell 47

3.1 Bewegungen des Angreifers im Netzwerk 54
3.2 Die erweiterte CERT-Taxonomie 57
3.3 Darstellung der Cyber-Kill-Chain 59
3.4 Angaben zur Hackergruppe APT28 in der MITRE ATT&CK™ Datenbank 62
3.5 Grafische Analyse mit BloodHound 66
3.6 Ablauf eines Man-In-The-Middle-Angriffs am Beispiel einer NTLM Replay Attacke 70

4.1 Sicherheitsabhängigkeit zwischen Subjekten und einem Objekt 81
4.2 Transitivität zwischen mehreren Subjekten und Objekten 81
4.3 Sicherheitsabhängigkeiten beim Aufbau von AVS- und HSA-Systemen 82
4.4 Mögliche Abhängigkeiten der Sicherheitsschichten 86
4.5 Kommunikations- und Kontrollbeziehungen zwischen den Schichten . 87
4.6 Beispiel einer Berechtigungsaufteilung auf mehrere Konten 91
4.7 Beispiel der Struktur eines Ereignisüberwachungssystems 97

5.1 Struktur einer mittels IPsec abgesicherten HSA im Produktivnetz . . . 102
5.2 Struktur einer HSA in gesonderter Firewall-Zone. 104

5.3 Struktur einer HSA in eigenem LAN/VLAN 105
5.4 HSA als Administrationsforest 108
5.5 Einordnung von PC-Arbeitsplatztypen im Spannungsfeld zwischen Systemberechtigungen und Funktionalität 111
5.6 Einbindung eines Updateservers in die HSA 113

A.1 Prozess der Implementierung und des Betriebs einer HSA 161
A.2 Sub-Prozess der Entwicklung eines Detailkonzeptes 162
A.3 Sub-Prozess des Aufbaus einer Schicht 0 und HSA 163
A.4 Sub-Prozess der Verlagerung eines bereits vorhandenen AVD-Systems 164
A.5 Sub-Prozess des Update- und Patchmanagements 165

Tabellenverzeichnis

2.1 NTLM Kompatibilitätsebenen – LMCompatibilityLevel 30
2.2 Netzwerkdienste eines AVD-Systems 40

3.1 Schritte der Post-Exploitation-Phase 53

4.1 Denkbare Rollenverteilung auf einem System 84
4.2 Schicht 0 äquivalente Gruppen 89
4.3 Richtliniensystem für das MS-AMA-Verfahren 95
4.4 Beispielereignisse eines analytischen Überwachungssystems 99

6.1 Schutzbedarfskategorien 118

Glossar

Air Gap

Ein Air Gap (englisch für „Luftspalt“) bezeichnet in der IT-Technik eine grundsätzliche, physikalische und logische Trennung von IT-Systemen, die trotz der Trennung, in einem Prozess des Datenaustausches zueinander stehen.

AMA

Authentication Mechanism Assurance (AMA; deutsch „Authentifizierungsabsicherung“) beschreibt ein Verfahren, mit dessen Hilfe ein Kerberos Authentifizierungsprozess besonders abgesichert werden kann.

APT-Angriff

Advanced Persistent Threat (Advanced Persistent Threat (APT); deutsch „fortgeschrittene andauernde Bedrohung“) beschreibt eine spezielle Cyber-Attacke, die einen komplexen, zielgerichteten und meist lang andauernden Angriff darstellt, bei dem meist auch hoch spezialisierte Werkzeuge zum Einsatz kommen.

Brute-Force

Ein Brute-Force Verfahren (englisch für „rohe Gewalt “) bezeichnet einen Prozess, welcher durch reines Ausprobieren aller möglichen Varianten versucht eine Lösung zu finden.

C&C

Command and Control (C&C; deutsch „Kommando und Kontrolle“) beschreibt im Zusammenhang mit Cybersecurity einen Computer (Host) der als Plattform für Befehlsausführungen und der Steuerung entfernter Prozesse dient.

Cloud Computing

Cloud Computing (deutsch „Rechnerwolke“ oder „Datenwolke“) beschreibt eine Infrastruktur, bei Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Netzwerk zur Verfügung gestellt wird.

Common Criteria

Common Critera (CC; deutsch „Gemeinsame Kriterien “) beschreibt im Kontext dieser Arbeit einen international anerkannten Katalog von Kriterien um Sicherheitsfunktionalitäten eines Produkts auf vergleichbare Art und Weise prüfbar zu machen. Ziel ist es, eine darauf basierende CC-Zertifizierung transparent und innerhalb der Staatengemeinschaft vergleichbar durchführen zu können.

DNS

Domain Name System (DNS) ist eine der wichtigsten Dienste innerhalb IP-basierter Netzwerke. Er ist für die Zuordnung von Namen (hier menschlich lesbare Namen) in numerische IP-Adressen und vice versa (englisch: reverse DNS) zuständig.

Domäne

Domäne (englisch: domain von lateinisch dominium über französisch domaine „Herrschaft“, „Herrschaftsbereich“) steht in dieser Arbeit für den Zuständigkeitsbereich eines AVD-Systems. Im Bereich der Kerberos-Authentifizierung spricht man in diesem Zusammenhang von *Kerberos Realm*

Domain Controller

Ein Domain Controller (DC, häufig auch Domänencontroller) ist ein Serversystem, das in seinem Zuständigkeitsbereich die Authentifizierung und Autorisierung von Benutzer- und Computerobjekten übernimmt. Die Verfahrensweise wurde von IBM in den 1970er Jahren entwickelt und 1993 von Microsoft für *Windows NT* übernommen. Seit den 1990er Jahren gab es zudem *SAMBA*, die Entwicklung einer Open-Source-Variante.

Gruppenrichtlinienobjekt

Ein Gruppenrichtlinienobjekt (engl. Group Policy Object, GPO) ist in Softwareumgebungen des Herstellers MS ein digitales Richtlinieobjekt, das auf eine Gruppe von Zielobjekte (Benutzer- oder Computerkonten) Systemeinstellungen projiziert.

Infrastructure as a Service

Die Dienstleistung *Infrastructure as a Service* (IaaS) bietet dem Kunden IT-Ressourcen (Rechenleistung, Datenspeicher oder Netzanbindungen) als Dienst an. Der Kunde kann basierend auf dieser Dienstleistung Betriebssysteme und Anwendungen seiner Wahl installieren.

Institutionen

Der Begriff Institution (lateinisch *institutum* „Einrichtung“) wird in dieser Arbeit als Sammelbegriff für Unternehmen, Behörden und andere Organisationen verwendet.

Kerberos

Kerberos ist ein Objekt aus der griechischen Mythologie (deutsch auch Zerberos, „Dämon der Grube“). Im IT-technischen Sinn bezeichnet es ein Authentifizierungsverfahren, welches zwei Kommunikationspartner gegenseitig, basierend auf Tickets und einem asymmetrischen Kryptosystem, authentifiziert.

Microsoft Active Directory®

Das Active Directory® (AD) ist die von Microsoft implementierte Version eines zentralen Authentifizierungs- und Verzeichnisdienstes. Der Zuständigkeitsbereich eines AD wird als Domäne bezeichnet. Ein Server, auf dem die AD-Domain-Services (AD DS) laufen, wird als *Domain Controller* (DC) bezeichnet. Von diesem Server werden folgende Dienste bereit gestellt:

- Lightweight Directory Access Protocol
- NT Lan Manager Authentifizierungsprotokoll
- Kerberos Authentifizierungsprotokoll
- Server Message Block bzw. Common Internet File System
- Domain Name System (optional)

Microsoft Privilege Attribute Certificate Data Structure

Microsoft Privilege Attribute Certificate (MS-PAC; deutsch „Datenstruktur für Berechtigungseigenschaften“) ist ein proprietär vom Hersteller Microsoft implementiertes Datenfeld innerhalb eines Authentifizierungsprozesses, das für die Darstellung von Gruppenmitgliedschaften zur Autorisierung genutzt wird.

.NET Framework

Das .NET Framework ist eine Software-Entwicklungs- und -Laufzeitumgebung des Herstellers Microsoft Corporation (MS). Durch dieses Framework wird die Anwendungskompatibilität zwischen den verschiedenen MS Technologieplattformen und Betriebssystemen erhöht.

Object Identifier

Der Object Identifier (OID; deutsch „Objekt Bezeichner“) ist ein weltweit eindeutiger Knotenname, der ein Informationsobjekt addressiert. Er bildet sich aus einer durch Punkte getrennten Kette von ganzen Zahlen. Die Vergabe und Registrierung wird geregelt durch ISO/OSI 9834, entsprechend DIN 66334.

PDCA-Zyklus

Der PDCA-Zyklus (englisch für Plan – Do – Check – Act) beschreibt einen vierphasigen Ablauf, der der Optimierung von Prozesse dient. Ursprünglich in den

1930ern vom Physiker Walter A. Shewhart vorgestellt, wurde er in den 1980ern durch W. Edwards Deming weiterentwickelt. Er wird daher auch als Demingkreis bezeichnet.

Platform as a Service

Die Dienstleistung *Platform as a Service* (PaaS) bietet dem Kunden auf einer Platform standardisierte Schnittstellen an, ohne ihm dabei Zugriff auf zugrundeliegende Betriebssysteme und Hardware zu geben.

Public Key Infrastructure

Public Key Infrastructure (Public Key Infrastruktur (PKI); deutsch „Infrastruktur für öffenliche Schlüssel“) bezeichnet eine Systemumgebung zur Erzeugung, Verwaltung und Prüfung digitaler Zertifikate, die für Zertifikate ein asymmetrischen Kryptosystems (privatem / öffentlichem Schlüsselpaar) benutzen.

Referenzmodell

Ein allgemeines Modell für eine Klasse von Sachverhalten, das folgende Eigenschaften hat: Auf Basis des allgemeinen Modells können spezielle Modelle (als Grundlage für die Konstruktion ganz bestimmter Sachverhalte) geplant werden.

Remote Procedure Call

Remote Procedure Call (Remote Procedure Call (RPC); deutsch „Aufruf einer fernen Prozedur“) ist eine Kommunikationtechnik für Prozessaufrufe auf entfernten Computern. Die Ausbildung dieser Technik ist proprietär und damit in der Regel zwischen verschiedenen Herstellern nicht kompatible.

Replay-Angriff

Ein Replay-Angriff stellt eine kryptoanalytische Angriffsart dar, bei der ein Angreifer versucht, durch Wiedereinspielung zuvor aufgezeichneter Daten in einen laufenden Authentifizierungsprozess einzudringen.

Rootkit

Ein Rootkit (englisch etwa: „Administratorenbausatz“) bezeichnet eine Zusammenstellung von Softwarewerkzeugen, die auf dem kompromittierten System installiert werden können, um zukünftige Anmeldevorgänge (Logins) des Eindringlings zu verbergen und Prozesse und Dateien zu verstecken. Die Bezeichnung rootkit weist auf den bei unixähnlichen Betriebssystemen als *Administrator* fungierenden Benutzer *root* hin.

Round-Robin-Verfahren

Ein Rundlaufverfahren (englisch: Round Robin) bezeichnet ein Verfahren zur Lastverteilung (englisch: load balancing). Dabei werden gleichartige Ressourcen, die merhmals zur Verfügung stehen, gleichmäßig ausgenutzt. Es wird oft mit der Domain Name System (DNS) Technik verknüpft. Mehrere IP-Adressen werden einem DNS-Namen zugeordnet. Bei Abfragen werden diese alternierend ausgegeben.

Salt

Ein Salt (englisch für Salz) bezeichnet eine bekannte, zufällig gewählte Zeichenfolge, die bei der Berechnung des Hashwertes mit dem Kennwort verknüpft wird, um die Entropie zu erhöhen.

Single Sign-on

Ein Single Sign-on Verfahren (Single Sign-on (SSO), englisch für „Einmalanmeldung“) bezeichnet den Umstand, dass eine Anmeldung nur einmalig mit einer Authentifizierungsprüfung (z. B. durch Eingabe eines Kennwortes) erfolgt und der Authentifizierungsnachweis später nicht mehr abgefragt wird.

Smartcard

Eine Smartcard (oft auch Chipkarte oder Integrated Circuit Card, ICC) bezeichnet eine Kunstoffkarte, auf der eine Mikroprozessor-Logik (Prozessor und / oder nichtflüchtiger Speicher) aufgebracht ist. Mit speziellen kontakt- und / oder kontaktlosen Lesegeräten kann diese Karte beispielsweise zur sicheren Benutzerauthentifizierung genutzt werden.

Software as a Service

Die Dienstleistung *Software as a Service* (SaaS) bietet dem Kunden Softwareanwendungen (meist Web-gestützt) an. In diese Kategorie fallen beispielsweise Kollaborationsanwendungen.

Swapping

Swapping bezeichnet den Prozess der Auslagerung von Daten aus einem begrenzt vorhandenen schnellen Datenspeicher in einen langsameren, aber dafür mit höherer Kapazität vorhandenen Datenspeicher oder das entgegengesetzte Laden. Swapping bedeutet immer einen gewissen Zeitverlust, da für das Verschieben der Daten Zeit benötigt wird.

Thin-Client

Als Thin-Client wird ein sehr kleiner Computer bezeichnet, der über einen Bildschirm und Tastatur zur Ein- und Ausgabe verfügt, jedoch nicht über ein komplexes Betriebssystem mit eigenem Datenspeicher. Er wird über ein Netzwerk mit einem Server (Terminalserver) verbunden, der die Funktionen des üblichen Desktop bereit stellt.

Token

Eine Hardwarekomponente, die im Rahmen des Authentifizierungsprozesses als zweiter Faktor (Besitz) eingesetzt wird.

Tupel

Ein Tupel ist ein mathematisches Objekt, welches aus einer Liste endlich vieler Objekte besteht. Der Unterschied zur mathematischen Menge ist die definierte Reihenfolge der Objekte innerhalb des Tupels. Informationstechnisch entspricht ein Tupel einem Datensatz.

Whois

Whois (englisch *who is* „wer ist“) ist ein Protokoll, mit dessen Hilfe Informationen zu Internet-Domains, IP-Adressen und deren Eigentümern („Registrant“) ermittelt werden können.

Windows Management Instrumentation

Die Windows Management Instrumentation (Windows Management Instrumentation (WMI)) ist die Microsoft Implementierung des Common Information Models (CIM). Durch WMI kann lokal auf dem System oder über das Netzwerk auf nahezu alle Einstellungen eines Windows-basierten Betriebssystems zugegriffen werden (lesend und auch schreibend). Die Netzwerkkommunikation läuft über den sogenannten DCOM-Port (135/TCP).

Zero-Day-Exploit

Ein Exploit wird als Zero-Day-Exploit bezeichnet, wenn er zum Einsatz kommt, bevor es eine entsprechende Gegenmaßnahme in Form eines Sicherheitspatches gibt. Eine von Hackern entdeckte Sicherheitslücke wird gerne geheim gehalten und nicht den entsprechenden Herstellern gemeldet. Diese Zero-Day-Exploit werden zu hohen Summen angeboten und gehandelt.

Abkürzungsverzeichnis

2FA Zwei-Faktor-Authentifizierung 35, 108

ABAC Attribute Based Access Control 42

ACL Access Control List 78, 85

AD Active Directory® 5, 35, 74, 76, 85, 94, 95, *siehe Glossar:* Microsoft Active Directory®

AMA Authentication Mechanism Assurance 7, *siehe Glossar:* AMA

ANSI American National Standards Institute 9

API Application Programming Interface 14, 36, 63

APT Advanced Persistent Threat 1, 135

ARPANET Advanced Research Projects Agency Network 10

ATT&CK™ Adversarial Tactics, Techniques & Common Knowledge 61

AVD Authentifizierungs- und Verzeichnisdienst 2, 6, 24, 42, 51, 80, 127, 129

BDSG Bundesdatenschutzgesetzes 100

BSI Bundesamtes für Sicherheit in der Informationstechnik 4, 5, 128

C&C Command and Control 50, 52, 60, 64, 68, 79, *siehe Glossar:* C&C

CCEB Common Criteria Editorial Board 2

CCITT Comité Consultatif International Télégraphique et Téléphonique 36

CERT Computer Emergency Response Team 99, 122

CIFS Common Internet File System 137

COBIT Control Objectives for Information and related Technology 40

CSP Clean Source Prinzip 80

DAC Discretionary Access Control 42

DIB Directory Information Base 36

DIT Directory Information Tree 37, 132

DLL Dynamic Link Library 21, 76

DNS Domain Name System 31, 39, 70, 137, 139, *siehe Glossar:* DNS

DoS Denial of Service 2, 4, 17

DSA Distributed Systems Architecture 10

DSGVO Datenschutz-Grundverordnung 100

eCSIRT European Computer Security Incident Response Team 55

ESAE Enhanced Security Administrative Envirenment 7

FIDO Fast IDentity Online 35

FQDN Fully Qualified Domain Name 39

GPO Group Policy Object 102, 136, *siehe Glossar:* Gruppenrichtlinienobjekt

HSA hochsichere Administrationsumgebung 7, 82, 87, 89, 93, 101, 109, 112–117, 122, 125, 127, 161

HTML HyperText Markup Language 14

IaaS Infrastructure as a Service 128, 136, *siehe Glossar:* Infrastructure as a Service

IANA Internet Assigned Numbers Authority 40

IdM Identity Management 48

IDS Intrusion Detection System 64, 116

IPsec Internet Protocol Security 71, 102, 103

ISMS Informationssicherheit Management System 40

ISO International Organization for Standardization 9

ITIL® Information Technology Infrastructure Library 41

ITU-T International Telecommunication Union - Telecommunication Standardization Sector 36

KAS Kerberos Authentication Server 31, 74–76, 78

KDC Kerberos Key Distribution Center 31, 78, 93, 94

LAN Local Area Network 13

LAPS Local Administrator Password Solution 115

LDAP Lightweight Directory Access Protocol 35, 36, 66, 137

LLMNR Link Local Multicast Name Resolution 70, 71, 116

LSASS Local Security Authority Subsystem Service 76

LUN Logical Unit Number 20

MAC Mandatory Access Control 42

MFA Multi-Faktor-Authentifizierung 35, 93

MITM Man-in-the-Middle-Angriff 69

MLAPT Machine-Learning APT Correlation Analysis 96

MLS Multi-Level Security 47

MS Microsoft Corporation 5, 7, 21, 22, 24, 27, 29, 38, 63, 67, 72–74, 76, 77, 79, 85, 87, 88, 90–96, 101, 102, 107, 111, 115, 120, 136, 137

MS-DRSR Directory Replication Service Remote Protocol 38, 77, 78

MS-PAC Microsoft Privilege Attribute Certificate Data Structur 74, 94, 95, 137, *siehe Glossar:* Microsoft Privilege Attribute Certificate Data Structure

NBNS NetBIOS Name Service 70, 71

NetBIOS Network Basic Input Output System 70

NIST National Institute of Standards and Technology 43, 61, 128, 130

NTLM NT Lan Manager 27, 72, 73, 96, 137

OID Object Identifier 94, 137, *siehe Glossar:* Object Identifier

OSI Open Systems Interconnection 9, 10

OTP One-Time Password 27

PaaS Platform as a Service 128, 138, *siehe Glossar:* Platform as a Service

PDCA Plan – Do – Check – Act 123, *siehe Glossar:* PDCA-Zyklus

PKI Public Key Infrastruktur 93, 138, *siehe Glossar:* Public Key Infrastructure

PSK Pre Shared Key 12

QoS Quality of Service 3

RBAC Role Based Access Control 42, 108

RDP Remote Desktop Protocol 115

RPC Remote Procedure Call 138, *siehe Glossar:* Remote Procedure Call

SaaS Software as a Service 128, 129, 139, *siehe Glossar:* Software as a Service

SAML Security Assertion Markup Language 35

SAN Storage Area Network 20

SIEM Security Information and Event Management 115

SMB Server Message Block 115, 137

SNA System Network Architecture 10

SQL Structured Query Language 17

SSO Single Sign-on 26, 29, 33, 71, 96, 139, *siehe Glossar:* Single Sign-on

SSPI Security Support Provider Interface 27

ST Kerberos Service Ticket 32, 75

STIX™ Structured Threat Information eXpression 55

TGS Ticket Granting Service 31

TGT Ticket Granting Ticket 32, 74, 75, 94

TOM technische und organisatorische Maßnahmen 4, 7, 103, 115

TTP Trusted Third Party 31

VDI Virtual Desktop Infrastructure 21

VERIS Vocabulary for Event Recording and Incident Sharing 55

VLAN Virtual Local Area Network 20

VM Virtuelle Maschine 20, 23

VS Vertrauensstellung 33

WMI Windows Management Instrumentation 63, 140, *siehe Glossar:* Windows Management Instrumentation

Literaturverzeichnis

Alani, Mohammed M. (2014): *Guide to OSI and TCP/IP Models* -. Berlin, Heidelberg: Springer Verlag. ISBN: 978-3-319-05152-9 (siehe S. 10).

ANSI, American National Standards Institute (2004): *ANSI INCITS, 359-2004 : Role Based Access Control*. zuletzt abgerufen am 1.9.2020. Washington, DC, USA. URL: https://profsandhu.com/journals/tissec/ANSI+INCITS+359-2004.pdf (siehe S. 43).

Barafort, B. et al. (2002): "Benefits Resulting from the Combined Use of ISO/IEC 15504 with the Information Technology Infrastructure Library (ITIL®)". In: *Oivo M., Komi-Sirviö S. (eds) Product Focused Software Process Improvement*. Bd. 2559. Computer Science. Berlin, Heidelberg: Springer, S. 113–313. ISBN: 978-3-540-36209-8. DOI: 10.1007/3-540-36209-6_27 (siehe S. 41).

Bell, D. Elliott; LaPadula, Leonard J. (1973): *Secure computer systems: Mathematical foundations*. zuletzt abgerufen am 1.9.2020. Bedford, MA, USA. URL: https://apps.dtic.mil/sti/pdfs/AD0770768.pdf (siehe S. 45).

Bengel, Günther (2015): *Grundkurs Verteilte Systeme - Grundlagen und Praxis des Client-Server und Distributed Computing*. Berlin Heidelberg New York: Springer Verlag. ISBN: 978-3-834-82150-8 (siehe S. 12, 13, 15).

Bertocci, Vittorio (2016): *Modern Authentication with Azure Active Directory for Web Applications*. Redmond, Washington, USA: Microsoft Press. ISBN: 978-0-7356-9694-5 (siehe S. 35).

Bitkom e.V., BITKOM Bundesverband Informationswirtschaft (2015): *Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz im digitalen Zeitalter*. zuletzt abgerufen am 10.8.2020. URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf (siehe S. 121, 122).

BMI, Bundesministerium des Innern (2009): *Allgemeine Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Abs. 6 BSIG*. zuletzt abgerufen am 10.6.2020. URL: http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_08122009_IT5606000111.htm (siehe S. 55).

Borchers, Jens; Hamburg, Sopra Steria Consulting (2016): "Migration auf cloudbasierte Plattformen aus Sicht des klassischen Reengineering". In: *Softwaretechnik-Trends* 36.2 (siehe S. 128).

BSI, Bundesamt für Sicherheit in der Informationstechnik (2011a): *IT-Grundschutz Baustein B 3.304 Virtualisierung*. zuletzt abgerufen am 3.8.2020. URL: https://

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-GS-Bausteine/Virtualisierung/Baustein_Virtualisierung-B3_304.pdf?__blob=publicationFile&v=1 (siehe S. 92).

BSI, Bundesamt für Sicherheit in der Informationstechnik (2011b): *Leitfaden IT-Forensik*. zuletzt abgerufen am 29.9.2020. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/IT-Forensik/forensik_node.html (siehe S. 57).

– (2015): *Die Lage der IT-Sicherheit in Deutschland 2015*. Version 1.0. Bonn: Bundesanzeiger Verlag (siehe S. 120).

– (2016): *Ein Praxis-Leitfaden für IS-Penetrationstests*. zuletzt abgerufen am 23.9.2020. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/FSicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf (siehe S. 123, 124).

– (2017a): *IT-Grundschutz-Methodik, BSI-Standard 200-2*. Version 1.0. Bonn: Bundesanzeiger Verlag (siehe S. 83, 118).

– (2017b): *Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1*. Version 1.0. Bonn: Bundesanzeiger Verlag (siehe S. 83).

– (2017c): *Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3*. Version 1.0. Bonn: Bundesanzeiger Verlag (siehe S. 125).

– (2019a): *Die Lage der IT-Sicherheit in Deutschland 2019*. Version 1.0. Bonn: Bundesanzeiger Verlag (siehe S. 4, 5, 119).

– (2019b): *IT-Grundschutz-Kompendium*. Edition 2019. Bonn: Bundesanzeiger Verlag. ISBN: 978-3-846-20906-6 (siehe S. 8, 18, 90, 110).

Bucksteeg, M. et al. (2012): *ITIL® 2011 - der Überblick - Alles Wichtige für Einstieg und Anwendung*. 1. Auflage. München: Addison-Wesley Verlag. ISBN: 978-3-827-33128-1 (siehe S. 41).

Bütler, Ivan (2011): "Advanced Persistent Threats: die jüngste und gefährlichste Generation der Sicherheitsbedrohung". In: *netzwoche*. zuletzt abgerufen am 17.7.2020. URL: https://media.hacking-lab.com/ibuetler/NW11_11_Dossier_Digicomp.pdf (siehe S. 50, 51).

Cater-Steel, Aileen et al. (2006): "Transforming IT service management-the ITIL® impact". In: *Proceedings of the 17th Australasian Conference on Information Systems*. ACIS 2006. Australasian Association for Information Systems (siehe S. 41).

CCITT, Comité Consultatif International Télégraphique et Téléphonique (1989): *Data Communication Networks Directory Recommendations X.500-X.521*. zuletzt abgerufen am 15.9.2020. Geneva, Switzerland: ITU. ISBN: 92-61-03731-3. URL: https://dl.acm.org/doi/pdf/10.17487/RFC1823 (siehe S. 36, 37).

Cervone, Frank (2008): “ITIL®: a framework for managing digital library services”. In: *OCLC Systems & Services: International digital library perspectives*. Vol.24-Nr.2. Emerald Group Publishing Limited, S. 87–90. DOI: 10.1108/10650750810875430 (siehe S. 41).

Chen, Ping et al. (2014): “A Study on Advanced Persistent Threats”. In: *Communications and Multimedia Security*. Hrsg. von De Decker, Bart; Zúquete, André. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 63–72. ISBN: 978-3-662-44885-4 (siehe S. 49).

Cook, Melanie; Eikenberry, Heather (2001): *Guide to Securing Windows NT/9x Clients in a Windows 2000 Network*. zuletzt abgerufen am 14.8.2020. URL: https://apps.dtic.mil/sti/pdfs/ADA401579.pdf (siehe S. 30).

Core Security (2020): *Red Team*. zuletzt abgerufen am 23.9.2020. URL: https://www.coresecurity.com/penetration-testing/red-team (siehe S. 125).

Danielsson, Johan; Westerlund, Assar (1998): “Heimdal: An Independent Implementation of Kerberos 5”. In: *Proceedings of the Annual Conference on USENIX Annual Technical Conference*. ATEC ’98. New Orleans Louisiana USA: USENIX Association, S. 34 (siehe S. 6).

Deming, W. Edwards (1982): *Out of Crisis*. Cambridge, MA, USA: MIT Press. ISBN: 978-0-262-54115-2 (siehe S. 123).

Diathesopoulos, George (2017): “Computer Laboratory Setup for the Assessment of State-of-the-Art Penetration Testing Tools”. zuletzt abgerufen am 25.6.2020. Master Thesis. University of Piraeus. URL: http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/10380/Diathesopoulos_George.pdf (siehe S. 65).

Dreyfus, P. (1998): “The second wave. Netscape on usability in the services-based Internet”. In: *IEEE Internet Computing* 2.2, S. 36–40 (siehe S. 14).

Eckert, Claudia (2018): *IT-Sicherheit - Konzepte - Verfahren - Protokolle*. 10.Auflage. Berlin: Walter de Gruyter GmbH & Co KG. ISBN: 978-3-110-56390-0 (siehe S. 3, 4, 6, 11, 21, 42–47, 69).

Edelkamp, Stefan (2016): *Lehrbrief IT-Sicherheit, Kap. 7: Zugriffskontrolle*. Sommersemester 2016. zuletzt abgerufen am 1.9.2020. Darmstadt: Hochschule Darmstadt. URL: https://nms.kcl.ac.uk/stefan.edelkamp/lectures/itsec/slides/itsec-ws16-chap07-actrl.pdf (siehe S. 41, 45).

Eichler, Brigitte (1993): *Informations- und Vermittlungsdienste in offenen verteilten Systemen*. Wien: ADV Handelsges. ISBN: 978-3-901-19807-6 (siehe S. 36).

Falliere, Nicolas et al. (2012): *APT Case Study - W32.Stuxnet Dossier*. zuletzt abgerufen am 17.7.2020. URL: https://engineering.purdue.edu/dcsl/reading/2012/chris_apt_case_study.pdf (siehe S. 51).

Ferraiolo, David et al. (1995): “Role-based access control (RBAC): Features and motivations”. In: *Proceedings of 11th annual computer security application conference*. zuletzt abgerufen am 14.8.2020. National Institute of Standards und Technology (NIST), S. 241–48. URL: https://www.researchgate.net/profile/D_Kuhn2/publication/238743515_Role-based_access_control_features_and_motivations/links/562e7d3808ae04c2aeb5d98b.pdf (siehe S. 43).

Geschonneck, Alexander (2014): *Computer-Forensik (iX Edition) - Computerstraftaten erkennen, ermitteln, aufklären*. 6. Auflage. Heidelberg: dpunkt.verlag. ISBN: 978-3-86490-133-1 (siehe S. 49–51, 57, 117).

Ghafir, Ibrahim et al. (2018): “Detection of advanced persistent threat using machine-learning correlation analysis”. In: *Future Generation Computer Systems* 89, S. 349–359 (siehe S. 96).

Gilman, Evan (2016): “Zero Trust: Building Systems in Untrusted Networks”. In: *30th USENIX Large Installation System Administration Conference (USENIX LISA 16)*. zuletzt abgerufen am 24.9.2020. Boston, MA, USA: USENIX Association. URL: https://www.usenix.org/sites/default/files/conference/protected-files/lisa16_slides_gilman.pdf (siehe S. 129, 130).

Glass, Eric (2003): *The NTLM Authentication Protocol and Security Support Provider*. zuletzt abgerufen am 14.8.2020. URL: http://davenport.sourceforge.net/ntlm.html (siehe S. 27, 28).

Glinz, Martin (2005): *Lehrbrief Informatik II: Modellierung*. zuletzt abgerufen am 4.5.2020. URL: https://files.ifi.uzh.ch/rerg/arvo/ftp/inf_II/inf_II_kapitel_12.pdf (siehe S. 18).

Graeber, Matthew (2011): *PowerShell-based Code/Dll Injection Utility*. zuletzt abgerufen am 25.6.2020. URL: http://www.exploit-monday.com/2011/11/powersyringe-powershell-based-codedll.html (siehe S. 65).

– (2012): *PowerSploit -A PowerShell Post-Exploitation Framework*. zuletzt abgerufen am 25.6.2020. URL: http://www.exploit-monday.com/2012/05/powersploit-powershell-post.html (siehe S. 65).

Graham, G. Scott; Denning, Peter J. (1972): “Protection: Principles and Practice”. In: *Proceedings of the Spring Joint Computer Conference*, S. 417–429. DOI: 10.1145/1478873.1478928 (siehe S. 41).

Grobauer, B. et al. (2016): “Klassifikation von IT-Sicherheitsvorfällen”. In: *Datenschutz und Datensicherheit - DuD* 40. zuletzt abgerufen am 10.6.2020. DOI: 10.1007/s11623-016-0536-7. URL: https://link.springer.com/content/pdf/10.1007/s11623-016-0536-7.pdf (siehe S. 55).

Gutmann, Peter (2000): *X.509 Style Guide*. zuletzt abgerufen am 5.9.2020. URL: https://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt (siehe S. 93).

Häckelmann, H. et al. (2000): "Verzeichnissysteme". In: *Kommunikationssysteme*. Berlin, Heidelberg: Springer, S. 389–402. ISBN: 978-3-540-67496-2. DOI: 10.1007/978-3-642-57242-5_27 (siehe S. 36–38).

Heise Security (2020): *Massiver Angriff auf A1 Telekom Austria*. zuletzt abgerufen am 3.10.2020. URL: https://www.heise.de/hintergrund/Massiver-Angriff-auf-A1-Telekom-Austria-4775451.html (siehe S. 1).

Howard, John D.; Longstaff, Thomas A. (1998): *A Common Language for Computer Security Incidents*. zuletzt abgerufen am 18.07.2019. URL: https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/1998/988667.pdf (siehe S. 56).

Howes, T.; Smith, M. (1995): *RFC 1823: The LDAP Application Program Interface*. zuletzt abgerufen am 15.9.2020. University of Michigan. URL: https://dl.acm.org/doi/pdf/10.17487/RFC1823 (siehe S. 36).

Hubner, Edith (2019): *Cybercrime: Eine Einführung*. Wiesbaden: Springer VS. ISBN: 978-3-658-26149-8. DOI: 10.1007/978-3-658-26150-4 (siehe S. 56).

Hutchins, Eric et al. (2011): "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains". In: *Leading Issues in Information Warfare and Security Research*. Hrsg. von Ryan, Julie. Reading, RG4 9AY, UK: Academic Conferences Limited, S. 80–100 (siehe S. 58).

ISO, International Organization for Standardization (1982): *DIN/IEC/ISO 7498-1: Informationsverarbeitung Kommunikation Offener Systeme, Basis-Referenzmodell, ISO/OSI-Modell*. Geneva, CH: Beuth Verlag (siehe S. 10).

– (1999): *ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation*. zuletzt abgerufen am 9.9.2020. URL: https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v21.pdf (siehe S. 2).

– (2011): *ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management*. Geneva, CH (siehe S. 55).

Jonas, Ernst (2019): *Lehrbrief Systemanalyse und Systemhärtung*. Wintersemester 2019/2020. Wismar: WINGS GmbH (siehe S. 56).

Jones, Michael; Hardt, Dick (Okt. 2012): *The OAuth 2.0 Authorization Framework: Bearer Token Usage*. RFC 6750. zuletzt abgerufen am 13.8.2020. DOI: 10.17487/RFC6750. URL: https://rfc-editor.org/rfc/rfc6750.txt (siehe S. 35).

Kaffel-Ben Ayed, Hella (2016): "A generic Kerberos-based access control system for the cloud". In: *Annals of Telecommunications*, S. 555–567. DOI: 10.1007/s12243-016-0534-7 (siehe S. 129).

Kazanciyan, Ryan; Hastings, Matt (2014): *Investigating PowerShell Attacks*. zuletzt abgerufen am 25.6.2020. URL: https://docs.huihoo.com/blackhat/usa-2014/us-14-Kazanciyan-Investigating-Powershell-Attacks-WP.pdf (siehe S. 65).

Kiltz, Stefan et al. (2007): "Taxonomy for computer security incidents". In: *Cyber Warfare and Cyber Terrorism*. IGI Global, S. 421–418 (siehe S. 56).

Kindervagwith, John et al. (2010): *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. zuletzt abgerufen am 24.9.2020. URL: http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf (siehe S. 129).

Kohl, J.; Neuman, C. (1993): *RFC 1510: The Kerberos Network Authentication Service (V5)*. zuletzt abgerufen am 7.9.2020. URL: https://www.hjp.at/(st_a)/doc/rfc/rfc1510.html (siehe S. 30).

Köhntopp, Marit (2001): ""Wie war noch gleich Ihr Name? Schritte zu einem umfassenden Identitätsmanagement". In: *Verlässliche IT-Systeme 2001: Sicherheit in komplexen IT-Infrastrukturen*. Hrsg. von Fox, Dirk et al. Wiesbaden: Vieweg+Teubner Verlag, S. 55–55. ISBN: 978-3-663-05918-9. DOI: 10.1007/978-3-663-05918-9_5 (siehe S. 48).

Kono, K. et al. (2018): "An Unknown Malware Detection Using Execution Registry Access". In: *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. Bd. 02, S. 487–491 (siehe S. 49).

Kühner, Anja (2012): "Online-Banking – Konten der „High Roller" geplündert". In: *Wirtschaftsinformatik & Management* 4.1, S. 22–23. DOI: 10.1365/s35764-012-0173-3 (siehe S. 49).

Kumar, Rakesh; Charu, Shilpi (2015): "An importance of using virtualization technology in cloud computing". In: *Global Journal of Computers & Technology* 1.2. zuletzt abgerufen am 4.5.2020. URL: https://www.academia.edu/download/37821093/21-180-1-PB.pdf (siehe S. 20).

Lipp, Moritz et al. (Aug. 2018): "Meltdown: Reading Kernel Memory from User Space". In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, S. 973–990. ISBN: 978-1-939133-04-5. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/lipp (siehe S. 3, 92, 128).

Mansfield-Devine, Steve (2018): "The best form of defence – the benefits of red teaming". In: *Computer Fraud & Security* vol 10. zuletzt abgerufen am 17.4.2020, S. 8–12. DOI: 10.1016/S1361-3723(18)30097-6 (siehe S. 124).

Maynor, David et al. (2017): *The MeDoc Connection*. zuletzt abgerufen am 9.6.2020. URL: https://blog.talosintelligence.com/2017/07/the-medoc-connection.html (siehe S. 81).

Mell, Peter; Grance, Timothy (2020): "The NIST Definition of Cloud Computing". In: zuletzt abgerufen am 5.10.2020. National Institute of Standards und Technology (NIST). URL: https://nvlpubs.nist.gov/nistpubs/FLegacy/SP/nistspecialpublication800-145.pdf (siehe S. 128).

Metcalf, Sean (2016): "Beyond the MCSE:Active Directory for the Security Professional". In: *19th Black Hat USA Conference*. Las Vegas, USA: Trimarc Security. URL: https://www.blackhat.com/docs/us-16/materials/us-16-Metcalf-Beyond-The-MCSE-Active-Directory-For-The-Security-Professional-wp.pdf (siehe S. 115).

Microsoft (1996): *NTLM Pass-Through Authentication*. zuletzt abgerufen am 17.09.2020. URL: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-apds/5bfd942e-7da5-494d-a640-f269a0e3cc5d (siehe S. 29).

– (2007): *The ntlm authentication protocol*. zuletzt abgerufen am 14.8.2020. URL: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-nlmp/ (siehe S. 27, 29).

– (2012): *Authentication Mechanism Assurance for AD DS in Windows Server 2008 R2 Step-by-Step Guide*. zuletzt abgerufen am 27.7.2020. URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd378897(v=ws.10) (siehe S. 94).

– (2015): *Authentifizierungsrichtlinien und Authentifizierungsrichtliniensilos*. zuletzt abgerufen am 23.9.2020. URL: https://support.microsoft.com/de-de/help/3062591/microsoft-security-advisory-local-administrator-password-solution-laps (siehe S. 115).

– (2018): *Microsoft Kerberos*. zuletzt abgerufen am 5.09.2020. URL: https://docs.microsoft.com/de-de/windows/win32/secauthn/microsoft-kerberos (siehe S. 22).

– (2019a): *Advanced Threat Analytics-Handbuch zu verdächtigen Aktivitäten*. zuletzt abgerufen am 23.08.2020. URL: https://docs.microsoft.com/de-de/advanced-threat-analytics/suspicious-activity-guide (siehe S. 99).

– (2019b): *Enhanced Security Administrative Environment*. zuletzt abgerufen am 11.07.2019. URL: https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material (siehe S. 80, 81, 83, 87–89, 115).

– (2019c): *Privileged Access Workstations*. zuletzt abgerufen am 2.01.2020. URL: https://docs.microsoft.com/de-de/windows-server/identity/

securing-privileged-access/privileged-access-workstations (siehe S. 90, 111, 115).

Microsoft (2020): *How to configure a firewall for Active Directory domains and trusts*. zuletzt abgerufen am 20.09.2020. URL: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts (siehe S. 40).

Miessler, Daniel (2019): *The Definition of a Purple Team*. zuletzt abgerufen am 23.9.2020. URL: https://danielmiessler.com/study/purple-team/ (siehe S. 125).

Moen, R.; Norman, C. (2009): "Evolution of the PDCA Cycle". In: *7th ANQ Congress*. zuletzt abgerufen am 3.10.2020. Tokyo, JP: Asian Network for Quality. URL: https://Frauterberg.employee.id.tue.nl/lecturenotes/DG000%2520DRP-R%2Freferences/Moen-Norman-2009.pdf (siehe S. 123).

Moreira, Baesso G. et al. (2018): "Extending the VERIS Framework to an Incident Handling Ontology". In: *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*. Santiago, Chile: IEEE Computer Society, S. 440–445. ISBN: 978-1-538-67326-3. DOI: 10.1109/WI.2018.00-55 (siehe S. 55).

Neumann, J. von (1945): *First draft of a report on the EDVAC*. 30 Juni 1945. Ausz. in RandellRandell, 2013. University of Pennsylvania: Moore School of Electrical Engineering. ISBN: 978-3-642-61812-3 (siehe S. 3).

Niemann, Klaus D. (1995): *Client/Server-Architektur - Organisation und Methodik der Anwendungsentwicklung*. Wiesbaden: Springer Vieweg. ISBN: 978-3-663-00170-6 (siehe S. 12, 14).

Nusser, Stefan (1998): "Verzeichnisdienst". In: *Sicherheitskonzepte im WWW*. Berlin, Heidelberg: Springer, S. 107–116. ISBN: 978-3-540-63391-4. DOI: 10.1007/978-3-642-80474-8_6 (siehe S. 36).

Pereira, O. et al. (2018): "Formal Analysis of the FIDO 1.x Protocol". In: *Foundations and Practice of Security. FPS 2017. Lecture Notes in Computer Science* 10723. Hrsg. von Imine, A. et al. DOI: 10.1007/978-3-319-49109-7_90 (siehe S. 35).

Plattner, H. (1993): *Client/Server-Architekturen. In: Scheer AW. (eds) Handbuch Informationsmanagement*. Wiesbaden: Gabler Verlag. ISBN: 978-3-322-82846-0 (siehe S. 12).

Poeppelman, Jared (2020): *Reset the krbtgt account password/keys*. zuletzt abgerufen am 13.7.2020. URL: https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51 (siehe S. 76, 79).

Powell, Brian A. (2019): "The epidemiology of lateral movement: exposures and countermeasures with network contagion models". In: *Cyber Security Technology*. zuletzt

abgerufen am 25.6.2020. DOI: 10.1080/23742917.2019.1627702. URL: https://ui.adsabs.harvard.edu/abs/2019arXiv190307741P (siehe S. 67).

PRESECURE, Consulting GmbH (2002): *WP4 Clearinghouse Policy*. zuletzt abgerufen am 10.6.2020. URL: http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6 (siehe S. 55).

Proehl, Mark (2012): *Kerberos - Single Sign-on in gemischten Linux/Windows-Umgebungen*. 1. Auflage. Heidelberg: dpunkt.verlag. ISBN: 978-3-864-91095-1 (siehe S. 27, 29, 31–33).

Raab-Düsterhöft, Antje (2018): *Lehrbrief Einführung in die IT-Sicherheit und Forensik*. Wintersemester 2018/2019. Wismar: WINGS GmbH (siehe S. 40).

Randell, B. (2013): *The Origins of Digital Computers - Selected Papers*. Berlin, Heidelberg: Springer Verlag. ISBN: 978-3-642-61812-3 (siehe S. 3, 153).

Raza, Khalid; Turner, Mark (2002): *Cisco Network Topology and Design*. zuletzt abgerufen am 24.9.2020. URL: https://www.ciscopress.com/articles/printerfriendly/25188 (siehe S. 129).

Robbins, Andrew; Vazarkar, Rohan (2018): *BloodHound: Six Degrees of Domain Admin*. zuletzt abgerufen am 25.6.2020. URL: https://github.com/BloodHoundAD/BloodHound (siehe S. 66).

Rogall, Rolf et al. (2019): *Industrial Security: WLAN-Sicherheit*. Dokument auf der CD. HS Wismar, Modul: Industrial Security, Gruppe HH-2, Semesterarbeit. URL: CD://HH2_WLAN_Security_Ausarbeitung_final.pdf (siehe S. 12).

Rose, Scott et al. (2020): "Zero Trust Architecture". In: zuletzt abgerufen am 24.9.2020. National Institute of Standards und Technology (NIST). DOI: 10.6028/NIST.SP.800-207. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (siehe S. 130).

Rosenberg, Jonathan B.; Remy, David L. (2004): *Securing web services with WS-security: Demystifying WS-security, WS-policy, SAML, XML signature, and XML encryption*. Sams Publishing. ISBN: 978-0-672-32651-6 (siehe S. 35).

Sandhu, Ravi (1996): "Role hierarchies and constraints for lattice-based access controls". In: *Computer Security — ESORICS 96*. Hrsg. von Bertino, Elisa et al. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 65–79. ISBN: 978-3-540-70675-5" (siehe S. 43).

Sanger, David E. (2012): *Confront and conceal: Obama's secret wars and surprising use of American power*. München: Penguin Verlag Random House. ISBN: 978-0-307-71802-0 (siehe S. 119).

Steffens, Timo (2018): *Auf der Spur der Hacker : Wie man die Täter hinter der Computer-Spionage enttarnt*. Berlin: Springer Vieweg. ISBN: 978-3-662-55953-6 (siehe S. 49, 68, 118, 119).

Steiner, Jennifer G. et al. (1988): “Kerberos: An Authentication Service for Open Network Systems”. In: *Project Athena*. Massachusetts Institute of Technology. Cambridge, MA, USA (siehe S. 6, 32).

Trust, Corporate (2016): *Golden Ticket und Pass the Hash: dringende TODOs*. zuletzt abgerufen am 22.9.2020. URL: https://www.corporate-trust.de/wp-content/uploads/2016/07/Manahmenempfehlungen-gegen-Golden-Tickets.pdf (siehe S. 115, 116).

Tsolkas, Alexander; Schmidt, Klaus (2017): *Rollen und Berechtigungskonzepte - Identity- und Access-Management im Unternehmen*. 2. Aufl. Berlin Heidelberg New York: Springer-Verlag. ISBN: 978-3-658-17987-8 (siehe S. 25, 26).

Wahl, M. (1997): *RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3*. zuletzt abgerufen am 15.9.2020. URL: https://dl.acm.org/doi/pdf/10.17487/RFC2256 (siehe S. 36).

Wahl, M. et al. (1997): *RFC 2251: Lightweight Directory Access Protocol (v3)*. zuletzt abgerufen am 15.9.2020. URL: https://dl.acm.org/doi/pdf/10.17487/RFC2251 (siehe S. 36).

Wegener, Christoph (2014): *Lehrbrief Management der Informationssicherheit*. 1. Aufl. zuletzt abgerufen am 5.5.2020. Bochum: Ruhr-Universität Bochum. URL: https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/1998/988667.pdf (siehe S. 3, 5).

Yeong, W. et al. (1993): *RFC 1487: X.500 Lightweight Directory Access Protocol*. zuletzt abgerufen am 15.9.2020. URL: https://dl.acm.org/doi/pdf/10.17487/RFC1487 (siehe S. 36).

– (1995): *RFC 1777: Lightweight Directory Access Protocol*. zuletzt abgerufen am 5.9.2020. URL: https://dl.acm.org/doi/pdf/10.17487/RFC1777 (siehe S. 36).

Zeilenga, K. (2006a): *RFC 4510: Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*. zuletzt abgerufen am 15.9.2020. OpenLDAP Foundation. URL: https://tools.ietf.org/pdf/rfc4510.pdf (siehe S. 36).

– (2006b): *RFC 4520: Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)*. zuletzt abgerufen am 15.9.2020. OpenLDAP Foundation. URL: https://tools.ietf.org/pdf/rfc4520.pdf (siehe S. 36).

Zhang, J. et al. (2017): “Security Analysis of OpenID Connect Protocol with Cryptoverif in the Computational Model”. In: *Cloud and Internet Computing. 3PGCIC 2016. Lecture Notes on Data Engineering and Communications Technologies* 1. Hrsg. von Xhafa, F. et al. DOI: 10.1007/978-3-319-49109-7_90 (siehe S. 35).

Index

*-Eigenschaft, 46
2FA, 93

access matrix model, 41
ADAL, 35
Administrationsforest, 107
Advanced Persistent Thread, 49
AMA-Verfahren, 93
Anmeldeinformation, 26
Anwendungsadministration, 22
Anwendungsvirtualisierung, 21
Arbeitsspeichervirtualisierung, 21
Assume-Breach-Paradigma, 119, 126
ATT&CK™, 61
Attribute Based Access Control, 42
Authentication Mechanism Assurance, 94
Authentifizierung, 26
Authentifizierungsabsicherung, 93
Authentifizierungsfirewall, 108
Authentifizierungsverfahren, 26
Authentikator, 30

Backend, 13
Balancer, 16
Batch Processing, 12
Bell-LaPadula-Modell, 45
Benutzerkonto, 25
Berechtigungsaufteilung, 91
Berechtigungsnachweis, 90
BloodHound, 65
Blue Team, 124
Broker, 16
Brute-Force-Angriff, 17

CERT, 99
CERT-Taxonomie, 56
CIA-Triade, 3
Client-Server-Bäumen, 16
Client-Server-Ketten, 16
Client-Server-Modell, 15
Client-Server-Server, 15
Client-Server-Systeme, 13
Cloud Computing, 20
Cloudbasierte Architekturen, 128
Commandlet, 63
Common Sense Security, 129
Computerkonto, 25
credential, 26, 90
Credential Cache, 71
Credential Guard, 73
Credential Partitioning, 91
Credential Theft, 52
Cyber-Kill-Chain, 57, 58

Defense Evasion, 62
Desktopvirtualisierung, 21
Dienstkonto, 17, 25
Directory Information Base, 36
Directory Information Tree, 37
Discretionary Access Control, 42
Domäne, 5, 33
Drei-Säulen-Modell, 5

Einmalkennwort, 27
Ereignisüberwachung, 96
Ereignissklassifizierung, 99
Exfiltration, 62
Exploitation, 60

Footprinting, 58
Frontend, 13

Generalschlüssel, 77
Golden-Ticket, 75

heterogenes Netzwerk, 21
Honeypot Object, 100
Horizontalbewegung, 54

Identität, 24
Identitätsdiebstahl, 52
Identitätsmanagement, 48
Incident Management, 122
Informationsfluss, 43
Informationssicherheit, 3
Informationsverbund, 83
Institutionen, 2
Integrität, 3
Integritätsüberprüfung, 83
Internetworking Netzwerkmodell, 129
Inveigh, 70
IT-Betriebs-Bereich, 18
IT-Schattensysteme, 129
IT-Sicherheit, 3

Kennwort-Richtlinie, 27
Kerberos, 27
Kerberos-Authentifizierungsprotokoll, 30
Kerberos-Principal-Name, 31
Kerberos-Realm, 33
Kerberos-Schlüsselverteilungscenter, 31
Kerberos-Trust, 33
Kill-Chain, 57
Kollaborationsanwendung, 128
Kompromittierung, 49
Kontrollserver, 68
Kronjuwelen, 118

Lateral Movement, 53, 62
LDAP-Protokoll, 35
LLMNR Verfahren, 70
Local Security Authority Subsystem Server (LSASS), 76

Man-in-the-Middle-Angriff, 69
Mandatory Access Control, 42
Meltdown, 3, 92
Metaverzeichnisse, 48
Mimikatz, 67
MITRE Corporation, 55, 61
MS-AMA, 94
Multi-Level Security, 47

Netzwerksonden, 98
Netzwerkvirtualisierung, 20
Nishang, 64
no-read-up Regel, 46
no-write-down Regel, 46
NTLM, 27
NTLM Pass-Through Authentication, 29

OAuth, 35
OSI-Modell, 9
Over-Pass-the-Hash, 73

Pass-the-Cache, 74
Pass-the-Hash, 71
Pass-the-Ticket, 73
Password Policy, 27
Peer-to-Peer Netz, 13
Penetrationstest, 63, 123
Perimeterabsicherung, 130
Pipe, 16
Post-Exploitation-Phase, 53
PowerShell, 63
PowerSploit Framework, 65
Principal, 30
Privilege Escalation, 54, 62
Privileged Access Workstations, 90

Proxy, 16
Purple Team, 125

RBAC-Modell, 42
Rechte-Eskalation, 54
Reconnaissance, 58
Red Teaming, 124
Red-Forest, 107
Referenzmodell, 9
Replay-Angriff, 69
Risikoanalyse, 117
Risikobewertung, 117
Role Based Access Control, 42
Rollenbasierte Zugriffskontrolle, 45
rootkit, 60

Schichtenmodell, 87
Schutzbedarf, 84
Schutzbedarfskategorien, 118
Schutzziele, 3
Schwachstellenanalyse, 63
Security Assessment, 123
Security Baselines, 111
Security Best Practices, 115
Seitwärtsbewegung, 53
Self-Service-Portal, 48
Serveradministration, 23
Serverkette, 16
Servervirtualisierung, 20
Service Account, 17
Session Key, 30
Sicherheitsabhängigkeit, 80
Silver-Ticket, 75
Simple-Security, 46
Sitzungsschlüssel, 30
Skeleton-Key, 77
Skeleton-Key-Angriff, 76
Smartcard-Anmeldung, 93
Spectre, 3, 92
Speichervirtualisierung, 20
Stapelverarbeitung, 12
Supply-Chain-Attack, 81

technische Identität, 25
Technischer Support Bereich, 18
Tier-0-Äquivalenz, 89
Tier-Modell, 87
Timesharing, 12
Timesharing-Systeme, 12
Trader, 16
Trust Boundary, 109

Verbindlichkeit, 4
Verfügbarkeit, 3
Verteilte Systeme, 13
Vertikalbewegung, 54
Vertrauensgrenze, 109
Vertrauensstellung, 33, 108, 115
Vertraulichkeit, 3
Verzeichnisdienst, 35
Virtualisierung, 18
Von-Neumann-Architektur, 3

Weaponization, 58

X.500-Standard, 36
X.509v3 Zertifikate, 93

Zero Day Exploits, 60
Zero-Trust-Architektur, 130
Zugriffskontrolle, 26
Zugriffsmatrix-Modell, 41
Zugriffsmodell, 41
Zurechenbarkeit, 4
Zwei-Faktor-Authentifizierung, 93

Selbstständigkeitserklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Es wurden keine anderen als die angegebenen Stellen und Hinweise verwandt.
Alle Quellen, die dem World Wide Web entnommen oder in einer sonstigen digitalen Form verwendet wurden, sind der Arbeit beigefügt. Der Durchführung einer elektronischen Plagiatsprüfung stimme ich hiermit zu. Die eingereichte Datei entspricht der eingereichten Druckfassung.
Die vorliegende Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Rangsdorf, 7. Oktober 2020 .....

Thesen

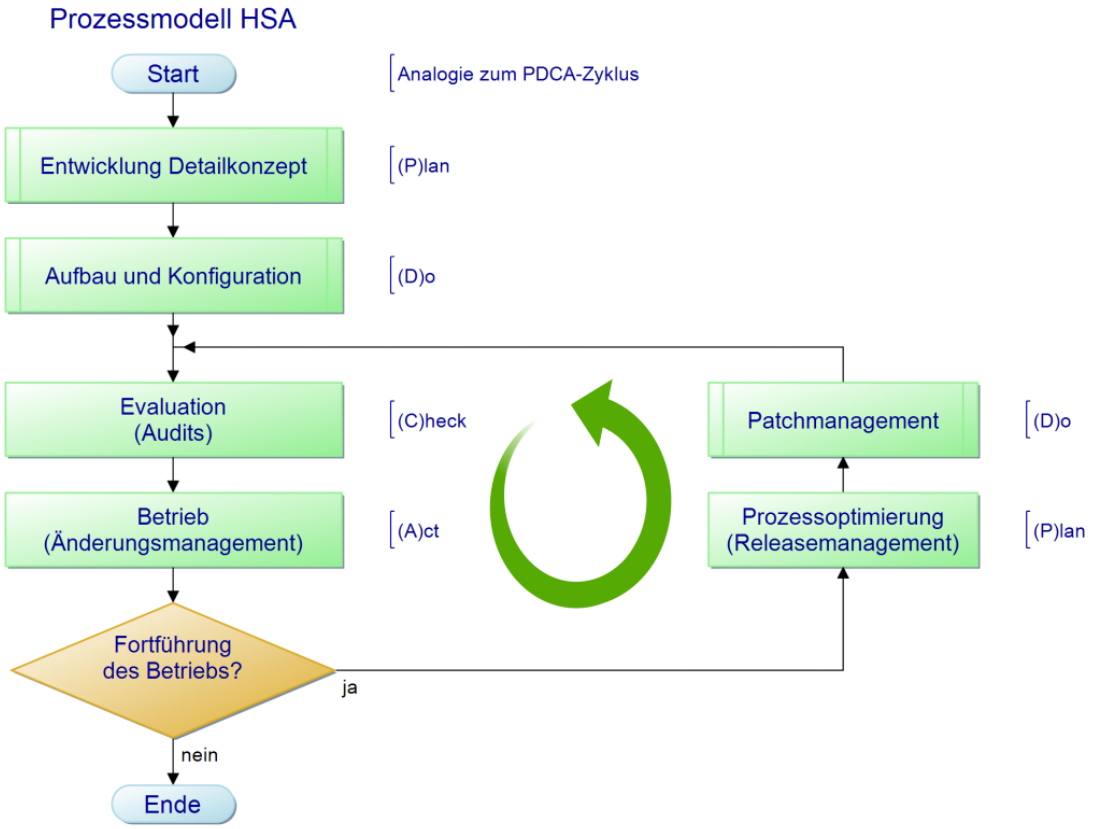
Folgende diskussionswürdige Schwerpunkte werden in dieser Arbeit vorgestellt:

- **Ein sicheres, vernetztes System ist eine Utopie.**
  (vgl. Abschnitt 1.1, auf Seite 2)
- **Daten sind in einer Von-Neumann-Architektur grundsätzlich unsicher.**
  (vgl. Abschnitt 1.2, auf Seite 3)
- **Authentifizierungssysteme mit Single Sign-On (SSO) sind grundsätzlich nicht sicher.**
  (vgl. Abschnitt 2.4.1, auf Seite 26)
- **In größeren Institutionen gehören kompromittierte Arbeitsstationen zur ständigen Bedrohungslage.**
  (vgl. Fußnote 3, auf Seite 52)
- **Ist ein hoch privilegierter Account kompromittiert, ist davon auszugehen, dass ein Golden Ticket erzeugt wurde.**
  (vgl. Fußnote 20, auf Seite 74)
- **Mittlerweile ist es notwendig, mit Sicherheitsvorfällen proaktiv umzugehen, statt sie nur abzuwehren.**
  (vgl. Abschnitt 6.1, auf Seite 119)

Anhang

A.1 Prototypisches Prozessmodell einer HSA-Implementierung

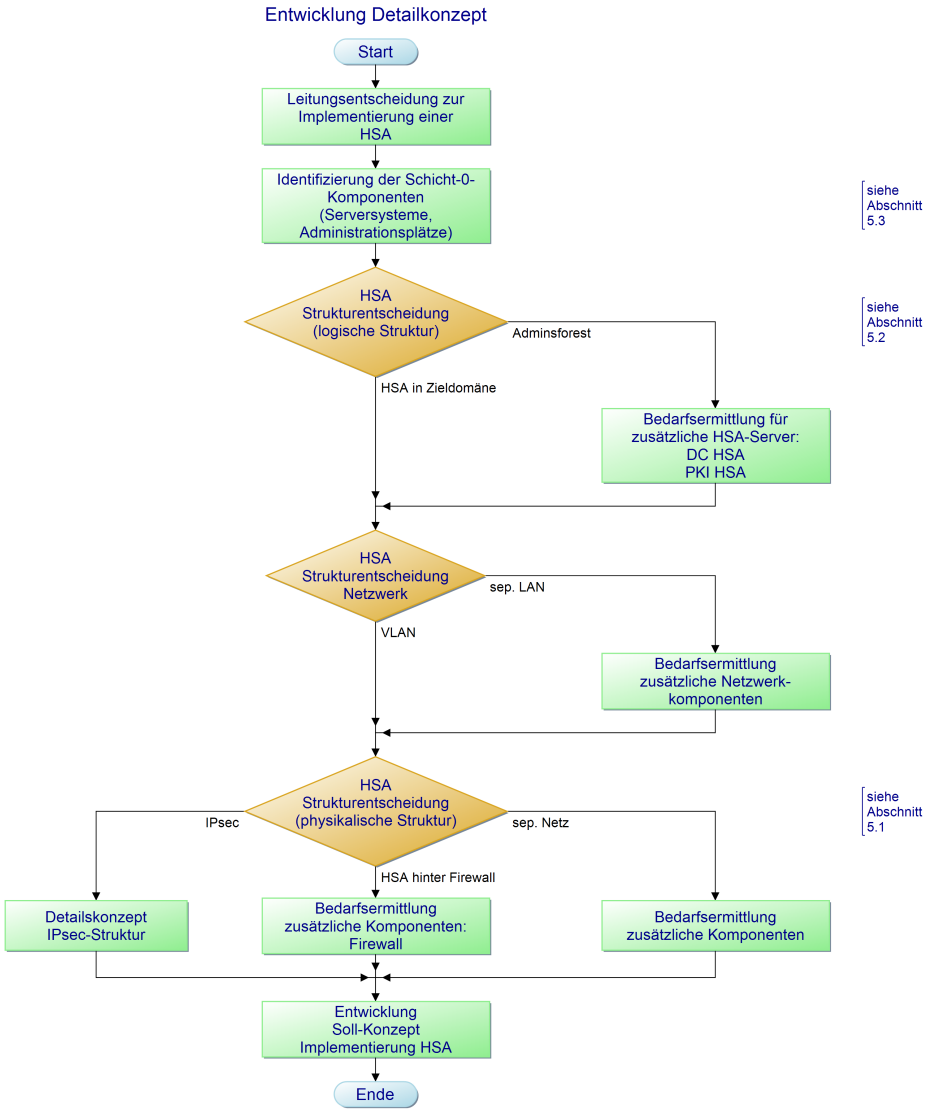
Die folgenden Abbildungen zeigen in Form von symbolischen Programmablaufpläne (PAP)[1] eine prototypische Implementierung einer hochsichere Administrationsumgebung (HSA).



Quelle: Eigene Darstellung

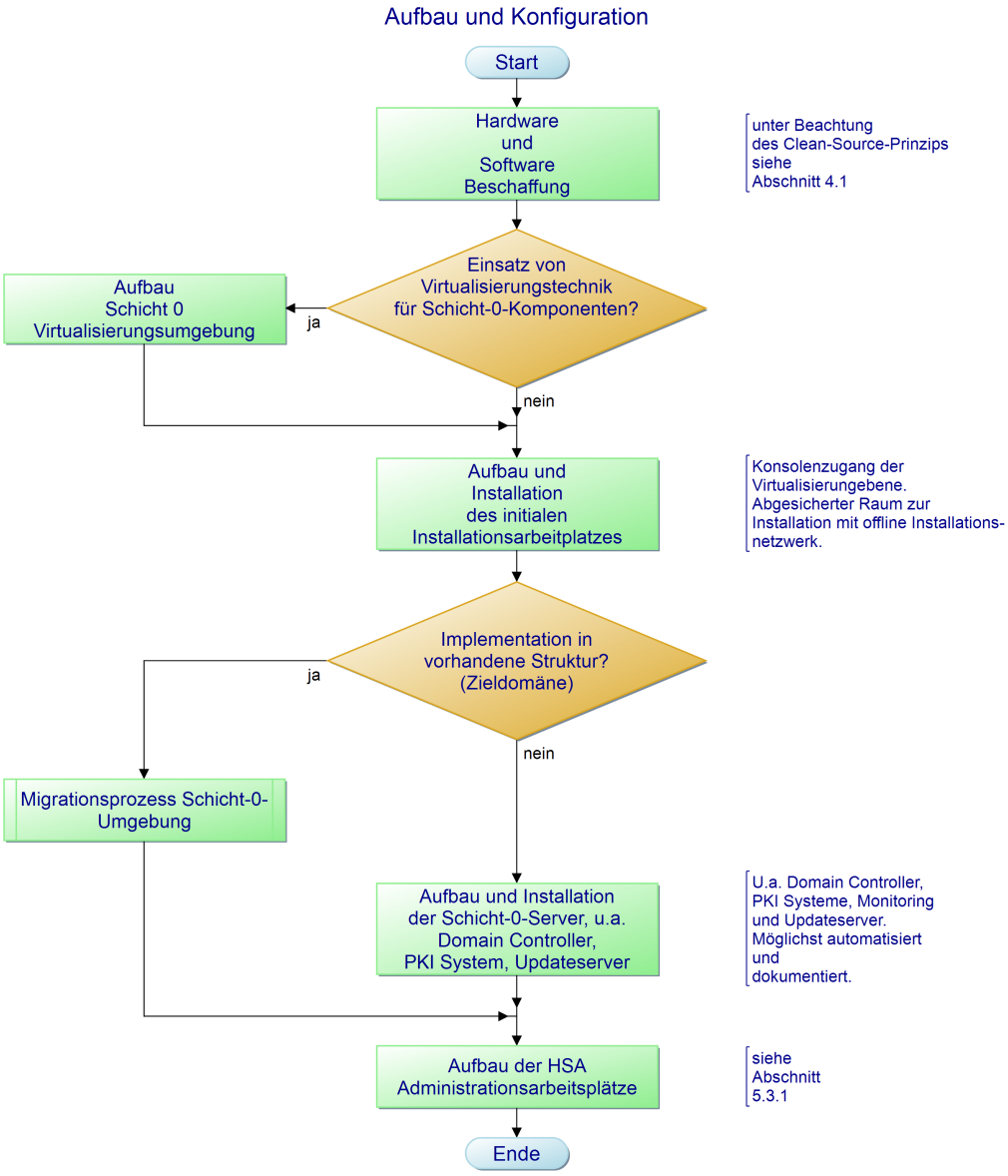
Abbildung A.1: Prozess der Implementierung und des Betriebs einer HSA

[1] Zur Erstellung wurde das Programm PapDesigner benutzt, welches im Rahmen nicht kommerzieller Zwecke auch für Abschlussprüfungen, Studienarbeiten, gemeinnützige Vereine und öffentlich geförderte Projekte und Maßnahmen lizenzkostenfrei nutzbar ist.
Quelle: `http://friedrich-folkmann.de/papdesigner/Lizenzabkommen.html`



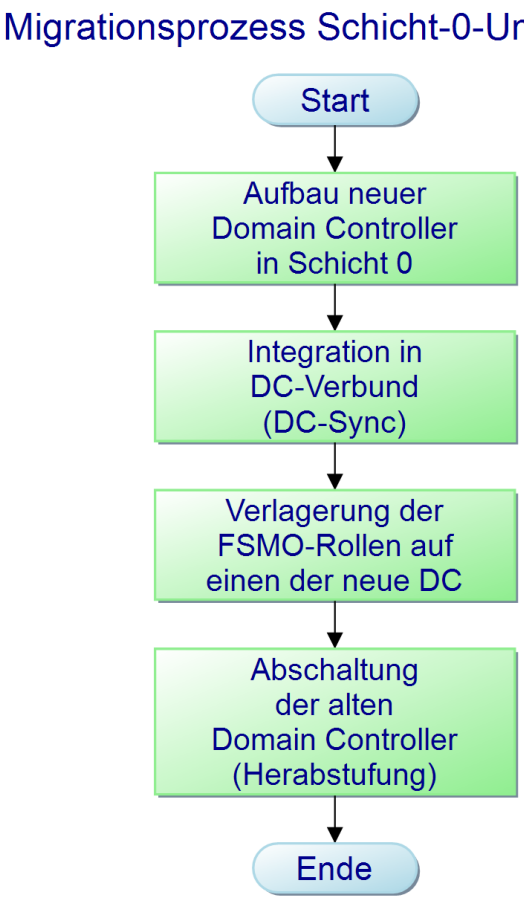
Quelle: Eigene Darstellung

Abbildung A.2: Sub-Prozess der Entwicklung eines Detailkonzeptes



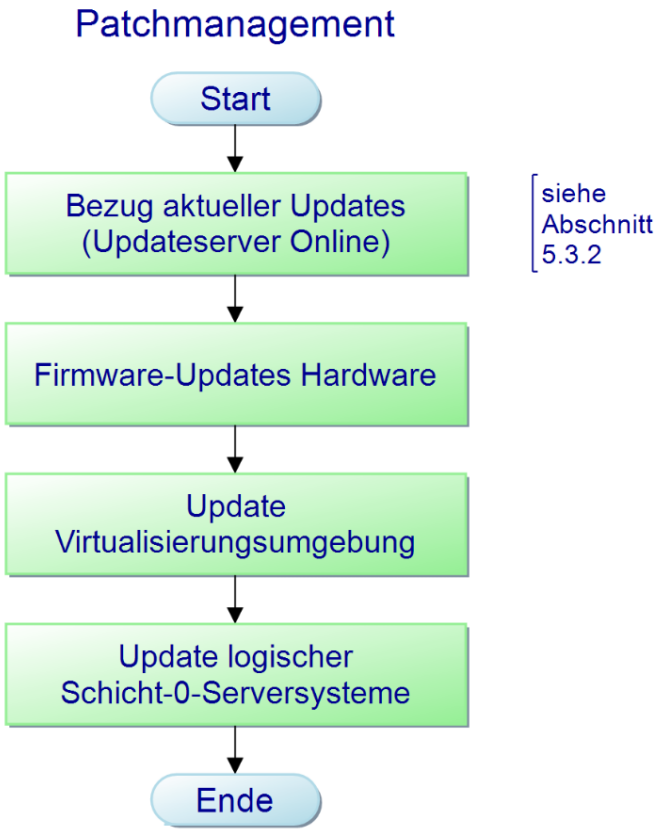
Quelle: Eigene Darstellung

Abbildung A.3: Sub-Prozess des Aufbaus einer Schicht 0 und HSA



Quelle: Eigene Darstellung

Abbildung A.4: Sub-Prozess der Verlagerung eines bereits vorhandenen AVD-Systems



Quelle: Eigene Darstellung

Abbildung A.5: Sub-Prozess des Update- und Patchmanagements