Bedrohungsanalyse für militärische Informationstechnik

Dissertation zur Erlangung des akademischen Grades
doctor rerum naturalium
(Dr. rer. nat.)

in der Wissenschaftsdisziplin
Internet Technologien und Systeme
eingereicht an der
Digital-Engineering-Fakultät
der Universität Potsdam von

Michael Meinig
meinig@uni-potsdam.de

Hasso-Plattner-Institut für IT Systems Engineering
Fachgebiet Internet Technologien und Systeme
August-Bebel-Str. 88
14482 Potsdam, Germany

Ort und Tag der Disputation: Potsdam, 05.12.2019
Hauptbetreuer:
Prof. Dr. Christoph Meinel

weitere Gutachter:
PD Dr. Dr. Torsten Albrecht
Prof. Dr. Ulrike Lechner

Soweit nicht anders gekennzeichnet ist dieses Werk unter einem Creative Commons Lizenzvertrag lizenziert:
Namensnennung 4.0 International. Dies gilt nicht für zitierte Inhalte anderer Autoren.
Um die Bedingungen der Lizenz einzusehen, folgen Sie bitte dem Hyperlink:
https://creativecommons.org/licenses/by/4.0/deed.de

Online veröffentlicht auf dem
Publikationsserver der Universität Potsdam:
https://doi.org/10.25932/publishup-44160
https://nbn-resolving.org/urn:nbn:de:kobv:517-opus4-441608

Zusammenfassung

Risiken für Cyberressourcen können durch unbeabsichtigte oder absichtliche Bedrohungen entstehen. Dazu gehören Insider-Bedrohungen von unzufriedenen oder nachlässigen Mitarbeitern und Partnern, eskalierende und aufkommende Bedrohungen aus aller Welt, die stetige Weiterentwicklung der Angriffstechnologien und die Entstehung neuer und zerstörerischer Angriffe. Informationstechnik spielt mittlerweile in allen Bereichen des Lebens eine entscheidende Rolle, u. a. auch im Bereich des Militärs. Ein ineffektiver Schutz von Cyberressourcen kann hier Sicherheitsvorfälle und Cyberattacken erleichtern, welche die kritischen Vorgänge stören, zu unangemessenem Zugriff, Offenlegung, Änderung oder Zerstörung sensibler Informationen führen und somit die nationale Sicherheit, das wirtschaftliche Wohlergehen sowie die öffentliche Gesundheit und Sicherheit gefährden. Oftmals ist allerdings nicht klar, welche Bedrohungen konkret vorhanden sind und welche der kritischen Systemressourcen besonders gefährdet ist.

In dieser Dissertation werden verschiedene Analyseverfahren für Bedrohungen in militärischer Informationstechnik vorgeschlagen und in realen Umgebungen getestet. Dies bezieht sich auf Infrastrukturen, IT-Systeme, Netze und Anwendungen, welche Verschlusssachen (VS)/Staatsgeheimnisse verarbeiten, wie zum Beispiel bei militärischen oder Regierungsorganisationen. Die Besonderheit an diesen Organisationen ist das Konzept der Informationsräume, in denen verschiedene Datenelemente, wie z. B. Papierdokumente und Computerdateien, entsprechend ihrer Sicherheitsempfindlichkeit eingestuft werden, z. B. „STRENG GEHEIM“, „GEHEIM“, „VS-VERTRAULICH“, „VS-NUR-FÜR-DEN-DIENSTGEBRAUCH“ oder „OFFEN“.

Die Besonderheit dieser Arbeit ist der Zugang zu eingestuften Informationen aus verschiedenen Informationsräumen und der Prozess der Freigabe dieser. Jede in der Arbeit entstandene Veröffentlichung wurde mit Angehörigen in der Organisation besprochen, gegengelesen und freigegeben, so dass keine eingestuften Informationen an die Öffentlichkeit gelangen.

Die Dissertation beschreibt zunächst Bedrohungsklassifikationsschemen und Angreiferstrategien, um daraus ein ganzheitliches, strategiebasiertes Bedrohungsmodell für Organisationen abzuleiten. Im weiteren Verlauf wird die Erstellung und Analyse eines Sicherheitsdatenflussdiagramms definiert, welches genutzt wird, um in eingestuften Informationsräumen operationelle Netzknoten zu identifizieren, die aufgrund der Bedrohungen besonders gefährdet sind. Die spezielle, neuartige Darstellung ermöglicht es, erlaubte und verbotene Informationsflüsse innerhalb und zwischen diesen Informationsräumen zu verstehen.

Aufbauend auf der Bedrohungsanalyse werden im weiteren Verlauf die Nachrichtenflüsse der operationellen Netzknoten auf Verstöße gegen Sicherheitsrichtlinien analysiert und die Ergebnisse mit Hilfe des Sicherheitsdatenflussdiagramms anonymisiert dargestellt. Durch Anonymisierung der Sicherheitsdatenflussdiagramme ist ein Austausch mit externen Experten zur Diskussion von Sicherheitsproblematiken möglich.

Der dritte Teil der Arbeit zeigt, wie umfangreiche Protokolldaten der Nachrichtenflüsse dahingehend untersucht werden können, ob eine Reduzierung der Menge an Daten möglich ist. Dazu wird die Theorie der groben Mengen aus der Unsicherheitstheorie genutzt. Dieser Ansatz wird in einer Fallstudie, auch unter Berücksichtigung von möglichen auftretenden Anomalien getestet und ermittelt, welche Attribute in Protokolldaten am ehesten redundant sind.

Abstract

Risks to cyber resources can arise from unintentional or deliberate threats. These include insider threats from dissatisfied or negligent employees and partners, escalating and emerging threats from around the world, the evolving nature of attack technologies, and the emergence of new and destructive attacks. Information technology now plays a decisive role in all areas of life, including the military. Ineffective protection of cyber resources can facilitate security incidents and cyberattacks that disrupt critical operations, lead to inappropriate access, disclosure, alteration or destruction of sensitive information, and endanger national security, economic welfare and public health and safety. However, it is often unclear which threats are present and which of the critical system resources are particularly at risk.

In this dissertation different analysis methods for threats in military information technology are proposed and tested in real environments. This refers to infrastructures, IT systems, networks and applications that process classified information/state secrets, such as in military or governmental organizations. The special characteristic of these organizations is the concept of classification zones in which different data elements, such as paper documents and computer files, are classified according to their security sensitivity, e.g. „TOP SECRET“, „SECRET“, „CONFIDENTIAL“, „RESTRICTED“ or „UNCLASSIFIED“.

The peculiarity of this work is the access to classified information from different classification zones and the process of releasing it. Each publication created during the work was discussed, proofread and approved by members of the organization, so that no classified information is released to the public.

The dissertation first describes threat classification schemes and attacker strategies in order to derive a holistic, strategy-based threat model for organizations. In the further course, the creation and analysis of a security data flow diagram is defined, which is used to identify operational network nodes in classification zones, which are particularly endangered due to the threats. The special, novel representation makes it possible to understand permitted and prohibited information flows within and between these classification zones.

Based on the threat analysis, the message flows of the operational network nodes are analyzed for violations of security policies and the results are presented anonymously using the security data flow diagram. By anonymizing the security data flow diagrams, it is possible to exchange information with external experts to discuss security problems.

The third part of the dissertation shows how extensive log data of message flows can be examined to determine whether a reduction in the amount of data is possible. The rough set theory from the uncertainty theory is used for this purpose. This approach is tested in a case study, also taking into account possible anomalies, and determines which attributes are most likely to be redundant in the protocol data.

Danksagung

Die Erlangung eines akademischen Grades und das Schreiben einer Dissertation ist wie ein Marathonlauf. Es gibt Höhen, wie die erfolgreiche Akzeptanz bei der Einreichung von Veröffentlichungen, und Tiefen, wie die Ablehnungen der selbigen mit teilweise zweifelhaften Kommentaren, die einen an sich selbst zweifeln lassen. In diesen Situationen ist es gut, Menschen an der Seite zu haben, die einen darin bestärken, die Berge und Täler zu bewältigen und den langen und beschwerlichen Weg weiter zu verfolgen. Der Lauf zur Promotion ist ein langes und ermüdendes Rennen, aber am Ende führt es auf der Zielgeraden zur Verteidigung und Veröffentlichung der Dissertation.

Ich möchte hiermit all denjenigen danken, die mich auf diesem Weg unterstützt haben und es mir ermöglicht haben, meine Ziele zu erreichen.

Vielen Dank!

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Motivation, Überblick und Beiträge der Arbeit

1.1. Motivation

Die Informations- und Kommunikationstechnologien (IKT) sind aus dem privaten Leben und aus dem Berufsleben vieler Menschen nicht mehr wegzudenken. Private, geschäftliche und öffentliche Bereiche werden immer stärker miteinander verbunden. Daraus entstehen gesellschaftliche und wirtschaftliche Chancen und aber auch Risiken. Die ständig zunehmenden Cyberangriffe können auf jedes von Software abhängige System abzielen. Unternehmen wissen deshalb um die Notwendigkeit des Schutzes vertraulicher, geheimer - klassifizierter - Informationen. Wettbewerber und Gegner wenden sich illegalen Methoden zu, um an vertrauliche Informationen zu gelangen. Sie versuchen, sich einen Wettbewerbsvorteil zu verschaffen oder eine technologische Lücke zu schließen sowie Abhängigkeiten von anderen zu verringern.

In militärischen Organisationen ist der Cyber- und Informationsraum nach Land, Meer, Luft und Raumfahrt die fünfte Dimension der Operationsführung [26], [28]. In diesen Dimensionen werden klassifizierte Informationen, sogenannte Verschlusssachen, verarbeitet. Unter Verschlusssachen versteht man Tatsachen, Sachverhalte oder Kenntnisse, die geheim gehalten werden müssen, unabhängig von der Art und Weise, in der die Informationen dargestellt werden (siehe Kapitel 2).

Informationssicherheit ist somit eines der entscheidenden Themen für die moderne Industrie und militärische Organisationen sowie Regierungsorganisationen. Schädliche Angriffe auf Industrieunternehmen und Regierungsorganisationen können jährlich hohe Schäden [124] verursachen. Illegaler Wissenstransfer und wirtschaftliche Sabotage sind kein seltenes Einzelereignis mehr, sondern ein Massenphänomen [36], [54], [135], [154].

Unternehmen geben Geld für Sicherheitslösungen aus, um ihre vertraulichen Informationen zu schützen. Sie setzen Richtlinien um, die sich aus Vorschriften und Gesetzen ableiten, um den Verlust der Vertraulichkeit, Verfügbarkeit und Integrität ihrer Informationen zu verhindern. Aufgrund der betrieblichen Anforderungen können jedoch Ausnahmen von den Richtlinien erlaubt und genehmigt werden [46].

Ein Mitarbeiter, der beispielsweise oft auf Geschäftsreisen unterwegs ist, darf möglicherweise über seinen USB-Anschluss Präsentationen herunterladen und gleichzeitig Informationen, die er auf seinen Reisen gesammelt hat, mit seinem Laptop in das Firmennetzwerk hochladen. Die Autorisierung dieser Ausnahmen basiert oft nur auf den geschäftlichen Anforderungen des einzelnen Mitarbeiters. Dies wirft die Frage auf, wie eine Berechtigung für eine Ausnahme das Sicherheitsrisiko für eine Organisation beeinflusst.

Neue Kommunikationsformen wie Instant Messaging, Voice over IP oder Blogs und Speichermöglichkeiten, z. B. Cloud Computing, werden in Unternehmen neben den traditionellen Anwendungen und Diensten wie z. B. E-Mail, Telefon, USB-Stick oder Festplatte eingesetzt [64]. Angriffe wie z. B. Spear-Fishing und Social Engineering sind beliebte Angriffsmethoden, die sich bewusst in das Netzwerk [141] einschleusen. Selbst die klügsten IT-Profis sind sich manchmal nicht des Unterschieds zwischen einem echten und einem gefälschten Event bewusst [93]. Wie können diese neuen Bedingungen in einem frühen Stadium des Entwicklungsprozesses berücksichtigt werden?

In den letzten Jahren haben viele Unternehmen aus allen Branchen Verletzungen der Datensicherheit bestätigt [38]. Diese Verletzungen, die durch Diebstahl oder „Verlust“ durch Innentäter und vertrauenswürdige Dritte verursacht werden, können vorsätzlich oder unbeabsichtigt sein [76]. Die Kosten, welche durch Verletzungen der Datensicherheit entstanden sind, belaufen sich für Unternehmen auf mehrere Millionen [111]. Die Modellierung dieser Bedrohungen ist kostengünstiger, wenn sie so früh wie möglich im Entwicklungsprozess eingesetzt wird. Die Kosten für Änderungen an solchen Modellen sind deutlich geringer als bei Änderungen an einem System in der Nutzung [139], [128].

1.2. Aufbau der Arbeit

Die vorliegende Dissertation widmet sich der Frage, wie eine Modellierung von solchen Bedrohungen durchgeführt werden kann. Darauf aufbauend werden Analyseverfahren entwickelt, welche Verletzungen der Datensicherheit identifizieren. Die Arbeit ist daher wie folgt gegliedert: In diesem Kapitel werden nach der bereits erfolgten kurzen Beschreibung der Motivation und der Darstellung der Struktur der Arbeit die wissenschaftlichen Beiträge skizziert.

Im folgenden Kapitel 2 wird in das zu untersuchende Problem eingeführt und die Hypothese für den Lösungsansatz aufgestellt. Im Kapitel 3 werden verwandte Arbeiten aus dem Bereich der Bedrohungsklassifikationsschemen und Angreiferstrategien präsentiert. Daraus abgeleitet wird im Kapitel 4 ein neues, ganzheitliches, strategiebasiertes Bedrohungsmodell für Organisationen entwickelt, welches jene Forschungsfragen aufwirft, die in den Folgekapiteln untersucht und für die Lösungen erarbeitet werden.

Im Kapitel 5 wird ein Datenflussdiagramm mit einem speziellen Sicherheitsfokus definiert. Dieses Sicherheitsdatenflussdiagramm wird verwendet, um eine Analyse durchzuführen, die in der Designphase jene operationelle Netzknotenstrukturen identifiziert, welche am stärksten von der Gefahr des Verlustes der Vertraulichkeit, Verfügbarkeit und Integrität ihrer klassifizierten Informationen beim Datenaustausch zwischen Netzwerken mit unterschiedlichen Geheimhaltungsgraden betroffen sind.

Im Kapitel 6 wird ein Ansatz vorgestellt, der Verstöße gegen Informationsräume durch eine automatisierte Nachrichtenflussanalyse findet. Dieser Ansatz berücksichtigt das Problem der Anonymisierung der Quellereignisprotokolle, wodurch das resultierende Datenflussmodell mit Experten und der Öffentlichkeit gemeinsam genutzt werden kann. Es werden hier die praktischen Auswirkungen der Anwendung des Ansatzes auf einen großen Datensatz einer Regierungsorganisation und wie die Anonymität des Konzepts

formal validiert werden kann diskutiert. Die Analyse aus Kapitel 5 wird für operationelle Netzknotenstrukturen in der Nutzungsphase weiter entwickelt.

Im Kapitel 7 wird eine neue Idee zur Reduzierung von Protokolldaten vorgestellt, welche als „Grobe Protokolle“ bezeichnet werden. Dabei wird die Theorie der groben Mengen (rough sets) nach Pawlak [106] zur Reduzierung der Anzahl der Attribute verwendet, die in Protokolldaten zur Darstellung von Ereignissen im System gesammelt werden. Der Ansatz wurde in einer großen Fallstudie getestet. Die Experimente zeigten, dass die von diesem Ansatz vorgeschlagenen Möglichkeiten zur Datenreduktion auch dann gültig bleiben, wenn die Protokollinformationen aufgrund von Anomalien im System geändert werden.

Die Dissertation schließt im Kapitel 8 mit einer Zusammenfassung der wesentlichen Punkte und gibt einen Ausblick über die Fortsetzung der hier dargestellten Arbeiten.

1.3. Beiträge der Arbeit

1.3.1. Beitrag 1 - Bedrohungsmodell

Durch die Arbeit wird eine neue Methode zur Kategorisierung von Bedrohungen in Unternehmen/Organisationen vorgeschlagen. Es wird das Problem der fehlenden Darstellung der Beziehung zwischen Organisationen und ihren einzelnen Bestandteilen und der Bedrohungen durch Angriffe analysiert. Das entwickelte Modell ist ein neuer, strategiebasierter Ansatz, der insbesondere organisatorische Aspekte von Regierungsorganisationen und des Militärs mit einschließt. Das Modell berücksichtigt dabei das Konzept der Informationsräume (z. B. „GEHEIM“, „NUR-FÜR-DEN-DIENSTGEBRAUCH“). Dieser ganzheitliche Ansatz ist in den momentan etablierten Modellierungsmethoden noch nicht dargestellt. Es hilft Unternehmen und Organisationen, den Verlauf eines Angriffs für einzelne Teilbereiche der Organisation besser zu beschreiben. Dies ermöglicht ein besseres Verständnis der Ziele eines möglichen Angreifers und es ermöglicht letztendlich der Organisation, geeignete Sicherheitsmaßnahmen abzuleiten, um die Risiken zu reduzieren und die eigenen Informationen zu schützen. Der Mehrwert dieses Bedrohungsmodells wird in Kapitel 4 anhand eines praktischen Beispiels einer Militärorganisation nachgewiesen.

1.3.2. Beitrag 2 - DFDsec

Der zweite Beitrag dieser Arbeit ist ein Modell für Datenflüsse unter Berücksichtigung von Cybersicherheitsaspekten (*Sicherheitsdatenflussdiagramm - DFDsec*). Es wird zur Identifizierung von Datenflüssen zwischen verschiedenen Informationsräumen verwendet. Eine Analyse dieser Datenflüsse und der in Kapitel 1, 3 und 4 dargestellten Sicherheitsprobleme selbst führt zu dem Schluss, dass einige operationelle Netzknoten (z. B. Teile der Organisation), die mit diesen Datenflüssen verbunden sind, stärker durch den Verlust von Vertraulichkeit, Verfügbarkeit und Integrität gefährdet sind als andere. Durch die teilautomatisierte Erstellung von DFDsec-Modellen wird ermöglicht, diese operationelle Netzknoten für notwendige Sicherheitsmaßnahmen zu priorisieren. Die vorliegende Arbeit erweitert hier Konzepte bisherige Arbeiten mit dem Konzept der Informationsräu-

me. Diese entwickelte Methode ermöglicht insbesondere Aussagen über die Wahrscheinlichkeit, mit der illegale und unerwünschte Operationen auf gültigen Datenflusswegen durchgeführt wurden (siehe Kapitel 5).

1.3.3. Beitrag 3 - Identifizierung von Informationsraumverletzungen

Der dritte Beitrag innerhalb dieser Dissertation ist ein praktischer Ansatz zur Identifizierung von Verstößen gegen Informationsräume als Sicherheitsbedrohung. Der Nachweis der Tauglichkeit des Ansatzes wird auf der Grundlage von Protokollen vergangener Informationsflüsse in einer militärischen Organisation durchgeführt. Ziel dieses Ansatzes ist es, Schwachstellen und unbekannte Angriffsvektoren in der Infrastruktur zu finden. Eine einzigartige Eigenschaft dabei ist die Anonymisierung der Quelldaten. Dies ist eine gängige Erwartung in Organisationen mit obligatorischen Informationsräumen, ist aber im Allgemeinen das Gegenteil von frei zugänglicher Sicherheitsforschung. Die Anonymisierungsforderung verhindert in der Regel auch die Zusammenarbeit mit externen Beratern oder zwingt sie, starke, rechtliche Geheimhaltungsvereinbarungen (Legal Non Disclosure Agreement- NDA) abzuschließen. Mit diesem Beitrag der Arbeit werden beide Aspekte gleichzeitig angegangen (siehe Kapitel 6).

1.3.4. Beitrag 4 - Grobe Protokolle

Ein weiterer Beitrag dieser Arbeit ist eine neue Methode zur Reduzierung der Menge der Protokolldaten, welche für Online-Analysen und die Erkennung von Anomalien benötigt werden. Dabei wird ein Ansatz der Unsicherheitstheorie namens *Grobe Mengen (Rough Sets)* verwendet, der es ermöglicht, Protokolldaten dadurch zu verkleinern, indem grob redundante Attribute in Protokolldateieinträgen entfernt werden. Die entfernbaren Attribute werden durch eine einmalige Analyse vorhandener Protokolldaten detektiert, welche die logischen Beziehungen zwischen den im Systemprotokoll aufgezeichneten Systemattributen identifiziert. Das Ergebnis sind „Grobe Protokolle“, welche das Systemverhalten auf eine unscharfe, aber dennoch repräsentative Weise beschreiben. Dieser Reduktionsansatz wurde mit einem umfangreichen Datensatz aus der Praxis getestet und erwies sich als robust, auch wenn Sicherheitsanomalien die Art der Originaldaten verändern (siehe Kapitel 7).

1.3.5. Publikationen

Im Rahmen dieser Arbeit entstanden folgende Publikationen, welche Beiträge der Arbeit direkt erläutern:

- Meinig, M., Sukmana, M. I. H., Torkura, K. A., and Meinel, C. *Holistic Strategy-Based Threat Model for Organizations.* In Proceedings of the 10th International Conference on Ambient Systems, Networks and Technologies, ANT 2019, Leuven, Belgien, April 29 – Mai 02, April-Mai 2019, [96] (siehe Kapitel 3 und 4).
- Meinig, M. and Meinel, C. *Securing the Flow - Data Flow Analysis with Operational Node Structures.* In Proceedings of the 4th International Conference on Information

Systems Security and Privacy, ICISSP 2018, Funchal, Madeira - Portugal, Januar 22-24, Seiten 241–250, DOI: 10.5220/0006570302410250, Januar 2018, [95] (siehe Kapitel 5).

- Meinig, M., Tröger, P., and Meinel, C. *Finding Classification Zone Violations with Anonymized Message Flow Analysis*. In Proceedings of the 5th International Conference on Information Systems Security and Privacy, ICISSP 2019, Prag, Tschechien, Februar 23-25, Seiten 284-292, Februar 2019, [97] (siehe Kapitel 6).

- Meinig, M., Tröger, P., and Meinel, C. *Rough Logs - A Data Reduction Approach for Log Files*. In Proceedings of the 21st International Conference on Enterprise Information Systems (ICEIS 2019), Heraklion, Kreta - Griechenland, Mai 03-05, Mai 2019, [98] (siehe Kapitel 7).

- Torkura, K. A., Sukmana, M. I. H., Meinig, M., Cheng, F., Meinel, C., and Graupner, H. *A threat modeling approach for cloud storage brokerage and file sharing systems*. In NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, DOI: 10.1109/NOMS.2018.8406188, April 2018, [137].

- Torkura, K. A., Sukmana, M. I. H., Meinig, M., Kayem, A. V. D. M., Cheng, F., Graupner, H., and Meinel, C. *Securing Cloud Storage Brokerage Systems Through Threat Models*. In 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Seiten 759–768, DOI: 10.1109/AINA.2018.00114, Mai 2018, [138].

2. Problemdarstellung und Idee der Arbeit

Dieses Kapitel führt in die Problemstellung der Bedrohungsanalyse militärischer Informationstechnik ein und stellt daraus abgeleitet die Idee der Arbeit und die Forschungsfragen vor. Dabei werden zunächst Hintergründe zu Informationsräumen und den darin enthaltenen Verschlusssachen erläutert und grundsätzliche Begriffe in diesem Bereich definiert. Danach werden die Begriffe Vertraulichkeit und Integrität eingeführt und die Bedrohungen der Verschlusssachen durch den Verlust der Vertraulichkeit und Integrität dargestellt. Schließlich wird das Problem und die Idee der Arbeit präsentiert.

2.1. Hintergründe und Definitionen

2.1.1. Verschlusssachen/Staatsgeheimnisse

In militärischen oder Regierungsorganisationen werden in Anwendungen, Infrastruktur, IT-Systemen und Netzen Verschlusssachen und Staatsgeheimnisse verarbeitet. Verschlusssachen sind unabhängig von ihrer Darstellungsform im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse [27]. Dasselbe gilt in Regierungsorganisationen für Staatsgeheimnisse. Staatsgeheimnisse gemäß § 93 StGB sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheimgehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden [23, §93 StGB].

Von Verschlusssachen/Staatsgeheimnissen dürfen nur Personen Kenntnis erhalten, die aufgrund ihrer Dienstpflichten von ihr Kenntnis haben müssen. Keine Person darf darüber umfassender oder eher unterrichtet werden, als dies aus dienstlichen Gründen unerlässlich ist. Es gilt der Grundsatz „Kenntnis nur, wenn nötig“ [27]. Der Grundsatz „Kenntnis nur, wenn nötig“ beschreibt, wenn er von Regierungen und anderen Organisationen, die zum Beispiel mit dem Militär in Beziehung stehen, verwendet wird, die Einschränkung von Daten, welche als sehr sensibel angesehen werden. Selbst wenn man über alle notwendigen behördlichen Genehmigungen, wie eine Sicherheitsüberprüfung, verfügt, um auf bestimmte Informationen zuzugreifen, wird man nicht auf solche Informationen zugreifen oder sich in einen geheimen Vorgang einlesen dürfen, es sei denn, es gibt eine spezifische Notwendigkeit es zu wissen. Wie bei den meisten Sicherheitsmechanismen besteht das Ziel darin, den Zugriff durch Unbefugte zu erschweren, ohne den rechtmäßigen Zugriff zu beeinträchtigen. „Kenntnis nur, wenn nötig“ zielt auch darauf ab, das Durchstöbern von sensitivem Material zu verhindern, indem der Zugriff auf die kleinstmögliche Anzahl von Personen eingeschränkt wird.

Verschlusssachen sind gemäß Sicherheitsüberprüfungsgesetz (SÜG) [21] je nach dem Schutz, dessen sie bedürfen, in folgende Geheimhaltungsgrade einzustufen:

1. STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann,

2. GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann,

3. VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann,

4. VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD), wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.

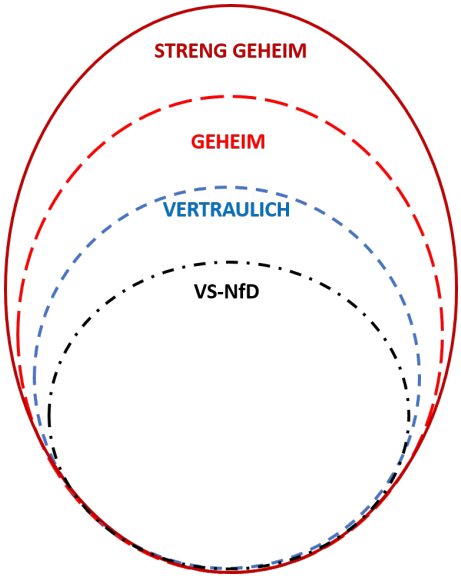

Abbildung 2.1.: Zusammenhang bei der Berücksichtigung der Geheimhaltungsgrade

Abbildung 2.1 zeigt den Zusammenhang zwischen den Geheimhaltungsgraden. Sie schließen sich gegenseitig ein, d.h. jede vertrauliche Information kann wie eine geheime Information behandelt werden, aber nicht umgekehrt. Der Bedrohung der Verschlusssachen durch Verlust der Vertraulichkeit, Verfügbarkeit und Integrität ist dabei mit technischen Schutzmaßnahmen entgegenzuwirken [27].

Die verschiedenen Geheimhaltungsgrade können einem Regierungsdokument, einer Datei oder einem Datensatz basierend auf der Sensibilität oder Geheimhaltung der Information zugewiesen werden [27]. Der Umgang mit solchen Informationen ist eine

sicherheitsrelevante Tätigkeit auch bezeichnet als eine „sicherheitsempfindliche“ Tätigkeit [21]. Diese wird durch Personen ausgeübt, welche Zugang zu Verschlusssachen haben oder ihn sich verschaffen können. Dazu müssen sie sich vorher einer Sicherheitsüberprüfung unterziehen [21].

Deutschland hat sich in gegenseitigen Geheimschutzabkommen verpflichtet, die Informationen internationaler Partner, wie zum Beispiel internationale Organisationen beispielsweise die North Atlantic Treaty Organisation (NATO) oder die Europäische Union (EU), aber auch einzelne Staaten, nach deren Vorgaben zu schützen, wenn sie in nationaler deutscher IT verarbeitet und/oder übertragen werden [25, S. 13]. Folgende ähnliche Geheimhaltungsgrade sind bei diesen Organisationen definiert [25, S. 15]:

NATO

- COSMIC TOP SECRET
- NATO SECRET
- NATO CONFIDENTIAL
- NATO RESTRICTED

EU

- TRES SECRET UE/EU TOP SECRET
- SECRET UE
- CONFIDENTIEL UE
- RESTREINT UE

Um Dokumente mit einem bestimmten Geheimhaltungsgrad z. B. von Deutschland aus in die NATO oder in die EU zu versenden, muss der Term „RELEASABLE TO NATO“, beziehungsweise „EU“ hinzugefügt werden, zum Beispiel DEU RESTRICTED RELEASABLE TO NATO [27]. Dies nennt man auch *formale Kategorie* und dient der Unterscheidung internationaler Geheimhaltungsgrade. Sobald Informationen in dieser Art klassifiziert werden, müssen die bereits erwähnten internationalen Geheimschutzabkommen zur Verarbeitung der Informationen eingehalten werden [25, S. 13].

Neben den Staatsgeheimnissen/Verschlusssachen gibt es offene und öffentliche Informationen. Offene Informationen sind nicht eingestufte Informationen, die nicht aus Gründen des Geheimschutzes oder des Datenschutzes der Pflicht zur Verschwiegenheit unterliegen (z. B. aus Gründen der Verschwiegenheit in vertragsrechtlichen Angelegenheiten). Sie sind hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität zu schützen [25, S. 16].

Informationen, die für die Öffentlichkeit bestimmt sind oder aus öffentlichen Quellen entnommen wurden, sind öffentliche Informationen. Sie unterliegen nicht der Amtsverschwiegenheit und hinsichtlich der Vertraulichkeit keinen IT-Sicherheitsanforderungen. Aus Gründen des Ansehens in der Öffentlichkeit oder aus rechtlichen Gründen können

diese Informationen jedoch Anforderungen an die Verfügbarkeit und/oder Integrität haben [25, S. 16].

2.1.2. Informationsräume

Durch die Bereitstellung von Informationen (über Schnittstellen) aufgrund der Geheimschutzabkommen mit anderen Nationen sowie der NATO und der EU entsteht ein *virtueller, IT-gestützter Informationsraum*. Dieser umfasst Geheimhaltungsgrade und Inhalte, wie beispielsweise Papierdokumente oder Computerdateien, denen ein Geheimhaltungsgrad zugewiesen wurde. Um diesen Informationsraum nutzen zu können, sind ein Informationsmanagement mit der Möglichkeit zur Filterung, Maßnahmen zur Zugriffskontrolle und einer bedarfsgerechten Informationsdarstellung notwendig [25, S. 215]. Durch die Zuweisung verschiedener Geheimhaltungsgrade entstehen *unterschiedliche Informationsräume*. Damit Informationen zwischen verschiedenen Informationsräumen ausgetauscht werden können, ist der Informationsfluss durch Sicherheitsgateways technisch zu steuern [25, S. 118].

Es ist üblich, in diesem Zusammenhang von roten und schwarzen Netzen zu sprechen. Von *roten Netzen* spricht man, wenn Verschlusssachen/Staatsgeheimnisse in Informationsräumen verarbeitet werden, die einen Geheimhaltungsgrad höher als „VS-NfD“ haben. In *schwarzen Netzen* werden Informationen verarbeitet, welche einen Geheimhaltungsgrad kleiner oder gleich „VS-NfD“ haben.

In einem militärischen oder behördlichen Umfeld können nun also Personen, Dokumente und Informationen zwei Arten von formalen Sicherheitsbezeichnungen erhalten: Zum einen die Klassifizierung oder Freigabe (z .B. „OFFEN“, „VS-NfD“, „VERTRAULICH“, „GEHEIM“ und „STRENG GEHEIM“) und zum anderen eine formale Kategorie (wie z. B. „NATO“, „EU“, und „DEU“). Die Kombination dieser beiden Sicherheitsbezeichnungen ist, wie bereits im Abschnitt 2.1.1 dargestellt, der „Geheimhaltungsgrad“. Um Geheimhaltungsgrade in der Modellierung besser nutzen zu können, werden indexbasierte Einstufungen verwendet. Dies ist ein übliches Verfahren in der Sicherheitsforschung, wie beispielsweise bei der Strukturfunktionsanalyse [42], der Risiko-Analyse (Hazard-Analysis) [77], der Software-Sicherheits-Risiko-Analyse (Software Safety Hazard Analysis) [86] oder dem integrierten System- und Sicherheitstechnik-Prozess (Integrated System and Safety Engineering Process) [87].

Der Geheimhaltungsgrad wird definiert als „I(c)“, wobei I die formale Kategorie und (c) die Klassifizierung oder Freigabe ist. Für Deutschland wäre ein Beispiel „I(c) = DEU (GEHEIM)“. Anstelle der Verwendung spezifischer Klassifizierungen werden für c, $c \in Z$, steigende numerische Zahlen verwendet, wie z. B.:

- Öffentlich = -1
- OFFEN = 0
- VS-NUR-FÜR-DEN-DIENSTGEBRAUCH = 1
- VS-VERTRAULICH = 2

- GEHEIM = 3
- STRENG GEHEIM = 4

Im Rahmen der NATO oder der EU wären durch die indexbasierte Einstufungen nur die formalen Kategorien zu ändern, da die Klassifizierungen sinngemäß genutzt werden können.

2.2. Vertraulichkeit und Integrität als Zielgrößen in IT-Systemen zur Verarbeitung von Verschlusssachen/Staatsgeheimnissen

Integrität und Vertraulichkeit sind neben der Verfügbarkeit klassische Grundwerte der Informationssicherheit [25]. Sie sind damit auch Zielgrößen in IT-Systemen zur Verarbeitung von Verschlusssachen/Staatsgeheimnissen. In diesem Abschnitt werden diese beiden Grundwerte einer genaueren Betrachtung unterzogen. Dabei wird untersucht, welche Wortbedeutung sie haben, welche rechtlichen Grundlagen es gibt und wie sie in unterschiedlichen wissenschaftlichen Gebieten verwendet werden. Ein genauerer Untersuchungsaspekt sind die Bedeutungen der Begriffe aus informationstechnischer Sicht. Ziel soll es sein, bestimmte Eigenschaften zu identifizieren, die eine Bewertung dahingehend zulassen, ob ein IT-System diese Grundwerte erfüllt oder nicht.

2.2.1. Vertraulichkeit

Wortbedeutung

Vertraulichkeit (confidentiality) ist die Eigenschaft, diskret (vertraulich) zu sein. Diese Eigenschaft kann man zusichern. Eine weitere Wortbedeutung ist allzu aufdringliches, nicht genügend distanziertes Verhalten. Dabei geht es um die Zudringlichkeit, in dem man sich Vertraulichkeiten erlaubt. Synonyme Wörter sind Diskretion, Geheimhaltung, Heimlichkeit, [Still]schweigen, Verschwiegenheit; (bildungssprachlich) Intimität; (bildungssprachlich veraltend) Konfidenz [8]. In der englischen Wortbedeutung beschreibt es den Zustand der Geheimhaltung: „The state of keeping or being kept secret or private“ [103].

Betrachtung aus rechtlicher Sicht und aus Sicht anderer Fachgebiete

Der Schutz der Vertraulichkeit ist Bestandteil vieler rechtlicher Grundlagen. In Deutschland ist die Verletzung der Vertraulichkeit des Wortes ein Vergehen, welches mit einer Freiheitsstrafe von bis zu drei Jahren bestraft werden kann. Hierbei geht es um die Aufnahme des nicht-öffentlich gesprochenen Wortes, welche zum Beispiel einem Dritten zugänglich gemacht wird. Ebenfalls strafbar ist das Abhören nicht öffentlich gesprochener Worte, die dann zum Beispiel der Öffentlichkeit mitgeteilt werden. Der Versuch dieser

Taten ist schon strafbar. Bei Amtsträgern, die einer besonderen Verpflichtung zur Wahrung der Vertraulichkeit unterliegen, kann die Freiheitsstrafe höher ausfallen, nämlich bis zu fünf Jahren [23, §201 StGB].

Grundrechtlich geschützt ist die Vertraulichkeit des Brief- sowie des Post- und Fernmeldegeheimnisses [22, §10 GG]. Die Verletzung des Briefgeheimnisses ist ein Straftatbestand, welches mit einer Freiheitsstrafe von bis zu einem Jahr bestraft wird. Dabei geht es um die Öffnung verschlossener Briefe oder Schriftstücke, die nicht zur unbefugten Kenntnis bestimmt sind. Das Fernmeldegeheimnis in [24] ist zusammen mit dem Postgeheimnis durch [23] geschützt. Dabei geht es um den Schutz des Inhalts der Kommunikation und deren Verbindungsdaten.

Für bestimmte Berufsgruppen ist die Vertraulichkeit der Kommunikation besonders geschützt. Ein Beispiel ist das Beichtgeheimnis, wobei es um Inhalte geht, welche der Beichtvater während der Beichte erfahren hat. Er kann nur vom Beichtenden selbst von der Schweigepflicht entbunden werden. Die Verletzung des Beichtgeheimnisses kann mit der Exkommunikation aus der Kirche bestraft werden [134]. In der Strafprozessordnung sind Berufsgeheimnisträger zur Verweigerung des Zeugnisses berechtigt. Weitere Berufsgeheimnisträger, beispielsweise Anwälte, Ärzte, Versicherungsangestellte oder Berufspsychologen sind verpflichtet, ihnen anvertraute Geheimnisse nicht zu offenbaren. Bei diesen Personen handelt es sich um Privatpersonen. Ebenso werden Amtsträger, also Angehörige des Staates, zur Verschwiegenheit verpflichtet [23, §203 StGB].

Neben der Vertraulichkeit der Kommunikation für verschiedene Berufsgruppen betrachten die Wirtschaftswissenschaften die Vertraulichkeit der persönlichen Informationen eines Kreditnehmers. Diese werden vom Kreditinstitut vertraulich behandelt. Eine Weitergabe von Informationen über das finanzielle Engagement an Dritte ist nur im rechtlich vorgegeben Rahmen von Datenschutz und Bankgeheimnis oder mit Zustimmung des Kunden möglich [57].

Wird die Vertraulichkeit durch Offenbarung von Tatsachen verletzt, die nicht für die Öffentlichkeit, nicht allgemein zugänglich und nicht für Dritte bestimmt sind, dann spricht man von Geheimnisverrat [23, §203 StGB], [23, §353 StGB]. Wenn es sich dabei um Staatsgeheimnisse [23, §93 StGB] handelt, dann ist dies Landesverrat [23, §94 StGB]. Der Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen, sogenannter Geschäftsgeheimnisse, vor rechtwidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung wird durch die Richtlinie 2016/943 des europäischen Parlaments und des Rates [50] geschützt.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wird vom allgemeinen Persönlichkeitsrecht umfasst. Dieses Recht ist kein eigenes Grundrecht, sondern eine Ableitung aus dem Persönlichkeitsrecht [22, §2 GG] und dient dem Schutz der persönlichen Daten, welche in informationstechnischen Systemen verarbeitet oder gespeichert werden. Eine Verletzung der Vertraulichkeit und Integrität ist demnach verfassungsrechtlich nur zulässig, wenn eine konkrete Gefahr besteht oder in näherer Zukunft eintritt [29].

Betrachtung aus informationstechnischer Sicht

So wie es verschiedene rechtliche und andere fachgebietstechnische Verwendungen des Wortes Vertraulichkeit gibt, sind auch verschiedene Blickwinkel in der Informationstechnik vorhanden. Der internationale Standard für Definitionen im Bereich der Informationssicherheit ist die ISO-Norm 27001. Gemäß dieser ist die Vertraulichkeit eine Eigenschaft, die für Informationen zutrifft. Die Vertraulichkeit von Informationen zu schützen und zu bewahren bedeutet, dass sie unbefugten Entitäten (Personen oder Prozessen) nicht zugänglich gemacht oder offengelegt werden [78]. Der deutsche Standard sind die IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik. In diesem wird die Vertraulichkeit als der Schutz vor unbefugter Preisgabe von Informationen definiert. Dabei dürfen vertrauliche Daten und Informationen ausschließlich Befugten in der zulässigen Weise zugänglich sein [16, S. 109]. Die Bundeswehr definiert die Vertraulichkeit als den Schutz vor unbefugter Informationsgewinnung/-beschaffung [25, S. 11]. Diese Standarddefinitionen werden in Vorlesungen in dieser oder leicht gewandelter, aber inhaltlich unveränderten Weise genutzt [55], [4], [146]. Neben dem Schutz vor unbefugter Preisgabe von Informationen wird die Vertraulichkeit auch als Verhinderung der unbefugten Weitergabe von Informationen „prevention of the unauthorised disclosure of information“ definiert [49]. In der Zuverlässigkeitsforschung ist Vertraulichkeit die Abwesenheit von unbefugter Offenlegung von Informationen: „Absence of unauthorized disclosure of information“. Hierbei ist Verlässlichkeit (dependability) ein integrierendes Konzept, dass sich über die letzten fünf Jahrzehnte entwickelt hat und die folgenden Attribute umfasst: Zuverlässigkeit (reliability), Verfügbarkeit (availability), Vertraulichkeit (confidentiality), Sicherheit (safety), Integrität (integrity) und Wartbarkeit (maintainability) [85]. Beispiele für formale Modelle, welche die Vertraulichkeit eines Computers beschreiben und umsetzen sind:

- Das Bell-La Padula Modell (Sichere Computersysteme: Einheitliche Exposition und Gebündelte Informations- und Rechendienst-Interpretation) [6],
- Das Brewer-Nash-Modell (Die Chinese Wall-Sicherheitsrichtlinie) [14].

Bedingungen und Eigenschaften von Vertraulichkeit

Zusammenfassend lassen sich aus den Wortbedeutungen von Vertraulichkeit, der Betrachtung von Vertraulichkeit aus rechtlicher Sicht, aus anderen Fachgebieten und aus informationstechnischer Sicht bestimmte Eigenschaften und Bedingungen identifizieren, die es möglich machen, festzustellen, ob bei einer Organisation der Aspekt der Vertraulichkeit betroffen ist, wann die Vertraulichkeit verletzt wird und wann es Rechtfertigungsgründe gibt, welche eine Vertraulichkeitsverletzung zulassen. Folgende Eigenschaften müssen für die Vertraulichkeit erfüllt sein:

- Zugänglich für Befugte
- Nicht für die Öffentlichkeit, nicht für Dritte, nicht allgemein zugänglich
- Schützenswerte oder bewahrungswerte Informationen

Die Vertraulichkeit ist verletzt, wenn es sich um ein oder eine

- Unbefugte/r/s oder rechtswidrige/r/s Aufnahme, Abhören, Erwerb, Kenntnis, Mitteilung, Nutzung, Offenbarung, Offenlegung, Öffnung, Preisgabe oder Weitergabe von nicht-öffentlichen oder verschlossenen Informationen (Briefe, Schriftstücke, Worte), Tatsachen, Geheimnissen an unbefugte Entitäten (Personen oder Prozesse), die Öffentlichkeit oder Dritte handelt.

Die Vertraulichkeitsverletzung ist zulässig und die Weitergabe von Informationen ist erlaubt, wenn:

- eine gesetzliche Grundlage vorhanden ist oder
- eine Zustimmung des Inhabers der Information vorliegt.

2.2.2. Integrität

Wortbedeutung

Integrität kommt von dem lateinischen Wort integritas, welches „Unversehrtheit“, „Reinheit“ oder „Unbescholtenheit“ bedeutet. Daraus ergibt sich die erste Wortbedeutung, welche die Begriffe Makellosigkeit, Unbescholtenheit und Unbestechlichkeit umfassen. Eine weitere Wortbedeutung ist die Unverletzlichkeit. Diese wird üblicherweise in der Politik oder in der Rechtssprache gebraucht. Ein Beispiel ist die Unverletzlichkeit eines Staatsgebietes, wo die territoriale Integrität eines Staates anerkannt und garantiert wird. Synonyme sind, neben den schon genannten, Anständigkeit, Ehrlichkeit, Rechtschaffenheit, Redlichkeit, Vertrauenswürdigkeit und Zuverlässigkeit [8].

In der englischen Wortbedeutung werden, neben den beiden auch im deutschen gebrauchten Wortbedeutungen, noch weitere beschrieben. Diese ergänzen die Bedeutung der Unverletzlichkeit. Es ist zunächst die strukturelle Unversehrtheit, zum Beispiel die eines Romans: „The condition of being unified or sound in construction.“ Im Weiteren beschreibt es die Prüfung der Integrität auf interne Konsistenz oder fehlende Korruption bei elektronischen Daten: „Internal consistency or lack of corruption in electronic data“ [103].

Betrachtung aus rechtlicher Sicht und aus Sicht anderer Fachgebiete

In den Wirtschaftswissenschaften ist Integrität das auf Erfahrungen und Erwartungen gestützte Ansehen bzw. Vertrauen, welches ein Akteur A bei anderen Akteuren B (C, D, usw.) hat, hinsichtlich der Berücksichtigung der (berechtigten) Interessen von B bzw. der Einhaltung von Verträgen sowie formellen und informellen Regeln. Der Aufbau von Integrität ist hierbei eng mit der Übernahme von Verantwortung verbunden [57].

Die körperliche Integrität bzw. Unversehrtheit des Menschen ist rechtlich durch das Grundgesetz geschützt [22, §22 GG]. Es schützt vor Eingriffen, welche die Gesundheit beeinträchtigen.

Der Schutz der Integrität ist neben der Körperintegrität Bestandteil einiger weiterer rechtlicher Grundlagen. In Deutschland ist die Verletzung der Integrität des berufssportlichen Wettbewerbs und des Wettbewerbs des organisierten Sports ein Vergehen, welches mit einer Freiheitsstrafe von bis zu drei Jahren bestraft werden kann. Hierbei geht es um die regelwidrige Beeinflussung des Wettbewerbs zum Vorteil für sich oder eines Dritten. Der berufssportliche Wettbewerb unterscheidet sich vom organisierten Sport darin, dass die teilnehmenden Sportler durch ihre sportliche Betätigung unmittelbar oder mittelbar Einnahmen von erheblichen Umfang erzielen [23, §265 StGB].

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wurde bereits im Abschnitt Vertraulichkeit behandelt, ist aber ebenfalls Teil der rechtlichen Grundlagen für Integrität.

Betrachtung aus informationstechnischer Sicht

So wie es verschiedene rechtliche und andere fachgebietstechnische Verwendungen des Wortes Integrität gibt, sind auch verschiedene Blickwinkel in der Informationstechnik vorhanden. Der internationale Standard für Definitionen im Bereich der Informationssicherheit ist wieder die ISO-Norm 27001. Gemäß dieser bedeutet Integrität Informationen zu wahren, die Genauigkeit und Vollständigkeit von Informationen und die Methoden, mit denen sie verarbeitet und verwaltet werden, zu schützen [78]. Gemäß der IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik wird die Integrität als Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen bezeichnet. Daten sollen dabei vollständig und unverändert sein. Wenn den Daten zusätzlich Attribute, wie z. B. Autor oder Zeitpunkt der Erstellung, zugeordnet werden, dann spricht man von Informationen (Daten mit Bedeutung [79]). Der Verlust der Integrität von Informationen kann bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden [16, S. 103]. Die Bundeswehr definiert Integrität als den Schutz vor unbefugter und unzulässiger Veränderungen von Information, IT-Diensten und Eigenschaften von IT sowie die Nachweisbarkeit und Beweisbarkeit von IT-gestützten Aktionen [25, S. 12]. Diese Standarddefinitionen werden in Vorlesungen in dieser oder leicht gewandelter, aber inhaltlich unveränderten Weise genutzt [55], [4], [146].

Neben der Sicherstellung der Korrektheit von Informationen wird die Integrität auch als Verhinderung der unbefugten Änderung von Informationen „prevention of the unauthorised modification of information“ definiert [49]. In der Zuverlässigkeitsforschung ist Integrität die Abwesenheit von unsachgemäßen Systemänderungen, wobei unsachgemäß hier unbefugt bedeutet: „absence of improper system alterations with improper meaning unauthorized“ [85].

Beispiele für formale Modelle, welche die Integrität eines Computers beschreiben und umsetzen, sind das:

- Biba-Modell (Integritätsüberlegungen für sichere Computersysteme) [7],
- Clark-Wilson-Modell (Ein Vergleich von kommerziellen und militärischen Computersicherheitsrichtlinien) [34].

Bedingungen und Eigenschaften von Integrität

Zusammenfassend lassen sich aus den Wortbedeutungen von Integrität, der Betrachtung von Integrität aus rechtlicher Sicht, aus anderen Fachgebieten und aus informationstechnischer Sicht bestimmte Eigenschaften und Bedingungen identifizieren, die es möglich machen, festzustellen, ob bei einer Organisation der Aspekt der Integrität betroffen ist, wann die Integrität verletzt wird und wann es Rechtfertigungsgründe gibt, welche eine Integritätsverletzung zulassen.

Folgende Eigenschaften müssen für die Integrität erfüllt sein:

- Zugänglich für Befugte,
- Unverfälschtheit, Unversehrtheit, Vollständigkeit der Information,
- Schützenswerte oder bewahrenswerte Informationen.

Die Integrität ist verletzt, wenn es sich um eine unbefugte (unerlaubte) oder rechtswidrige (regelwidrige) Änderung, Beeinflussung, Korruption, Manipulation, Veränderung, Verfälschung der internen Konsistenz oder der Funktionsweise eines Systems oder von Informationen handelt.

Die Integritätsverletzung ist zulässig, wenn:

- eine gesetzliche Grundlage vorhanden ist oder
- eine Zustimmung des Inhabers der Information vorliegt.

Militärische oder Regierungsorganisationen verarbeiten innerhalb unterschiedlicher Informationsräume in ihren/ihrer Anwendungen[1], Infrastruktur[2], IT-Systemen[3] und Netzen[4] Verschlusssachen und Staatsgeheimnisse. Diese Verarbeitung bedingt die Eigenschaften von Vertraulichkeit und Integrität, da es sich um geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse handelt, die nur einem begrenzten Personenkreis zugänglich, je nach Schutzbedarf in unterschiedliche Geheimhaltungsgrade einzustufen und vor dem Verlust der Vertraulichkeit und Integrität zu schützen sind [23, §93 StGB], [27]. Der folgende Abschnitt untersucht nun, ob und wo dabei Probleme auftreten und es Vertraulichkeits- und/oder Integritätsverluste gibt.

[1] Anwendungen sind Software und Dienste, die zur Verarbeitung von Verschlusssachen/Staatsgeheimnissen genutzt werden.

[2] Die Infrastruktur umfasst alle baulich-physischen Gegebenheiten. Dies beinhaltet Gebäude, Energieversorgung, Klimatisierung, Räume und die Verkabelung.

[3] IT-Systeme sind technische Anlagen, die der Verarbeitung von Verschlusssachen/Staatsgeheimnissen dienen. Dies schließt u.a. Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches, Drucker, Kopierer, Fax und Sicherheitsgateways ein.

[4] Unter Netzen werden alle Aspekte verstanden, die sich auf die Kommunikation und Verbindungen zwischen diesen IT-Systemen beziehen. Dies inkludiert zum Beispiel Bluetooth, LAN, Modem, VOIP, VPN, und WLAN.

2.3. Vertraulichkeits- und Integritätsverluste

Im letzten Abschnitt wurde erläutert, dass Integrität und Vertraulichkeit Zielgrößen in IT-Systemen zur Verarbeitung von Verschlusssachen und Staatsgeheimnissen sind und welche Bedeutungen sie in unterschiedlichen wissenschaftlichen Gebieten, insbesondere aus Sicht der Informationstechnik, haben. Dabei wurden Eigenschaften identifiziert, welche diese Zielgrößen besitzen, wann eine Verletzung eintritt und welche möglichen Rechtfertigungsgründe es geben könnte. Dieser Abschnitt wird darstellen, dass es gesamtgesellschaftliche Probleme gibt, die Vertraulichkeit und Integrität sicherzustellen, aber diese jedoch auch innerhalb von militärischen und Regierungsorganisationen zu finden sind.

Behörden und andere staatliche Einrichtungen sind auf computergestützte (Cyber-) Informationssysteme und elektronische Daten angewiesen, um ihre Aufgaben durchzuführen und wichtige Informationen zu verarbeiten, zu pflegen und zu melden. Die Sicherheit dieser Systeme und Daten ist entscheidend für das Vertrauen der Öffentlichkeit und die Sicherheit, den Wohlstand und das Wohlergehen des Landes. Ohne die Informationsressourcen und den Schutz dieser ist es schwierig, wenn nicht gar unmöglich, die behördlichen Aufgaben zu erfüllen. Dies kann zu erheblichen Auswirkungen auf ein breites Spektrum staatlicher Tätigkeiten und Vermögenswerte haben [157]:

- Betriebsmittel, wie Zahlungen und Einziehungen, könnten verloren gehen oder gestohlen werden;
- Computerressourcen können für unbefugte Zwecke verwendet werden, einschließlich der Einleitung von Angriffen auf andere;
- sensible Informationen, wie beispielsweise geistiges Eigentum, nationale Sicherheitsdaten und persönlich identifizierbare Informationen, z. B. Steuerzahlerdaten, Sozialversicherungsunterlagen und medizinische Unterlagen können unbefugt hinzugefügt, gelöscht, gelesen, kopiert, offengelegt oder für Zwecke wie Spionage, Identitätsdiebstahl oder andere Arten von Verbrechen geändert werden;
- kritische Operationen, wie z. B. die Unterstützung der nationalen Verteidigungs- und Rettungsdienste, könnten gestört werden;
- Daten können zu Betrugs- oder Störungszwecken verändert oder zerstört werden;
- Behördliche Aufgaben könnten durch peinliche Vorfälle untergraben werden, die das Vertrauen in die Fähigkeit der Behörde, Aufgaben durchzuführen und seiner Verantwortung nachzukommen, mindern.

Die Informationssysteme und Netzwerke militärischer Organisationen und Regierungsorganisationen sind von Natur aus gefährdet. Sie sind hochkomplex und dynamisch, technologisch vielfältig und oft geografisch verstreut. Diese Komplexität erhöht die Schwierigkeit, die unzähligen Betriebssysteme, Anwendungen und Geräte, aus denen die Systeme und Netzwerke bestehen, zu identifizieren, zu verwalten und zu schützen. Hinzu

kommt, dass die von den Bundesbehörden verwendeten Systeme oft mit bekannten und unbekannten Sicherheitslücken behaftet sind [157].

Staatliche Systeme und Netzwerke sind oft auch mit anderen internen und externen Systemen und Netzwerken einschließlich des Internets verbunden, wodurch die Anzahl der Angriffswege erhöht und ihre Angriffsfläche erweitert wird. Darüber hinaus entwickeln sich Cyber-Bedrohungen für Systeme, die den Bund und kritische Infrastrukturen unterstützen, weiter und werden immer ausgefeilter. Diese Bedrohungen kommen aus unterschiedlichen Quellen und unterscheiden sich in der Art und den Fähigkeiten der Akteure, ihrer Handlungsbereitschaft und ihren Motiven [157].

Dazu gibt es verschiedene Berichte und Umfragen über Angriffstypen (z. B. Malware, webbasierte Angriffe, Denial of Service, Physische Manipulation/Schaden/Diebstahl/Verlust oder Phishing), Angriffsvektoren (z. B. Cyberkriminelle, Insider, Nationalstaaten, Unternehmen, Hackaktivisten, Cyber-Kämpfer, Cyber-Terroristen Script-Kiddies), Sektoren (z. B. Bank- und Finanzwesen, Regierung und Vollzugsbehörden, Medizin/Gesundheitswesen) und Kosten von Verstößen [33, 38, 48, 52, 61, 73, 76, 111, 143, 145, 150, 152].

Risiken für Cyberressourcen können durch unbeabsichtigte und absichtliche Bedrohungen entstehen. Dazu gehören Insider-Bedrohungen von unzufriedenen oder nachlässigen Mitarbeitern und Partnern, eskalierende und aufkommende Bedrohungen aus aller Welt, die stetige Weiterentwicklung der Angriffstechnologien und die Entstehung neuer und zerstörerischer Angriffe [157]. Ineffektiver Schutz von Cyberressourcen kann Sicherheitsvorfälle und Cyberattacken erleichtern, die kritischen Vorgänge stören, zu unangemessenem Zugriff auf, Offenlegung, Änderung oder Zerstörung von sensiblen Informationen führen und die nationale Sicherheit, das wirtschaftliche Wohlergehen sowie die öffentliche Gesundheit und Sicherheit gefährden [157].

Im Jahr 2017 wurden sehr viele Investitionen in die IT-Sicherheit getätigt, dennoch ist es auch ein Jahr, in dem Rekorde von Cyber-Angriffen aller Art, Datenschutzverletzungen und Informationsverlusten aufgestellt wurden [48]. Bis Ende 2017 wurden nach einer Studie von Risk Based Security 5.207 Verstöße weltweit gemeldet, die etwa 7,89 Milliarden Datensätze enthüllten [124]. Privilegierte Benutzer stellen dabei die größte Bedrohung dar. Laut einer Umfrage sind privilegierte Benutzer, wie Manager mit Zugang zu sensiblen Informationen, die größte Insider-Bedrohung für Unternehmen (60%), gefolgt von Auftragnehmern und Beratern (57%) und regulären Mitarbeitern (51%) [68]. Physischer Verlust und Diebstahl waren einmal die wichtigsten Ursachen für Datenschutzverletzungen [140], welche durch Hacking oder Malware im Ranking abgelöst wurden. Dennoch sind sie nach wie vor eine der Hauptursachen für Datenschutzverletzungen [151]. Nachfolgend werden einige Beispiele dargestellt, in der die Ursachen der Verstöße und die Auswirkungen auf den öffentlichen Sektor und die Wirtschaft signifikant waren:

2013 wurden drei Milliarden Yahoo-Konten durch einen Hack kompromittiert. Dies war vermutlich eine der größten Datenschutzverletzungen. Alle Yahoo-Nutzer waren von der Verletzung betroffen. Dies wurde erst 2017 durch Yahoo bestätigt [36].

Zwischen Februar und März 2014 forderte eBay 145 Millionen Benutzer auf, ihre Konto-Passwörter zu ändern. Grund dafür war ein Angriff, der verschlüsselte Passwörter

zusammen mit anderen persönlichen Daten gefährdete. Hacker erhielten Zugang zu eBay-Konten durch gestohlene Zugangsdaten, welche nicht von den Kunden selbst stammten, sondern von eBay-Mitarbeitern [154].

Im Jahr 2017 wurde das Kreditbüro Equifax angegriffen, wodurch die Daten von über 147 Millionen Amerikanern und vielen Menschen in anderen Ländern gefährdet wurden. Dabei wurden Identitäten, darunter der Name, Teile der Informationen auf dem Führerschein und/oder die Sozialversicherungsnummer gestohlen. Hacker konnten Equifax knacken, indem sie eine Schwachstelle in der Open-Source-Software Apache Struts ausnutzten [54].

2018 wurde bekannt, dass die Firma Cambridge Analytica Facebook-Daten von mehr als 87 Millionen Nutzern für eigene Analysen und Umfragen sammelte. Die Daten wurden durch eine Anwendung namens „thisisyourdigitallife“ gesammelt. Diese wurde von Aleksandr Kogan, einem Akademiker der Universität Cambridge, durch seine Firma Global Science Research in Zusammenarbeit mit Cambridge Analytica entwickelt. Hunderttausende von Nutzern erhielten eine geringe Aufwandsentschädigung für einen Persönlichkeitstest und stimmten der Erhebung ihrer Daten zu. Die Anwendung erfasste aber auch die Informationen der Freunde der Teilnehmer, was die immense Anhäufung von Daten von weiteren Millionen Nutzern ermöglichte [135].

Die dargestellten Vorfälle zeigen, dass Vertraulichkeits- und Integritätsverluste ein generelles Problem sind. Nachfolgend wird dargestellt, dass auch der Staat und das Militär Opfer von Datenschutzverletzungen und Informationsverlusten sind.

Cyber-Angriffe auf die Regierungsnetze werden täglich durchgeführt [17], [18]. Dabei sind die Regierungsnetze neben ungezielten Massenangriffen auch von gezielten Angriffskampagnen betroffen. E-Mails mit Schadprogrammen gehören zu den am häufigsten gezählten Angriffen auf die Bundesverwaltung [17], [18]. Die Angreifer benutzen häufig E-Mail-Anhänge mit in Archiven gepacktem JavaScript oder Makrocode in Office-Dokumenten, um dann das eigentliche Schadprogramm aus dem Internet nachzuladen. Vereinzelt sind unter den Angriffen auch persistente Watering-Hole-Angriffe, bei denen Täter mit Spionagehintergrund Schadcode auf von Regierungsmitarbeitern häufig genutzten Webseiten platzieren. Der Schadcode wird dabei im Abstand von mehreren Monaten durch neue Varianten ersetzt [17], [18].

Im Mai 2015 wurde der Deutsche Bundestag angegriffen. Dabei wurden mindestens 16 Abgeordnetenbüros durch einen digitalen Angriff infiltriert, um Postfächer zu kopieren, Festplatten auszuspionieren und dadurch an vertrauliche Daten zu gelangen [161].

Das Identity Theft Resource Center verfolgt seit 2005 Sicherheitslücken in den USA. Es unterscheidet dabei in verschiedene Branchen der Cybersicherheitsverletzungen. Diese sind Unternehmen, Bildungswesen, Gesundheitsversorgung, Regierung/Militär und Finanzwesen. Aus den vorhandenen Daten lässt sich feststellen, dass im Regierungs- und Militärsektor über einen Betrachtungszeitraum von 13 Jahren (2005-2017) im Durchschnitt pro Jahr 77 Cybersicherheitsverletzungen gemeldet worden sind [73].

Ein ehemaliger Auftragnehmer der Nationalen Sicherheitsbehörde der USA wurde wegen Verletzung des Spionagegesetzes im August 2016 angeklagt. Grund für diese Anklage war der Diebstahl von circa 50 Terrabyte an klassifizierten Daten über einen Zeitraum von 20 Jahren. Dies wird als der größte Diebstahl von klassifiziertem Regierungsmaterial

aller Zeiten angesehen [155].

Am 25. Februar 2017 wurde von Sicherheitsforschern über Twitter bekannt gegeben, dass die US Airforce schwere Datenschutzverletzungen erlitten hat. Dabei wurde aufgedeckt, dass eine große Masse von klassifizierten und damit sensiblen Datensätze enthüllt wurden [147].

Auch die Bundeswehr ist von solchen Vorfällen betroffen, wie folgende Beispiele zeigen:

Im August 2010 wurden Aussagen einer eingestuften Studie vor einer Freigabe im Internet veröffentlicht, in der es um sicherheitspolitische Implikationen knapper Ressourcen ging [116].

Im Juni 2011 wurde ein Bild in der Bildzeitung veröffentlicht, welches aus einem geheimen Bundeswehrdokument stammt. Es zeigte einen Schützenpanzer vom Typ Marder, wie er nach einem Anschlag aussah [9]. Das Bild wurde im Nachhinein von der Online-Plattform wieder entfernt.

Im November 2017 wurden ebenfalls eingestufte Aussagen der „Strategischen Vorausschau 2040“ im Spiegel veröffentlicht. Hierbei handelt es sich um eine Studie, in der gesellschaftliche und politische Trends bis 2040 durchgespielt werden [129].

2.4. Methoden, Mittel und Maßnahmen zur Sicherstellung von Vertraulichkeit und Integrität

Zur Sicherstellung der Vertraulichkeit und Integrität gibt es verschiedene Methoden, Mittel und Maßnahmen. Hierbei kann man diese in unterschiedliche Bereiche einteilen. So gibt es infrastrukturelle, organisatorische, personelle und informationstechnische Maßnahmen. Typische Vertreter in diesen Bereichen sind:

- Infrastrukturelle Maßnahmen [13], [16], [43], [48], [65], [66], [112]:
  - Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
  - Regelungen für Zutritt (Bildung von Sicherheitszonen/-bereichen, Zutrittskontrollsystem)
- Organisatorische Maßnahmen [13], [16], [43], [46], [48], [56], [64], [65], [66], [112]:
  - Festlegung von Verantwortlichkeiten und Regelungen
  - Informationsbeschaffung über Sicherheitslücken des Systems
  - Nutzungsverbot nicht freigegebener Hard- und Software
  - Regelung des Passwortgebrauchs
  - Regelungen für den Einsatz von Fremdpersonal
  - Software-Abnahme- und Freigabe-Verfahren
  - Vergabe von Zutritts-/Zugangsberechtigungen
  - Vergabe von Zugriffsrechten
  - Zutrittsregelung und -kontrolle

- Personelle Maßnahmen [13], [16], [43], [48], [64], [65], [66], [81], [110], [112]:
  - Einweisung und Schulung der Mitarbeiter in die Nutzung der Informationstechnik
  - Sensibilisierung der Mitarbeiter für mögliche Gefährdungen
  - Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- Informationstechnische Maßnahmen [1], [13], [16], [43], [46], [48], [56], [64], [65], [66], [70], [81], [94], [110], [112]:
  - Bildschirmsperre
  - Einsatz von Demilitarisierten Zonen (DMZ) in Verbindung mit Firewalls
  - Einsatz von Intrusion Detection- und Intrusion Prevention Systemen
  - Einsatz von Protokollierung
  - Einsatz von Verschlüsselung, Kryptomodulen, Checksummen oder Digitalen Signaturen
  - Einsatz von Viren-Schutzprogrammen
  - Elektronische Authentifizierungsverfahren
  - Passwortschutz für IT-Systeme, inklusive der regelmäßigen Änderung
  - Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras
  - Verhinderung des Abgreifens von vertraulichen Informationen durch marktverfügbare Lösungen wie [20], [71], [75]
  - Zugriffsbeschränkung (wie z. B. Öffnen, Drucken, Kopieren, Ändern) von Dokumenten

Die in Abschnitt 2.3 dargestellten Beispiele zeigen, dass die hier genannten Maßnahmen nicht ausreichen, um Vertraulichkeits- und Integritätsverluste zu verhindern. Daher wird im folgenden Abschnitt das zu untersuchende Problem erläutert.

2.5. Problemdarstellung

Wie in Abschnitt 2.1 dargestellt, ist ein gemeinsamer Ansatz für den Umgang mit sensiblen Daten das Konzept der *Informationsklassifizierung* nach Geheimhaltungsgraden [51], [21]. Verschiedene Datenelemente, wie z. B. Papierdokumente und Computerdateien, werden entsprechend ihrer Sicherheitsempfindlichkeit klassifiziert. Die Gruppierung erfolgt nach dem Begriff der *Informationsräume*. Dabei wird der *virtuelle, IT-gestützte Informationsraum* nach den Geheimhaltungsgraden, wie z. B. „STRENG GEHEIM“, „GEHEIM“, „VS-NfD“ und „OFFEN“ strukturiert. Organisationen in der NATO, in der EU oder in einem Land (z. B. Deutschland) verfügen über unterschiedliche operationelle

Netzknotenstrukturen und verarbeiten klassifizierte Daten zwischen diesen Netzknoten durch Nutzung unterschiedlicher Informationsräume.

Alle Datenelemente in einer Organisation, ihre Speichermöglichkeiten und die darauf zugreifenden Personen werden nach diesem Schema kategorisiert. Die täglichen Abläufe und die IT-Infrastruktur sind nun verpflichtet, den Lese- und Schreibzugriff auf Datenelemente so zu regeln, dass ihr Informationsraum berücksichtigt wird. Die notwendige Zugangskontrolle und -überwachung kann wie in Abschnitt 2.4 dargestellt durch Softwaremechanismen, wie Zugriffskontrolle, elektronische Authentifizierungsverfahren und automatisierte Sicherheitsaudits oder durch klassische Sicherheitsmittel, wie physische Trennung und Zugangssicherung erfolgen.

Abbildung 2.2 zeigt die potenziellen Sicherheitsrisiken für eine Infrastruktur, welche auf der Idee der Informationsräume basiert. Am Beispiel von drei Schutzkategorien (OFFEN = DEU_0, VS-NUR-FÜR-DEN-DIENSTGEBRAUCH (VS-NfD) = DEU_1, GEHEIM = DEU_3) zeigt sich, dass sie sich gegenseitig einschließen, d.h. jede offene Information kann wie eine geheime Information behandelt werden, aber nicht umgekehrt. Es gibt 4 mögliche *Informationsflüsse*, die nun stattfinden können:

Der erste Informationsfluss speichert ein niedrig klassifiziertes Dokument auf einem niedrig klassifizierten Server, was eine zulässige Aktivität ist. Der zweite mögliche Informationsfluss speichert ein niedrig klassifiziertes Dokument auf einem hoch klassifizierten Server. Dieser Informationsfluss ist nur in eine Richtung zulässig, ein Informationsrückfluss muss vermieden werden. Dies wird typischerweise mit einer Datendiode [62] erreicht. Der dritte Informationsfluss versucht, ein hoch klassifiziertes Dokument auf einen niedrig klassifizierten Server zu übertragen. Dieser Informationsfluss ist verboten. Der vierte Informationsfluss speichert ein hoch klassifiziertes Dokument auf einem hoch klassifizierten Server, was wiederum eine erlaubte Aktivität ist.

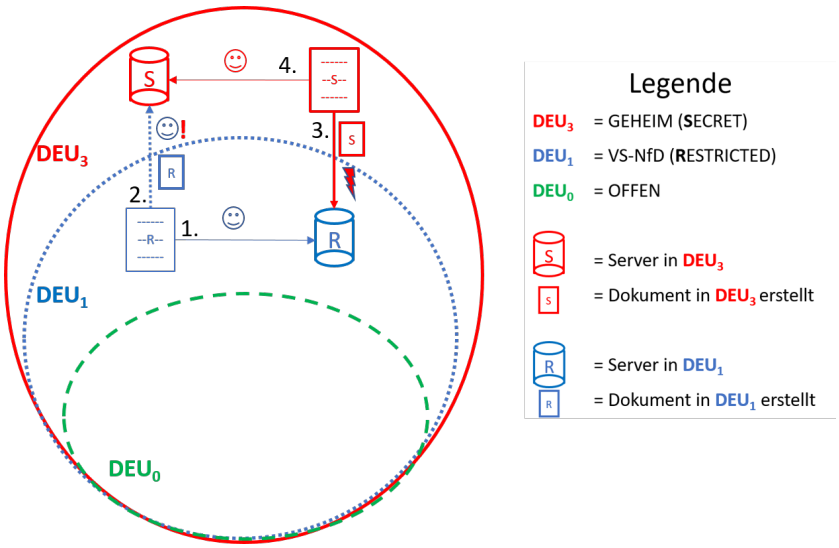

Abbildung 2.2.: Informationsräume/-flüsse und -bedrohungen

Ausgehend von diesem allgemeinen Grundsatz bestehen die folgenden Sicherheitsrisiken:

- Informationsflüsse von einem höheren Informationsraum zu einem niedrigeren Informationsraum
- Unkontrollierter Informationsfluss vom unteren zum oberen Informationsraum (Rückflussproblem - 2. Informationsfluss in Abbildung 2.2)
- Informationsflüsse zwischen nicht kategorisierten externen Stakeholdern und internen Servern

Es ist zu beachten, dass „OFFEN“ nicht gleichbedeutend mit einem uneingeschränkten Lese- oder Schreibzugriff für externe Parteien ist. Die gesamte Infrastruktur des Informationsraums wird nach wie vor als geschlossenes System behandelt. Das Problemszenario lässt sich leicht auf menschlichen Interessengruppen erweitern, die ebenfalls zu einem bestimmten Informationsraum gehören. Sie können als eine spezielle Art von „Server“ behandelt werden, der Lese- und Schreibzugriff auf ein geheimes Dokument erhält.

2.6. Idee der Arbeit

Das untersuchte Problem im Kontext dieser Arbeit kann informell wie folgt formuliert werden: Angesichts einer Reihe von „Geheimhaltungsgraden“, die den „Informationsräumen“ entsprechen, und einer genauen Spezifikation möglicher Wege, auf denen Informationen zwischen ihnen fließen können, soll eine Methodik konstruiert werden, welche alle Objekte eines Geheimhaltungsgrades in einem Informationsraum darstellt. Daraufhin sollen zunächst alle Verbindungen identifiziert werden, welche innerhalb und zwischen den Informationsräumen existieren. Ein besonderer Fokus liegt auf den Verbindungen, die zwischen unterschiedlichen Informationsräumen verlaufen. Der Grund hierfür ist, dass eine direkte physische Verbindung zwischen diesen Informationsräumen potentiell nicht zulässig ist [25]. Aufgrund von Sicherheitsverletzungen ist der Verlust von Vertraulichkeit und Integrität dann immanent. Gültige Informationspfade könnten zur Durchführung illegaler und unerwünschter Operationen verwendet werden. Wenn Verschlusssachen unbefugt veröffentlicht werden, hat dies Auswirkungen auf die beteiligten Gruppen, da sie eine Bedrohung, einen Schaden oder Nachteil für die Beteiligten der Interessengruppen darstellen könnten.

Angesichts der beschriebenen Problematik ist die Idee der Arbeit, Modellierungs- und Analyseansätze zu entwickeln, die Informationsflüsse innerhalb und zwischen verschiedenen Informationsräumen identifizieren und analysieren. Dabei sollen militärische Informationssysteme innerhalb unterschiedlicher Informationsräume zur Darstellung von Datenflüssen modelliert und Bedrohungsanalysen in diesen Informationssystemen durchgeführt werden, um Strategien für konkrete Handlungsoptionen in der Zukunft abzuleiten. Die gewählten Ansätze sollen den Austausch mit externen Experten ermöglichen, welche nicht über die Freigabe zur Betrachtung klassifizierter Daten verfügen.

2.7. Forschungsfragen

Ableitend aus dem dargestellten Problem sind folgende Fragestellungen in Bezug auf die zugrunde liegenden Bedrohungen entstanden.

2.7.1. Forschungsfragen - Bedrohungsmodell

Zunächst ist es wichtig festzustellen, welche konkreten Bedrohungen für militärische und Regierungsorganisationen vorliegen. Dazu werden folgende Forschungsfragen aufgestellt:

1. Welche Bedrohungsklassifikationen und Angreiferstrategien gibt es?
2. Wie sieht ein praktikables Bedrohungsmodell für militärische und Regierungsorganisationen aus?

Die Antworten auf diese Fragen werden im Kapitel 3 und 4 erörtert. Bei den nun folgenden Fragen wird bereits das Konzept zur Kategorisierung von Bedrohungen verwendet, welches aus dem Bedrohungsmodell entsteht und im Kapitel 4 im Detail eingeführt wird. Das Bedrohungsmodell liefert verschiedene Angreiferstrategien, u.a. Informationsgewinnung und Angriff auf das Ziel. Daraus entstehen folgende Forschungsfragen:

2.7.2. Forschungsfragen - Informationsgewinnung

Nach Zugriff auf Infrastruktur, Anwendungen, IT-Systeme und Netze versuchen die Angreifer Informationen zu gewinnen. Eine Art der Informationsgewinnung ist die Identifizierung wichtiger operationeller Netzknoten innerhalb von Informationsräumen zwischen denen Informationen ausgetauscht werden. Eine weitere Art der Informationsgewinnung ist die Identifizierung von Geheimhaltungsgraden. Daraus ergeben sich folgende Forschungsfragen:

1. Wie kann man feststellen, welche operationellen Netzknoten in Informationsräumen wichtig sind?
2. Wie kann man feststellen, welche Geheimhaltungsgrade innerhalb von Informationsräumen vorhanden sind?

Die Antworten auf diese Fragen werden im Kapitel 5 präsentiert.

2.7.3. Forschungsfragen - Angriff auf das Ziel

Nachdem bestimmte Informationen gewonnen wurden, erfolgt der Angriff auf das Ziel. Eine Bedrohung ist der Informationsfluss von oben (z. B. GEHEIM) nach unten (z. B. Öffentlich) [6]. Weitere Bedrohungen sind die Überwindung der physikalischen Grenzen zwischen Informationsräumen sowie das unbefugte Eindringen in Informationsräume. Daraus kann man folgende Forschungsfragen ableiten:

1. Wie kann man den Informationsfluss innerhalb und zwischen Informationsräumen feststellen?

2. Wie kann man die Überwindung der physikalischen Trennung zwischen Informationsräumen feststellen?

3. Wie kann man das unbefugte Eindringen in Informationsräume feststellen?

Antworten auf diese Fragen werden im Kapitel 6 und in Kapitel 7 diskutiert.

2.8. Zusammenfassung

Vertraulichkeit und Integrität sind nichtfunktionale Eigenschaften in IT-Systemen zur Verarbeitung von Verschlusssachen und Staatsgeheimnissen. Dieses Kapitel hat gezeigt, dass diese Sicherheitsziele an einigen Stellen nicht erfüllt sind und welche Probleme daraus u.a. für militärische oder Regierungsorganisationen entstehen. Desweiteren wurde die Idee der Arbeit diskutiert und Forschungsfragen aufgestellt. In den folgenden beiden Kapiteln wird untersucht, warum diese Eigenschaften nicht erfüllt werden. Dabei wird das Bedrohungsmodell für militärische Organisationen und Regierungsorganisationen entwickelt.

3. Bedrohungen

Das letzte Kapitel hat gezeigt, dass Vertraulichkeits- und Integritätsverluste gesamtgesellschaftliche Probleme sind. Regierungsnetze des Staates und Netzes des Militärs, in denen Verschlusssachen und Staatsgeheimnisse verarbeitet werden, sind dabei ebenfalls Ziel von Angriffskampagnen. Die IT-Sicherheitsziele Vertraulichkeit und Integrität werden dann nicht erfüllt. Ursache dafür sind Bedrohungen, welche auf die Infrastruktur, IT-Systeme, Netze, Anwendungen, Menschen und Informationsräume einwirken [16]. Dieses Kapitel wird diese Bedrohungen untersuchen bzw. genauer beleuchten und dafür die Ergebnisse einer Literaturrecherche präsentieren.

Eine Bedrohung ist ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann [16, S. 99]. Für die Integrität bedeutet diese Beeinträchtigung die unbefugte Änderung, Beeinflussung, Korruption, Manipulation, Veränderung, Verfälschung der internen Konsistenz oder der Funktionsweise eines Systems oder von Informationen (vgl. Abschnitt 2.2.2). Für die Vertraulichkeit ist es der/die/das unbefugte Aufnahme, Abhören, Erwerb, Kenntnis, Mitteilung, Nutzung, Offenbarung, Offenlegung, Öffnung, Preisgabe oder Weitergabe von nicht-öffentlichen oder verschlossenen Informationen (vgl. Abschnitt 2.2.1). Das IT-Sicherheitsziel Verfügbarkeit (availability) ist nicht Gegenstand der Betrachtung dieser Arbeit. Daher wird auf eine genauere Untersuchung der Beeinträchtigung des Ziels durch Bedrohungen verzichtet.

3.1. Methodik der Literaturrecherche

Um einen verständlichen und nachvollziehbaren Überblick der Bedrohungen der Vertraulichkeit und Integrität zu erhalten, die in militärischen oder Regierungsorganisationen auftreten können, wurde eine Literaturrecherche durchgeführt. Damit dieser Überblick möglichst breit und umfassend ist, wurden die Datenbanksysteme der IEEE[1], ACM[2], Google Scholar[3] und die Bibliotheken der Berliner Universitäten, z. B. die Humboldt-Universität (HU) Berlin[4] genutzt. Es wurde in einem ersten Schritt nach Konferenz-

[1] https://ieeexplore.ieee.org/
[2] http://dl.acm.org/
[3] https://scholar.google.de/
[4] https://hu-berlin.hosted.exlibrisgroup.com/primo_library/

Publikationen, Standards und Büchern gesucht, welche folgende Stichwörter für die Bereiche Anwendungen, IT-System, Netze, Menschen und Infrastruktur enthielten:

- „Bedrohungen“ (engl. „Threats“),
- „Bedrohungsmodelle“ (engl. „Threat Models“),
- „Bedrohungsklassifikationen“ (engl. „Threat Classifications“),
- „Angriffe“ (engl. „Attacks“),
- „Angriffsmuster“ (engl. „Attack Patterns“),
- „Angreiferstrategie“ (engl. „Attack Strategy“),

Nach dieser recht allgemeinen Suche wurden anhand der Literaturverzeichnisse und der in der Quellen enthaltenen Fachbegriffen weitere Quellen erschlossen. Die gefundenen Bedrohungen wurden in das Bedrohungsmodell integriert, welches in Kapitel 4 näher erläutert wird. Bedrohungen und Angriffe auf die Verfügbarkeit wurden von denen auf die Vertraulichkeit und Integrität getrennt und nicht in das Bedrohungsmodell aufgenommen. Die Sortierung erfolgte nach vorhandenen und möglichen künftigen Bestandteilen von militärischen und Regierungsorganisationen. Für die weitergehende Recherche in den identifizierten Quellen wurden für die Bereiche Anwendungen, IT-System, Netze, Menschen und Infrastruktur folgende Suchbegriffe verwendet:

Infrastruktur

- Räume
- Gebäude
- Verkabelung

IT-System

- Adapter, Router, Switch, Hub
- Drucker
- Fax
- Kryptomodul
- Laptop, Smartphone, Tablet, USB
- Server
- Tastatur
- Speicher
- Virtualisierung

Netze

- Protokolle (z. B. IP, FTP, TLS)
- Bluetooth
- DNS
- LAN
- VOIP
- VPN
- WLAN

Anwendungen

- Software
- Betriebssysteme
- Dienste

Menschen

- Social Engineering
- Fehler und Unterlassung
- Administration
- Vorsatz, Fahrlässigkeit
- Phishing

In einem letzten Schritt wurde eruiert, ob es in der Literatur und den bereits identifizierten Quellen spezielle Bedrohungen für den Bereich Informationsräume gibt. Dabei wurden folgende Suchbegriffe genutzt:

Informationsräume

- „Geheimhaltungsgrade“
- „Kenntnis nur wenn nötig/Need to know“
- „Informationsräume“

Schließlich wurden die gefundenen Angreiferstrategien und Bedrohungsklassifikationen strukturiert (siehe Abschnitt 3.2) und daraus das Bedrohungsmodell dieser Arbeit abgeleitet (siehe Kapitel 4).

3.2. Bedrohungsklassifikationsschemen/Angreiferstrategien

In der Literatur gibt es unterschiedliche Darstellungen von Angreiferstrategien und wie man eine große Anzahl von Bedrohungen klassifizieren kann. Einige Quellen *listen die häufigsten Bedrohungen* oder *die häufigsten Schwachstellen* auf. Darüber hinaus gibt es *angriffsbasierte*, *kriterienbasierte* und *strategiebasierte* Bedrohungsklassifikationsschemen.

3.2.1. Auflistung der häufigsten Bedrohungen

Einige Literaturquellen geben einen Überblick über die häufigsten Bedrohungen, um Organisationen die Möglichkeit zu geben, ihre eigene Bedrohungsumgebung mit diesen Bedrohungen abzugleichen. Die NIST-Klassifikation [66] basiert auf Häufigkeit- und Signifikanzkriterien und unterscheidet folgende Sicherheitsbedrohungen:

- Fehler und Unterlassung („Errors and Omissions“),
- Betrug und Diebstahl („Fraud and Theft“),
- Sabotage durch Mitarbeiter („Employee Sabotage“),
- Verlust der physischen und Infrastrukturunterstützung („Loss of Physical and Infrastructure Support)“,
- Abhören von Daten („Interception of Data“),
- Böswillige Hacker („Malicious Hackers”),
- Industriespionage („Industrial Espionage”),
- Böswilliger Code („Malicious Code“),
- Ausländische Regierungsspionage („Foreign Government Espionage“),
- Bedrohung der Privatsphäre („Threats to Personal Privacy”) [66].

Diese Darstellung ist sehr allgemein, gibt einen ersten Überblick und kann gut genutzt werden, um sie auf die eigene Organisation anzupassen bzw. das eigene Bedrohungsprofil zu schärfen.

In [43] werden die häufigsten Cyberangriffe dargestellt und erläutert. Es sind insgesamt 27, wovon hier nur einige, in Gruppen zusammengefasst, genannt werden:

- Anwendungsangriffe per E-mail, wie z. B. Phishing/Spearphishing oder Malware/Botnet/Ransomware,
- Angriffe auf Webseiten, wie z. B. Drive-By/Watering Hole/Malvertising/Graffiti,
- Angriffe auf die Identität oder Passwörter, wie z. B. Keylogging/Session Hijacking, Pass-the-Hash and Pass-the-Ticket, Credential Harvesting, Idenitity Theft,

- gezielte Angriffe auf die Verfügbarkeit, wie z. B. DDoS, Burndown/Meltdown (Angriff, welches das Opfer zurück in die „Steinzeit – Bleistift und Papier“ bringt),
- weitere typische Angriffe, wie z. B. Industriespionage, Sabotage oder Decapitation – wörtlich Enthauptung, gemeint ist ein gezielter Angriff auf die Unternehmensführung [43].

Diese Darstellung gibt einen guten Überblick über einzelne Bedrohungen. Die jeweilige Organisation kann sie nutzen, um festzustellen, ob sie von dieser Art von Bedrohung betroffen sein könnte.

Das „Open Web Application Security Project“ (OWASP) beschreibt die wichtigsten Sicherheitsrisiken für Webanwendungen. Die Auflistung dieser Risiken soll Organisationen in die Lage versetzen, ein Bewusstsein zu schaffen und diese Risiken in ihren Organisationen zu reduzieren. Die wichtigsten Sicherheitsrisiken sind:

- Einspeisung/Einbringung („Injection“ – Dabei werden nicht vertrauenswürdige Daten als Teil eines Befehls oder einer Abfrage an einen Interpreter gesendet. Daraus folgen die Ausführung unbeabsichtigter Befehle, Zugriff auf sensible Daten ohne die erforderliche Berechtigung zu haben.),
- Gebrochene Authentifizierung („Broken Authentication“ – Schwachstellen in diesem Bereich ermöglichen es, Angreifern Passwörter, Schlüssel oder Sitzungstoken zu kompromittieren, um die Identität anderer Benutzer vorübergehend oder dauerhaft anzunehmen.),
- Exposition sensibler Daten („Sensitive Data Exposure“),
- Externe XML-Entitäten („XML External Entities“ (XXE) – XXE können genutzt werden, um interne Daten offenzulegen),
- Gestörte bzw. gebrochene Zugriffskontrolle („Broken Access Control“ – Nutzung und Zugriff auf nicht autorisierte Funktionen und/oder Daten, z. B. Einsicht in vertrauliche Dateien, Zugriff auf Konten anderer Benutzer, Ändern von Zugriffsrechten),
- Sicherheitsfehlkonfiguration („Security Misconfiguration“ – dies betrifft die sichere Konfiguration der Systeme, das Patchmanagement und die Aktualisierung aller Komponenten),
- Websiteübergreifendes Scripting („Cross-Site Scripting“ (XSS) – XSS ermöglicht es Angreifern, Skripte im Browser des Opfers auszuführen, Websites zu verunstalten, Benutzersitzungen zu übernehmen oder den Benutzer auf bösartige Websites umzuleiten),
- unsichere Umwandlung von Datenströmen in Objekte („Insecure Deserialization“ – Diese Schwachstellen können genutzt werden, um z. B. Replay-Attacken, Injektions-Attacken und Privileg-Eskalations-Attacken durchzuführen),

- die Nutzung von Komponenten mit bekannten Schwachstellen („Using Components with Known Vulnerabilities“ - Sicherheitslücken in diesen Komponenten können z. B. die Abwehrmechanismen der Anwendung untergraben),
- unzureichende Protokollierung und Überwachung („Insufficient Logging & Monitoring“) [136].

Ein detaillierter Gefährdungskatalog im gleichen Anwendungsfeld der Kompromittierung einer Webseite, ihrer Daten oder ihrer Benutzer ist die Bedrohungsklassifizierung des Web Application Security Consortiums (WASC). Diese beschreibt insgesamt 34 Angriffe und 15 Schwachstellen [153].

3.2.2. Auflistung von Schwachstellen durch Gruppierung

Wesentlich detaillierter sind die Quellen, welche die Masse der Schwachstellen zunächst erfasst und dann nach bestimmten Kategorien oder Konzepten strukturiert haben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) listet zur Darstellung der Gefährdungslage im Grundschutzkatalog insgesamt 710 Bedrohungen für die IT-Sicherheitsziele Verfügbarkeit, Vertraulichkeit und Integrität auf. Diese sind auf sechs Bereiche verteilt: Elementare Gefährdungen (46 Bedrohungen), Höhere Gewalt (19 Bedrohungen), Organisatorische Mängel (214 Bedrohungen), Menschliches Versagen (124 Bedrohungen), Technisches Versagen (101 Bedrohungen) und Vorsätzliche Handlungen (206 Bedrohungen). Ziel des Grundschutzkataloges ist es, auf Grundlage der Gefährdung spezifische Maßnahmen für die Bereiche Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge zu entwickeln [16]. Der Grundschutzkatalog ist sehr gut geeignet, um für typische Einsatzszenarien Sicherheitsmaßnahmen auszuwählen und den Grundschutz sicherzustellen. Für höhere Schutzbedarfe, die insbesondere bei Verwendung verschiedener Informationsräume entstehen, müssen zusätzliche Sicherheitsanalysen (Erfassung der Bedrohungen, Entwicklung von Maßnahmen) durchgeführt werden.

Der Common Weakness Enumeration (CWE)-Katalog stellt bekannte Softwaresicherheitsprobleme kategorisiert dar, insgesamt 716 Schwachstellen. Er soll als Grundlage für die Schwachstellenidentifikation, -minderung und -prävention dienen. Unterschieden wird dabei in drei Konzeptarten: Forschungskonzepte (Erforschung von Schwachstellen und ihrer gegenseitigen Abhängigkeiten zur Identifizierung und Schließung theoretischer Lücken), Entwicklungskonzepte (Schwächen bei Konzepten in der Softwareentwicklung) und Architekturkonzepte (Identifizierung von Fehlern, die bei der Entwicklung des Designs von Software auftreten können) [37]. Dieser Katalog ist insbesondere für die Nutzung zur Identifikation von Schwachstellen im Bereich der Anwendungssoftware geeignet.

3.2.3. Angriffsbasierte Bedrohungsklassifikationsschemen

Eines der bekanntesten Modelle, um Bedrohungen zu klassifizieren ist das Modell „STRIDE“ von Microsoft. Es wird dabei in sechs Kategorien unterschieden: Spoofing (Vortäuschung), Tampering (Manipulation), Repudiation (Abstreitbarkeit), Information

Disclosure (Offenlegung von Informationen), Denial of Service (Dienstleistungsverhinderung), Elevation of privilege (Erhöhung von Rechten). Ziel der Nutzung des Modells ist es, Bedrohungen in einem System zu erkennen und zu finden. Dabei wird das zu untersuchende System vollständig in Prozesse („processes“), Datenspeicher („data stores“), Datenflüsses („data flows“) und Vertrauensgrenzen („trust boundaries“) zerlegt [133].

Wesentlich ausführlicher ist der CAPEC-Katalog. Dieser Katalog stellt die bekannten Angriffsmuster (insgesamt 519 Angriffsmuster) kategorisiert nach Angriffsmechanismen (Täuschende Interaktionen, Missbrauch bestehender Funktionalitäten, Manipulation von Datenstrukturen, Systemressourcen, Zeitzuständen, Status, Sammlung und Analyse von Informationen, Unterlaufen der Zugriffssteuerung) bzw. Angriffsbereichen (Software, Hardware, Kommunikation, Lieferkette, Social Engineering, physische Sicherheit) dar [5].

A. Wiesauer und J. Sametinger verbinden Sicherheitsdesignmuster („Security Design Pattern“) mit Angriffsmustern des CAPEC-Katalogs, um Lösungen für Angriffsproblematiken leichter identifizieren zu können. Dabei wird die Beschreibung der Angriffsmuster mit dem Zweck und der Absicht der Sicherheitslösung verknüpft [156].

3.2.4. Kriterienbasierte Bedrohungsklassifikationsschemen

Gerić et al. beschreibt in seinem C3-Modell („Information System Security Threat Cube Classification Model“) drei Kriterien. Das erste Kriterium ist die Bedrohungshäufigkeit („Security threat frequency“), also wie oft eine Bedrohung eintritt. Mit diesem Kriterium unterscheidet er sich von vielen anderen Modellen, da das Kriterium dynamisch ist und bei verschiedenen Organisation unterschiedlich sein kann. Das zweite Kriterium benennt das Gebiet oder den Schwerpunktbereich einer Bedrohungsaktivität („Area/Focus Domain“). Hierbei werden fünf vorgegebene Bereiche benannt: Physische Sicherheit, persönliche Sicherheit, Kommunikations- und Datensicherheit und Betriebssicherheit. Das dritte Kriterium, die Angriffsquelle („Security Threat Source“), ist ein häufig genutztes und unterscheidet zwischen Insidern und Außenstehenden [63].

Ruf et al. nutzt ein orthogonales Klassifikationsschema, um die Angriffsbedrohung strukturiert darzustellen. Hierbei wird in drei Unterräume unterschieden. Im ersten Unterraum „Agent“ geht es um den Angreifertyp (Mensch, Technik, Höhere Gewalt). Im zweiten Unterraum „Motivation“ wird beschrieben, warum ein Angreifer einen Angriff durchführt (absichtlich, zufällig). Im dritten Unterraum „Localization“ wird dargestellt, woher die Bedrohung kommt (außerhalb bzw. innerhalb) [117].

Das Bedrohungsklassifikationsmodell von Jouini et al. ist eine Erweiterung des Modells von [117]. Jouini et al. unterscheidet zwischen der Angriffsquelle („source“), dem Angreifertyp („agent“), der Angreifermotivation („motivation“), der Angreiferabsicht („intention“) und den Auswirkungen des Angriffs („impacts“). Zwei Kriterien stellen eine Erweiterung dar, Motivation und Auswirkungen. Bei der Motivation wird zwischen „böswillig“ und „nicht böswillig“ unterschieden. Die Angreiferabsicht (absichtlich, zufällig) ist mit der Angreifermotivation von Ruf [117] gleichzusetzen. Wirklich neu ist das Kriterium „Auswirkungen“. Hierbei wird die Sicherheitsverletzung beschrieben, die von einer Bedrohung ausgeht (Zerstörung, Verletzung, Diebstahl und Verlust, Offenlegung

von Information, illegale Nutzung, Verweigerung der Nutzung, Erhöhung der Berechtigung) [82].

3.2.5. Strategiebasierte Bedrohungsklassifikationsschemen

Donaldson et al. beschreibt einen fünfschrittigen Prozess. Dabei wird in Schritt 1 „Establish Foothold“ durch Ausnutzung verschiedener Schwachstellen ein initialer Zugriff erzeugt. Das Ergebnis dieses Schrittes ist ein kompromittierter Server, Endpoint oder Nutzer-Account. In Schritt 2 „Command and Control“ werden Verbindungen hergestellt, welche es ermöglichen, die Steuerung und Kontrolle über das System zu übernehmen. Danach wird in Schritt 3 „Escalate Privileges“ durch den Angreifer versucht, die Rechte auszuweiten. In Schritt 4 „Move Laterally“ bewegt der Angreifer sich im System, um sein Ziel zu finden. Im letzten Schritt „Complete the Mission“ wird das angegriffene System in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit ausgebeutet [43]. Um einen gezielten Angriff durchführen zu können, müssen vor der Ausnutzung verschiedener Schwachstellen zunächst Informationen über das betreffende Ziel gewonnen werden. Dieser Schritt wurde bei Donaldson et.al nicht beschrieben, da der Fokus auf dem wirksamen Zugriff auf das Ziel lag.

Gaycken erklärt die Angreiferstrategie als 6 Phasen des Hackings. In der ersten Phase „Targeting“ geht es um die Auswahl des Ziels. Unterschieden wird dabei zwischen gezielten und opportunistischen Angriffe. In Phase 2 „Abbildung des Ziels“ versucht der Angreifer eine Lücke bzw. weitere Schwachstellen im System zu finden. Danach erstellt der Angreifer in Phase 3 „Bau des Angriffs“ eine Schadsoftware, welche die gefundenen Schwachstellen im System ausnutzen kann. In Phase 4 „Angriff ins Ziel bringen“ versucht der Angreifer sich, mit Hilfe der zuvor erstellten Schadsoftware, Zugang zum System zu verschaffen, um so lange wie möglich im System zu bleiben. Dabei unterscheidet Gaycken in verschiedene Stufen des Angriffs: Zugang, Ausschaltung weitere Sicherheitsmaßnahmen, Installation und Verstetigung des Angriffs. In Phase 5 „Operation“ beginnt der Angreifer damit Daten und Informationen aus dem System zu entnehmen oder seine gewonnen Rechte auszuweiten. Diese Phase kann unterschiedliche Längen haben. Insbesondere bei „Advanced Persistent Threats (APT)“ kann diese Phase sehr lange dauern. In der letzten Phase „Entfernung des Angriffs“ beseitigt der Angreifer seine Spuren [60]. Gaycken beschreibt bei seiner Darstellung Aktionen, die außerhalb des anzugreifenden Ziels und ohne Zugriff darauf stattfinden (vgl. Phase 1 und Phase 3).

Das BSI unterscheidet in drei Phasen eines Cyber-Angriffs. In Phase 1 „Initiierung“ wird die Absicht (Grundwerte Integrität, Vertraulichkeit, Verfügbarkeit), das Ziel (Informationen, IT-Dienste, IT-Systeme) und die Reichweite des Angriffs (gezielt, ungezielt, großflächig, klein) beschrieben. In Phase 2 „Vorbereitung“ geht es um die Sammlung von Informationen über das Angriffsziel, z. B. Angriffspunkte, welche Angriffswerkzeuge der Angreifer nutzt und wie der Angreifer seinen Angriff tarnt. In Phase 3 „Durchführung“ wird der eigentliche Angriff beschrieben. Dabei wird erläutert, welche Methoden der Angreifer nutzt, um das Ziel zu infiltrieren, welche Angriffspunkt er wählt und wie er seine Spuren beseitigt [19]. Das BSI wählt bei der Darstellung der Angreiferstrategie einen umfassenden Ansatz, welcher von der Angreifermotivation über die Durchführung

bis zur Beseitigung des Angriffs alle möglichen Aspekte beschreibt.

3.3. Bewertung der Literaturrecherche

Dieses Kapitel beschäftigte sich mit dem Problem der Bedrohungsklassifizierung und der Identifizierung von verwandten Arbeiten in diesem Bereich. Ziel war es, Bedrohungsklassifikationen und Angreiferstrategien zu identifizieren. Die Literaturrecherche hat gezeigt, dass einige Quellen sehr breit aufgestellt sind, wie z. B. der „Grundschutzkatalog“ des BSI [16], „Enterprise Cybersecurity“ von Donaldson et al. [43], die „Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description“ [5] oder das „InfoSec Handbook“ von Rao et al. [112]. Andere Quellen hingegen sind in bestimmten Teilbereichen einer Organisation sehr aussagekräftig, wie z. B. „Art of Deception“ von Mitnick et al. [99] für den Teilbereich Menschen, hier insbesondere Social Engineering, oder „WASC Threat Classification“ [153] und „OWASP Top 10“ [136] für den Teilbereich Anwendungen. Für militärische Organisationen und Regierungsorganisationen sind alle identifizierten Quellen nicht hinreichend geeignet, da insbesondere der Teilbereich Informationsräume kaum Beachtung findet. Aber genau dieser Teilbereich ist für diese Organisationen von besonderer Bedeutung. Auf diese Besonderheit wird im folgenden Kapitel 4 durch das abgeleitete Bedrohungsmodell eingegangen.

4. Strategiebasiertes, ganzheitliches Bedrohungsmodell für Organisationen

Kapitel 2 hat des Problem dieser Arbeit, die Sicherheitsrisiken für Informationsräume, präsentiert. Im Kapitel 3 wurde ein Überblick über Bedrohungsklassifikationschemen gegeben. Ableitend aus den zuvor dargestellten Bedrohungsklassifikationsschemen und den darin enthaltenen Bedrohungen wird hier nun ein neues Bedrohungsmodell vorgestellt, welches die Struktur ziviler und staatlicher Organisationen einerseits und die Angreiferperspektive auf einzelne Komponenten dieser Organisationen andererseits kombiniert. Im folgenden Abschnitt wird die Methodik, welche zur Entwicklung dieses Modells geführt hat, und der Aufbau dieses Modells erläutert. Im weiteren Verlauf wird die Anwendung des Modells an einer militärischen Organisation belegt.

4.1. Methodik des Modells

Das Bedrohungsmodell wurde aus den Ergebnissen der Literaturrecherche entwickelt. Der Aufbau einer militärischen bzw. Regierungsorganisation diente dabei als Blaupause für die Suchkriterien. Eine militärische Organisation bzw. Regierungsorganisation besteht aus sechs Teilbereichen:

- Infrastruktur,
- IT-System,
- Netze,
- Anwendungen,
- Menschen und
- Informationsräume.

Die vier erstgenannten sind Bestandteile der Bausteinkataloge des IT-Grundschutz-Katalogs des Bundesamts für Sicherheit in der Informationstechnik [16, S. 73]. Die Teilbereiche „Menschen“ und „Informationsräume“ wurden ergänzt. Der Teilbereich Menschen hat sich insbesondere aus den kriterienbasierten Bedrohungsklassifikationsschemen ergeben, wie z. B. in Gerić et al. [63] oder in Ruf et al. [117]. Der Teilbereich Informationsräume entstand aus der Problemstellung und der besonderen Bedeutung für militärische Organisationen und Regierungsorganisationen.

Die strategiebasierten Bedrohungsklassifikationsschemen in [60], [43], [19] wurden dahingehend weiterentwickelt, dass Dinge, die außerhalb des Angriffsziels stattfinden oder

Hintergründe des Angriffs erläutern, nicht berücksichtigt wurden, wie z. B. Zielauswahl (Targeting), Bau des Angriffs [60] oder Angreifermotivation, Reichweite des Angriffs [19] und jene Dinge, welche zu den Phasen eines Angriffs gehören, wie z. B. Informationsgewinnung, ergänzt wurden.

Daraus entstand das strategiebasierte, ganzheitliche Bedrohungsmodell. Für das Anwendungsbeispiel wurden die in der Literaturrecherche gefundenen Bedrohungen entsprechend ihrer Zugehörigkeit zu Organisationsteilbereichen und Phasen eines Angriffs sortiert. Dabei wurden vorhandene und mögliche künftige Bestandteilen von militärischen und Regierungsorganisationen berücksichtigt. Die Sortierung der Bedrohungen erfolgte anhand der Beschreibungen der gefundenen Bedrohungen. Dadurch war es möglich jede Bedrohung einer bestimmten Unterkategorie zuzuordnen.

4.2. Aufbau

Der grundsätzliche Aufbau des Modells ist in Abbildung 4.1 dargestellt. Das Modell besteht einerseits aus den Teilbereichen der Organisation (den Teilzielen des Angreifers) und andererseits aus den Phasen eines Angriffs.

4.2.1. Teilbereiche einer Organisation - Teilziele eines Angreifers

Aus der Sicht eines Angreifers ist das Erreichen von Verfügbarkeits-, Integritäts- und/oder Vertraulichkeitsverlusten in der avisierten Organisation das Hauptziel. Organisationen bestehen aus sechs Teilbereichen, die alle einzeln Ziel eines Angriffs werden können:

- **Infrastruktur:** Dieses Teilziel umfasst baulich-physikalische Bedingungen, wie z. B. Gebäude, Energieversorgung, Klimatisierung, Räume und Verkabelung,
- **IT-System:** Dieses Teilziel umfasst technische Installationen, welche der Verarbeitung von Informationen innerhalb der Organisation dienen (z. B. Server, Clients, Einzelplatzrechner, Mobiltelefone, Router, Switches, Drucker, Kopierer, Faxgeräte und Sicherheitsgateways),
- **Netze:** Dieses Teilziel bezieht sich auf alle Aspekte der Kommunikation und Verbindungen zwischen den IT-Systemen (z. B. Bluetooth, LAN, Modem, VOIP, VPN und WLAN),
- **Anwendungen:** Dieses Teilziel umfasst eine Liste von Software und Dienstleistungen, die in der Organisation zur Unterstützung seiner Arbeit verwendet werden. Es kann sich um eine eigenständige Anwendung oder um vernetzte Dienste handeln.
- **Menschen:** Diese werden von ihrer Organisation befähigt, Informationen zu verarbeiten und z. B. sicherheitsrelevante Aktivitäten durchzuführen,

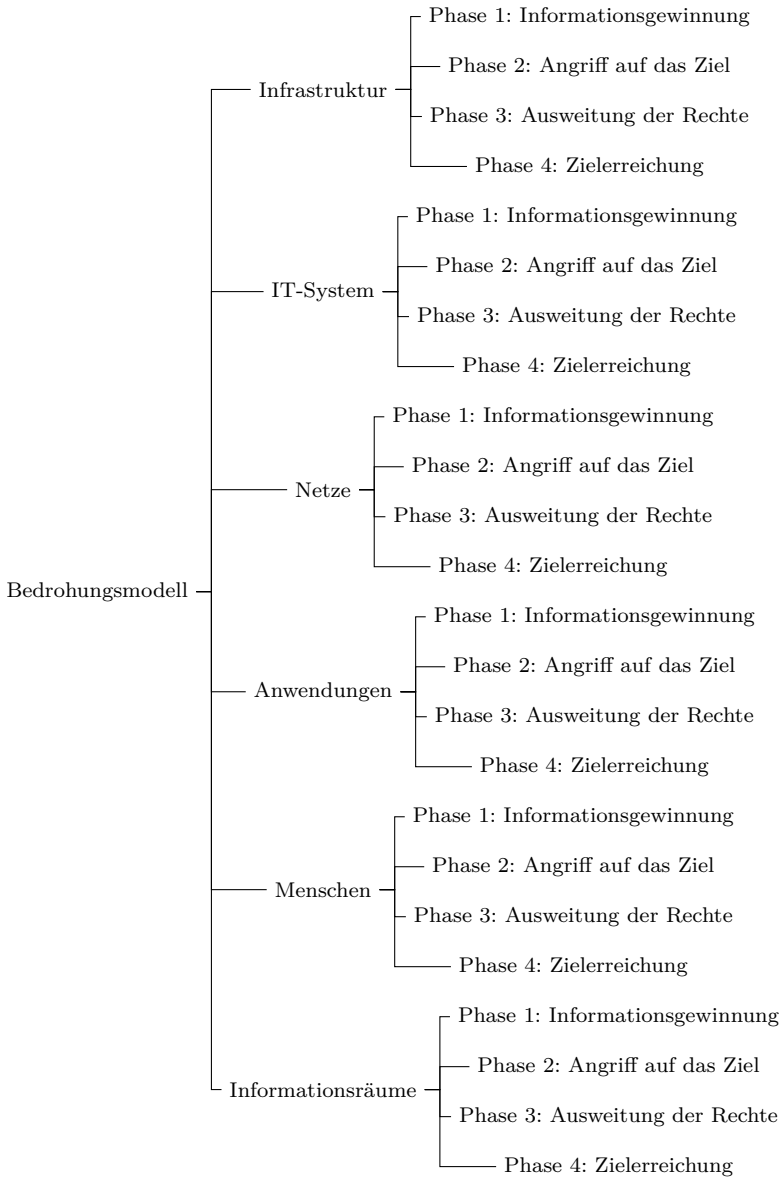

Abbildung 4.1.: Ganzheitliches, strategiebasiertes Bedrohungsmodell

- **Informationsräume:** Dieses Teilziel bezieht sich wie in Abschnitt 2.1 dargestellt auf nationale und internationale Geheimhaltungsgrade (z. B. „GEHEIM“, „VS-NUR-FÜR-DEN-DIENSTGEBRAUCH“, „OFFEN“) und ist ein besonderes Teilziel, weil es im Querschnitt über alle anderen funktioniert. Das bedeutet, dass sich jeder andere Bereich von Regierungs- oder Militärorganisationen innerhalb verschiedener Informationsräumen befinden kann (z. B. geheime Infrastruktur oder offene Infrastruktur). Es handelt sich jedoch um ein separates Teilziel mit eigenen Bedrohungen, die nur aufgrund dieses Bereichs entstehen und nicht den anderen Teilzielen hinzugefügt werden können (z. B. ein unbefugter Informationsfluss von einem geheimen Informationsraum in einen offenen Informationsraum).

4.2.2. Phasen eines Angriffs - Angreiferstrategie

Diese Aufteilung in Teilzielen führt zu einer ersten Reduzierung der Komplexität. Dennoch, wenn Bedrohungen in diese Teilziele eingeteilt werden, ist ihr Umfang für diejenigen, die Entscheidungen über künftige Investitionen im Bereich IT-Sicherheit treffen, noch nicht verständlich genug. Um ein Verständnis des Angreifers zu schaffen und seine Handlungsweisen verstehen zu können, wurden in einem weiteren Schritt Angreiferstrategien über die genannten Teilziele gelegt. Diese Angreiferstrategien bestehen aus 5 Phasen und beschreiben einen Ablauf.

Phase 1 „Informationsgewinnung“ besteht darin, Informationen über das zu kompromittierende System zu finden, zu identifizieren, zu sammeln und zu erhalten. Je nach Ziel (Infrastruktur, IT-System, Netzwerke, Anwendungen, Personen oder Informationsräume) versucht der Angreifer, z. B. Funkwellen abzufangen, Signale aufzunehmen oder Personen zur Informationsweitergabe zu bewegen. Dies hilft dem Angreifer, ein Abbild des Systems zu erstellen und es für weitere Angriffsschritte zu analysieren.

Phase 2 „Angriff auf das Ziel“ befasst sich mit der absichtlichen Gefährdung des Zielsystems. Die durchgeführten Aktionen sind unerwünscht und/oder unbefugt. In diesem Fall werden gefälschte Komponenten eingesetzt, Fehlfunktionen erzeugt z. B. durch bösartige Programme, in das Zielsystem eingedrungen, z. B. durch Software-Manipulationen und das IT-System missbraucht durch z. B. gefälschte Identitäten (Spoofing). Schwachstellen und fehlende oder unzureichende Sicherheitsmechanismen sowie die Manipulation menschlichen Verhaltens ermöglichen diese Angriffe.

In **Phase 3 „Ausweitung der Rechte“** geht es darum, die Rechte des Angreifers im System zu erhöhen. Dies ermöglicht ihm, die Kontrolle über zusätzliche Server und Endpunkte zu übernehmen, welche näher am eigentlichen Angriffsziel liegen. In modernen Organisationen mit vernetzten Konten kann diese Technik die Kontrolle über Systemadministrationskonten beinhalten, die die Berechtigung haben, sich an einer großen Anzahl von Computern in der Organisation anzumelden. Die Erweiterung der Rechte kann in verschiedenen Phasen erfolgen oder vorbereitet werden, z. B. bei der Herstellung, Lieferung der Hardware oder im Betrieb durch Keylogger.

Phase 4 „Zielerreichung“ ist das Ergebnis der vorangegangenen Phasen. Dabei hat der Angreifer durch den Zugriff auf die Infrastruktur und durch den Zugriff auf Anwendungen, IT-Systeme und/oder Netzwerke Verfügbarkeits-, Integritäts- und/oder

Vertraulichkeitsverluste erlitten. Insbesondere in Organisationen, die in verschiedenen Informationsräumen arbeiten, bedeutet dies, dass sensible Informationen ihre Integrität und/oder Vertraulichkeit verlieren und der Organisation schweren Schaden zufügen.

Phase 5 „Nachbereitung“ beschreibt eine Phase, welche als optional betrachtet werden kann. Nachdem die Phase 4 abgeschlossen ist, wurden die „Kronjuwelen“ bereits gestohlen und die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit verletzt. Der Angreifer wird nun seinen Angriff nachbereiten und Beweismittel entfernen. Das ultimative Ziel eines Verteidigers ist es jedoch, für Aufklärungszwecke diese letzte Phase nicht geschehen zu lassen. Sie folgt den anderen Phasen und beinhaltet die Schritte, die ein Angreifer unternimmt, um seine Spuren zu verwischen. Eine Möglichkeit besteht darin, Protokolldateien zu löschen, welche Beweise für seine Handlungen darstellen.

Die Klassifizierung von Bedrohungen unter Berücksichtigung der Organisation und der Angreiferperspektive ist ein neues strategiebasiertes Modell, das die organisatorischen Aspekte aller Organisationen, einschließlich staatlicher und militärischer, mit Angreiferstrategien kombiniert. Insbesondere berücksichtigt das Modell das Konzept der Informationsräume. Dieser ganzheitliche Ansatz ist in den bestehenden Modellen noch nicht dargestellt. Es hilft den Organisationen, den Verlauf eines Angriffs für einzelne Teilbereiche der Organisation (Teilziele eines Angreifers) zu beschreiben. Dies ermöglicht ein besseres Verständnis der Ziele eines Angreifers und ermöglicht es, geeignete Sicherheitsmaßnahmen zur Reduzierung der Risiken abzuleiten. Das Modell berücksichtigt alle Teile einer Organisation und alle Phasen eines Angriffs und deckt Sicherheitsrisiken ab, welche die Systeme gefährden können. Fortgeschrittene, andauernde Bedrohungen (Advanced-Persistent-Threats) finden ebenfalls Berücksichtigung, da diese Angriffe in Teilschritte (Phasen eines Angriffs) zerlegt werden können und sich somit im Bedrohungsmodell wiederfinden. Das Modell funktioniert unabhängig von der Art des Angreifers (interner bzw. externer Täter) und seiner Motivation (bösartig bzw. nicht bösartig), denn für den verursachten Schaden ist das zunächst irrelevant.

4.3. Anwendung

Um zu zeigen, dass dieser Vorschlag in einem organisatorischen Szenario umgesetzt werden kann, wurden die im Abschnitt 3.2 dargestellten Ergebnisse berücksichtigt, erweitert und auf dem Gebiet einer militärischen Organisation unter Berücksichtigung der Methodik aus Abschnitt 4.1 verwendet. Wie im Abschnitt 3.1 dargestellt lag der Fokus auf den IT-Sicherheitszielen Integrität und Vertraulichkeit. Die Analyse betrachtete alle sechs Teilziele („Infrastruktur“, „IT-System“, „Netze“, „Anwendungen“, „Menschen“, „Informationsräume“) sowie die Phasen 1-4 („Informationsgewinnung“, „Angriff auf das Ziel“, „Ausweitung der Rechte“, „Zielerreichung“) der Angreiferstrategien. Die Nachbereitung der Phase 5 eines Angriffs stand nicht im Fokus der Untersuchung.

Die Sortierung der Bedrohungen wurde anhand der Beschreibungen der gefundenen Bedrohungen nach Teilzielen und Phasen eines Angriffs durchgeführt. So entstanden disjunkte Teilmengen. In den Teilzielen IT-System, Anwendungen und Netze wurden die allgemeinen Bedrohungen, welche alle Bestandteile der Teilziele betreffen, nach den

Phasen eines Angriffs kategorisiert. Zusätzliche, spezielle Bedrohungen für einzelne Bestandteile, wie z. B. Betriebssysteme (Teilziel Anwendungen), Protokolle (Teilziel Netze) oder Mobile Endgeräte (Teilziel IT-System), wurden gesondert ausgewiesen. Dies führte zu einer besseren Darstellung der Bedrohungen für die spätere Priorisierung des Handlungsbedarfs. Insgesamt wurden 608 Bedrohungen durch den Autor identifiziert (25 im Bereich Infrastruktur, 82 im Bereich IT-System, 67 Netzwerkbedrohungen, 310 Anwendungsbedrohungen, 105 im Bereich Menschen, 19 Informationsraumbedrohungen). Ein Überblick der Untersuchung ist in Tabelle 4.1 dargestellt. In der ersten Reihe befinden sich die Teile der Organisation, also Infrastruktur, IT-System, Netze, Anwendungen, Menschen und Informationsräume. In den Reihen 2 bis 5 sind die Phasen eines Angriffs dargestellt (Informationsgewinnung, Angriff auf das Ziel, Ausweitung der Rechte, Zielerreichung). In Zeile 6 steht die Gesamtzahl der Bedrohungen für jeden einzelnen Teilbereich der Organisation und in der letzten Zeile sind die Quellen aufgeführt, aus denen die Bedrohungen erfasst wurden. Im Folgenden wird nun auf jeden Teilbereich der Organisation eingegangen. Hierbei werden die einzelnen Phasen eines Angriffs mit Beispielen aus der Untersuchung erläutert, um eine Vorstellung zu erhalten, welche Bedrohungen existieren.

4.3.1. Infrastruktur

Für den Bereich der Infrastruktur konnten insgesamt 25 Bedrohungen identifiziert werden. Das Sammeln von Informationen kann z. B. durch die Aufzeichnung der unkontrollierten Ausbreitung von Funkwellen in Räumen oder Gebäuden erreicht werden [16]. Ebenfalls ist die Ausstrahlung der Verkabelung eine Bedrohung [110]. In Phase 2 kann der „Angriff auf das Ziel“ über die Energieversorgung/Klimatisierung [66,83], die Räume und Gebäude [5, 16, 66, 120] oder die Verkabelung [13, 16, 66, 84, 110] erfolgen. Beispiele für Angriffe sind Seitenkanalangriffe, unbefugtes Eindringen in Räumlichkeiten, Abhören von Leitungen, unzulässige Kabelverbindungen, Datenlogger an der internen Verkabelung, Übersprechen.

Ein Beispiel für einen Angriff aus Phase 3, welcher die Rechte im Bereich der Infrastruktur erweitern kann, ist ein Keylogger im Kabelkanal. Die Ausweitung der Rechte kann auch über die Anwendungen, IT-Systeme und Netze erfolgen. Phase 4, die Zielerreichung, geschieht über den Zugriff auf Anwendungen, IT-Systeme und Netze.

4.3.2. IT-System

Den Bereich IT-System betreffen 82 Bedrohungen. Die Informationsgewinnung (Phase 1) kann z. B. über Footprinting [5], Schultersurfen [13] oder aber auch den physikalischen Zugriff (Diebstahl) [5, 16, 65, 66, 108, 112, 120] geschehen. Angriffe auf das Ziel (Phase 2) werden z. B. durch Eindringen, Missbrauch und Fehlfunktionen der IT-Systeme verursacht [16, 43, 84, 112]. Weitere Angriffe in dieser Phase differenzieren nach den verwendeten IT-Systemen (z. B. Router, Kryptomodule, mobile Endgeräte, Server) [16, 43, 66, 94, 112, 120]. Beispiele dafür sind der unberechtigte Zugang zu aktiven Netzkomponenten, Abhören von Mobilfunktelefonaten oder der einfache Datendiebstahl.

Tabelle 4.1.: Überblick über die Bedrohungen einer Organisation

	Infra-struktur	IT-System	Netze	Anwen-dungen	Men-schen	Informa-tions-räume
Informationsgewinnung	3	10	5	7	12	2
Angriff auf das Ziel	19	67	59	287	91	13
Ausweitung der Rechte	2	3	1	11	1	2
Zielerreichung	1	2	2	5	1	2
Gesamtzahl	25	82	67	310	105	19
Quellen	[5, 13, 16, 66, 83, 84, 110, 120]	[5, 11, 13, 16, 43, 65, 66, 94, 108, 110, 112, 120]	[5, 11, 13, 16, 43, 56, 65, 70, 81, 83, 94, 108, 110, 112, 120]	[1, 5, 11, 13, 16, 35, 37, 43, 56, 65, 66, 70, 81, 83, 94, 108, 110, 112, 120, 133, 136, 153]	[5, 11, 13, 16, 35, 37, 43, 56, 65, 66, 81, 83, 94, 99, 108, 110, 112, 136]	[6, 16, 43, 84, 112]

Durch Manipulation der IT-Systeme z. B. während der Herstellung oder der Auslieferung kann die Phase 3 „Ausweitung der Rechte“ erreicht werden [5, 16, 43]. Das Ziel (Phase 4) in diesem Bereich ist erreicht, wenn es zu Integritätsverlusten (Tampering) und Vertraulichkeitsverlusten bei IT-Systemen kommt [16, 133].

4.3.3. Netze

Für den Bereich des Netzwerks konnten 67 Bedrohungen ermittelt werden. Hierbei gewinnt der Angreifer Informationen (Phase 1) durch Analyse des Nachrichtenflusses, durch Nutzung von Netzanalysetools oder auch durch Sniffing sowie Traffic Injection [5,16,56,65,108,110,112]. Angriffe auf die Netze (Phase 2) erfolgen über die genutzten Protokolle und Schwachstellen in den Netzwerken [5, 16, 56, 70, 81, 83, 94, 110, 112, 120] z. B. durch Spoofing, Hijacking. Durch Nutzung interner Netzverbindungen für laterale Bewegungen [43] können in der Phase 3 die Rechte ausgeweitet werden. Durch diese verschiedenen Schritte kommt es zu Vertraulichkeits- und Integritätsverlusten der Netze (Phase 4) [16, 133].

4.3.4. Anwendungen

Der komplexeste Bereich für Bedrohungen ist der Bereich der Anwendungen. Hier wurden 310 Bedrohungen identifiziert. Die Informationsgewinnung (Phase 1) geschieht durch Reverse Engineering [5,16,108] oder durch Ausspähen von Information, wie z. B. Finger- oder Footprinting [5, 108, 153]. Angriffe im Bereich der Anwendungen (Phase 2) können auf der Betriebssystemebene oder bei der Anwendungssoftware und Diensten auftreten [5, 16, 37, 43, 56, 81, 94, 108, 110, 112, 136, 153]. Konkrete Bedrohungen in diesem Bereich sind:

- Authentisierungsangriffe [5, 13, 16, 43, 65, 81, 83, 108, 110, 112, 120, 153],
- Einspielen/Wiedereinspielen von Nachrichten [16, 70, 83, 110],
- Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen [16],
- Hijacking (z. B. Browser Hijacking) [43, 70, 81, 83, 110, 112, 120],
- Kryptographieangriffe [16, 43, 70, 83, 112],
- Manipulation von Software [5, 16, 153],
- Repudiation [133],
- Schadsoftware [1, 11, 13, 16, 35, 43, 56, 65, 66, 81, 83, 94, 110, 112, 120],
- Spoofing/Identitätsdiebstahl [5, 16, 35, 43, 65, 70, 81, 112, 120, 133, 153],
- Software-Schwachstellen oder -Fehler [5, 16, 37, 56, 70, 83, 110, 112, 153].

Die Ausweitung der Rechte (Phase 3) erfolgt durch Missbrauch von Administrator- und Benutzerrechten [16, 43, 65, 83, 108, 133, 136] oder aber auch durch Fernzugriff [16, 35, 66, 94, 108, 136]. Diese Angriffe verursachen in Phase 4 Integritäts- und Vertraulichkeitsverluste in den Anwendungen. Hierbei liegt die höchste Gefahr, da es dadurch zu Verlusten/Manipulationen schützenswerter Informationen kommt [16, 43, 133, 136].

4.3.5. Menschen

Der Bereich Menschen umfasst 105 Bedrohungen. Die Informationsgewinnung (Phase 1) erfolgt über das Auspähen von Informationen [16, 66, 112] oder durch Social Engineering [5, 16, 99, 108]. Bei dieser Art des Social Engineerings geht es um die einfache Informationserhebung, der Sorglosigkeit im Umgang mit Informationen und der Weitergabe falscher oder interner Informationen. Angriffe auf das Ziel (Phase 2) erfolgen entweder durch Fehler/Unterlassung/Mangelnde Erfahrung in der Administration und Konfiguration [16, 37, 43, 56, 66, 94, 112, 136] bzw. Fehler und Unterlassung in der Nutzung durch Fahrlässigkeit oder Vorsatz [16, 66, 112] sowie durch Social Engineering [5, 13, 16, 35, 56, 65, 81, 83, 99, 108, 110, 112], wie zum Beispiel:

- Baiting,
- Drive-by-Pharming,
- Fehlende oder unzureichende Identifizierung zwischen Gesprächsteilnehmern,
- Manipulation menschlichen Verhaltens (z. B. durch Familienangehörige oder Besucher),
- Nötigung, Erpressung oder Korruption,
- Pharming,
- Phishing,
- Reverse Social Engineering,
- Spear Phishing,
- SPIT und Vishing,
- Sorglosigkeit im Umgang mit Informationen und
- Tailgaiting.

Die Ausweitung der Rechte (Phase 3) erfolgt nach erfolgreicher Manipulation des Menschen über die Anwendungen, IT-Systeme und Netze. Das Ziel in Phase 4 ist der Zugang, Zutritt, Zugriff zu Infrastruktur, Anwendungen, IT-Systemen und Netzen.

4.3.6. Informationsräume

Insgesamt wurden 19 Bedrohungen im Teilziel Informationsräume identifiziert. Die Phase 1 Informationsgewinnung erfolgt nach Zugriff auf Infrastruktur, Anwendungen, IT-Systemen und Netzen. Hierzu gehören zum Beispiel die Identifizierung wichtiger operationeller Knoten oder die Identifizierung von Geheimhaltungsgraden. Durch die Identifizierung kann der Angreifer Schwerpunkte für Folgeangriffe setzen. Je höher ein Geheimhaltungsgrad, desto interessanter ist die Information, die sich dahinter verbirgt. Je wichtiger ein operationeller Knoten, desto mehr Informationen verarbeitet dieser.

In der Phase 2 Angriffe auf das Ziel konnten Bedrohungen, wie der Informationsfluss von oben (z. B. GEHEIM) nach unten (z. B. Öffentlich) [6] oder das Abgreifen von Informationen, wenn sie unverschlüsselt sind [43], identifiziert werden. Dahinter steckt die Absicht des Angreifers, illegale Datenflüsse zu erzeugen, um an vertrauliche oder geheime Informationen zu gelangen. Weitere selbst ermittelte Bedrohungen sind die fehlende Kontrolle der Geheimhaltungsgrade, das unbefugte Eindringen in Informationsräume oder die Überwindung der physikalischen Grenzen zwischen Informationsräumen.

Die Ausweitung der Rechte (Phase 3) kann durch Manipulation der Geheimhaltungsgrade oder durch die Änderung der Höhe der Sicherheitsüberprüfung des Personals erfolgen. Im ersten Fall kann der Angreifer durch Herabstufen von Geheimhaltungsgraden in Dokumenten die Verbreitung dieser Dokumente ermöglichen. Wird zum Beispiel ein geheimes Dokument auf den Geheimhaltungsgrad „Öffentlich“ gesetzt, dann kann dieses Dokument in den öffentlichen Informationsraum (ins Internet) entweichen (neudeutsch: „geleakt“ werden). Im zweiten Fall können Personen durch Änderung der Höhe der Sicherheitsüberprüfung Zugang zu sensibleren Informationen erhalten, zu denen sie eigentlich gar keinen Zugriff erhalten sollten.

Das Ziel im Bereich Informationsräume (Phase 4) ist erreicht, wenn:

- Integritätsverluste, z. B. Fehlinformationen, als authentisch wahrgenommen werden, oder
- Vertraulichkeitsverluste, z. B. der Abfluss von elektronisch gespeicherten Dokumenten aus höheren Geheimhaltungsgraden und Informationsräumen,

auftreten.

Die Bedrohungen des Teilziels Informationsräume sind in der Literatur nicht gut beschrieben. Daher wurden einige Bedrohungen hinzugefügt, die selbst ermittelt wurden. Diese wurden hier bereits vorgestellt und werden in Abbildung 4.2 und 4.3) dargestellt.

4.4. Zusammenfassung

In diesem Kapitel wurde ein neu entwickeltes Bedrohungsmodell für militärische Organisationen und Regierungsorganisationen im Überblick dargestellt. Das vollständige Modell befindet sich im Anhang A. Das Modell ist durch Verwendungen von Teilbereichen (wie z. B. Anwendungen oder IT-System) auch für andere Organisationen verwendbar. Damit ist es an verschiedene Organisationen anpassbar und kann benutzt werden, um

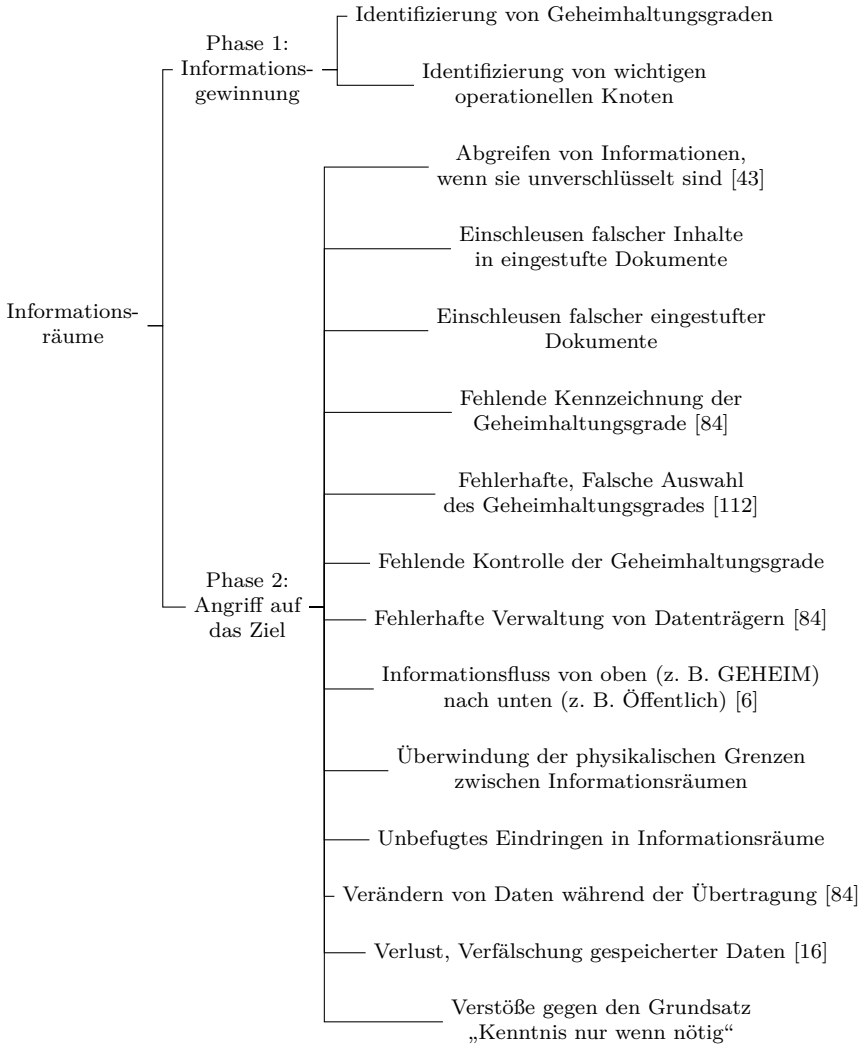

Abbildung 4.2.: Bedrohungen der Informationsräume in Phase 1 und 2

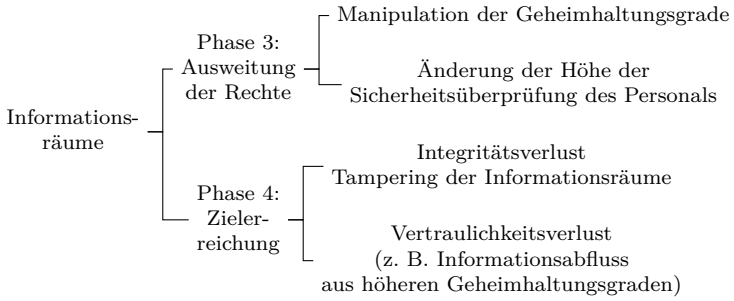

Abbildung 4.3.: Bedrohungen der Informationsräume in Phase 3 und 4

Einblicke in das Untersuchungsgebiet zu gewinnen. Es ermöglicht, Strategien zur Risikominderung für einzelne Teilbereiche eines Unternehmens zu entwickeln. Das Modell enthält alle Teilbereiche einer Organisation und alle Phasen eines Angriffs sowie Klassifizierungskriterien, die definieren, welche Bedrohungen in jeder Kategorie platziert werden sollten. In den folgenden Kapiteln werden diese identifizierten Bedrohungen mit Bezug auf die Forschungsfragen aus Abschnitt 2.7 aufgegriffen.

5. Sichere Informationsflüsse - Datenflussanalyse mit operationellen Netzknotenstrukturen

In diesem Kapitel wird sich mit der Frage beschäftigt, welche operationellen Netzknoten in einem IT-System wichtig sind und wie man diese identifizieren kann. Dabei wird auch auf die Frage eingegangen, wie Geheimhaltungsgrade in einem IT-System, beispielsweise bei staatlichen oder militärischen Organisationen, bei der Analyse explizit berücksichtigt werden können. Diese Art der Bedrohungen geschehen in der Angriffsphase Informationsgewinnung (vgl. Abschnitt 4.2.2).

Nachfolgend wird dafür ein neuer Sicherheitsansatz vorgestellt, welcher dabei hilft, Bedrohungen zwischen unterschiedlichen und innerhalb der gleichen Informationsräume auf gültigen Datenflusswegen zu identifizieren. Gültige Datenflüsse sind erlaubte Informationsflüsse, welche innerhalb der Organisation genutzt werden. Der folgende Ansatz kann verwendet werden, um Sicherheitsherausforderungen innerhalb von Organisationen darzustellen, die geheime Informationen verwenden, wie z. B. Regierungs- oder Militärorganisationen. Mit diesem Sicherheitsansatz werden auch neue Attribute für Datenflüsse in angeschlossenen Systemen oder Prozessen eingeführt. Dieses Sicherheitsdatenflussdiagramm wird dann verwendet, um eine Analyse durchzuführen, die operationelle Netzknotenstrukturen in der Designphase identifiziert, welche am stärksten von der Gefahr des Verlustes der Vertraulichkeit, Verfügbarkeit und Integrität ihrer klassifizierten Informationen beim Datenaustausch zwischen Netzwerken mit unterschiedlichen Geheimhaltungsgraden betroffen sind.

5.1. Informations- und Datenflussmodelle

Es existieren viele Veröffentlichung im Bereich von Informationsflüssen und Informationsflussmodellen. D.E. Bell und J. LaPadula führten ein Sicherheitsmodell für Computersysteme ein, das die Vertraulichkeit von Informationen durch ein System von erzwungenen Regeln schützt. Informationen eines höheren Schutzniveaus können weder gelesen noch auf ein niedrigeres Schutzniveau übertragen werden [6]. Kenneth J. Biba hat ein Sicherheitsmodell entwickelt, welches sich mit der Integrität von Daten befasst und den Lese- und Schreibzugriff in einem Computersystem [7] überprüft. D.E. Denning untersuchte Mechanismen, die einen sicheren Informationsfluss in einem Computersystem gewährleisten [40]. Sie schlug ein Gittermodell (lattice model) für einen sicheren Informationsfluss vor. Dessen Struktur entwickelt sich aus verschiedenen Geheimhaltungsgraden und wird durch die Semantik eines Informationsflusses validiert. Basierend auf diesem Mo-

dell demonstrierten D.E. Denning und P.J. Denning einen Zertifizierungsmechanismus zur statischen Überprüfung des sicheren Informationsflusses in einem Programm [41].

A.C. Myers und B. Liskov führten ein Modell zur Steuerung des Informationsflusses in Systemen mit gegenseitigem Misstrauen und dezentraler Autorität ein. In diesem Modell ist es möglich, Informationen mit nicht vertrauenswürdigem Code auszutauschen und darüber hinaus zu entscheiden, an wen die Informationen weitergegeben wird [100]. J. Rushby schlug vor, dass sichere Systeme als verteilte Systeme konzipiert werden sollten, bei denen die Sicherheit zum Teil durch die physische Trennung ihrer einzelnen Komponenten und zum Teil durch die Vermittlung von vertrauenswürdigen Funktionen innerhalb einiger dieser Komponenten erreicht wird [118]. W.S. Harrison, et al. stellten eine gemeinsame Forschungsarbeit zwischen Wissenschaft, Industrie und Regierung vor, die Multiple Independent Levels of Security and Safety (MILS) genannt wird. Das Ergebnis war die Entwicklung und Implementierung einer hochsicheren Echtzeitarchitektur für eingebettete Systeme. Das Ziel der MILS-Architektur ist es, sicherzustellen, dass alle Systemsicherheitsrichtlinien nicht umgangen werden, auswertbar, immer aufgerufen und manipulationssicher sind [67].

Alle diese Veröffentlichungen und Ansätze bilden eine Grundlage für Methoden und Modellen für sichere Systeme und deren Informationsflüsse. Sichere Informationsflüsse gewährleisten, dass sensible Informationen während der Programmausführung nicht an unbefugte Personen weitergegeben werden. In den gängigen Publikationen [6], [7], [40], [100], [118], [67] wird weniger das Problem fokussiert, dass die Implementierung oder Nutzung eines sicheren Systems - aufgrund von Implementierungsfehlern oder verschiedenen Angriffsvektoren, wie z. B. Social Engineering - überhaupt nicht sicher ist. Somit sind Sicherheitsbedrohungen oder -schwachstellen, bei denen illegale und unerwünschte Operationen über gültige Informationspfade und über Netzwerkgrenzen hinweg durchgeführt werden, in den etablierten Methoden kaum berücksichtigt. Im Folgenden wird daher ein Ansatz entwickelt, der genau auf diese Idee der „eigentlich“ gültigen Datenflüsse aufbaut.

5.2. Informations- und Datenflussanalyse

Datenflussdiagramme oder ähnliche Techniken zur Darstellung des Informationsflusses in Systemen, wie z. B. Flussdiagramme, werden seit den 70er Jahren in der Literatur definiert [58], [39], [159].

Swiderski et al. [133] stellen die Verwendung von Datenflussdiagrammen (DFD) innerhalb der Bedrohungsmodellierungsmethode von Microsoft dar, die Teil des Security Development Lifecycle (SDL) ist. A. Shostack beschrieb in einer Veröffentlichung ein Jahrzehnt Erfahrung mit der Modellierung von Bedrohungen bei Microsoft. Er stellte fest, dass DFD sehr datenzentriert sind und die Analyse sich auf „das Richtige“ konzentriert [126]. K. Schmidt et al. stellen einen Sicherheitsanalyseansatz vor, welcher behilflich ist, Sicherheitsprobleme in einer Automobilarchitektur zu identifizieren und zu priorisieren. Dieser Ansatz verwendet ebenso Datenflussdiagramme für eine strukturierte Bedrohungsanalyse und Risikobewertung in einem sicherheitsorientierten Entwicklungs-

prozess [123]. K. Schmidt, et al. verwenden Kommunikationszonen, in denen Entitäten aufgrund einer gemeinsamen Kommunikationsschicht direkt miteinander kommunizieren können.

In dem nun folgenden neuen Ansatz ist das Modell der Datenflüsse mit Sicherheitsattributen verbunden. Anstelle von Kommunikationszonen werden Informationsräume verwendet. Mit Hinblick auf die Ausführungen in Kapitel 2 wird davon ausgegangen, dass Informationsräume physisch voneinander getrennt sind und eine direkte Kommunikation ist nicht möglich.

5.3. Definition Sicherheitsdatenflussdiagramm (DFDsec)

Ein Datenflussdiagramm enthält Prozesse, Datenspeicher, externe Entitäten und Datenflüsse [133]. Im hier definierten DFDsec-Ansatz werden den Datenflüssen Geheimhaltungsgrade als Sicherheitsattribute hinzugefügt. Darüber hinaus werden jene Geheimhaltungsgrade verwendet, um die Informationsräume um die ursprünglichen Datenflussdiagrammelemente herum zu erstellen. Dies ist vergleichbar mit den Arbeiten von Microsoft und Schmidt et al., die zuvor diskutiert wurden. Die Grenzen der Informationsräume sind vorhanden, da eben eine direkte physische Verbindung aus Sicherheitsgründen nicht erlaubt ist. Innerhalb oder zwischen den Informationsräumen werden Sicherheitsprinzipien und Schutzmaßnahmen angewandt, die verhindern sollen, dass eingestufte Informationen und Daten die Vertraulichkeit, Verfügbarkeit und Integrität verlieren.

Die folgenden vier Fälle beschreiben alle möglichen Informationsflüsse in einem Sicherheitsdatenflussdiagramm (DFDsec), welche im Bereich der Regierungs- und Vollzugsbehörden auftreten können:

- Daten werden innerhalb desselben Informationsraumes gesendet (z. B. vertrauliche Informationen - technisches Know-how) - erlaubter Informationsfluss
- Daten werden von einer niedrigeren zu einer höheren Informationsraum gesendet (z. B. persönliche identifizierbare oder gesundheitsbezogene Informationen) - verbotener Rückfluss von Informationen.
- Daten werden aus einer höheren oder niedrigeren Informationsraum (z. B. Abflug- oder Zielort) gesendet - freigegebener Informationsrückfluss.
- Es werden keine Daten aus einer höheren Klassifizierung in ein öffentliches Netz (z. B. Staatsgeheimnisse) gesendet - verbotener Informationsfluss

Ein Sicherheitsdatenflussdiagramm wird definiert durch

Definition 1. $DFDsec =< P_{(n)}, E_{(n)}, S_{(n)}, F_{I(z)}, I_{(z)} >$

wo:

- Prozesse $P_{(n)}$ von 1..n stellen normalerweise in einem Standard-Datenflussdiagramm eine Aufgabe im System dar, die Daten verarbeitet

oder eine Aktion basierend auf Daten ausführt. In diesem Modell werden sie mit Entitäten verknüpft, welche Aktivitäten durchführen, indem sie eingehende Daten verarbeiten und möglicherweise Output erzeugen (z. B. operationelle Netzknoten, die vertrauliche Informationen erzeugen). Der Grund für diese Verknüpfung ist lediglich die Identifizierung des Verursachers der Aktivität. Dies ist für eine spätere Risikobewertung notwendig. Prozesse werden durch kreisförmige Formen in den Abbildungen dargestellt.

- Externe Entitäten $E_{(n)}$ von 1..n sind Akteure außerhalb des geprüften Systems, von denen das System abhängt. Sie können die Quelle oder das Ziel von Informationen sein. Sie können Teil eines anderen oder sogar ein eigener Informationsraum sein. Externe Entitäten $E_{(n)}$ können nicht verwendet werden, wenn noch funktionale Anforderungen definiert werden. In diesem Stadium der Entwicklung ist das zukünftige System überhaupt noch nicht definiert. Daher ist es nicht möglich zu bestimmen, welcher der Prozesse $P_{(n)}$ innerhalb oder außerhalb eines Systems fungiert. Rechteckige Formen stellen dabei externe Entitäten in den Abbildungen dar.

- Datenspeicher $S_{(n)}$ von 1..n sind physische oder logische Speicher zum Speichern oder Abrufen von Daten (z. B. Benutzer, Datenbanken, Dateisystem). Datenspeicher S(n) können nicht verwendet werden, wenn noch funktionale Anforderungen definiert werden, da zu diesem Zeitpunkt das zukünftige System noch gar nicht definiert ist. Deshalb ist auch noch nicht klar, welches physische oder logische Repository für das zukünftige Projekt verwendet wird. Datenspeicher werden durch offene, rechteckige Formen in den Abbildungen dargestellt.

- Datenflüsse $F_{I(z)}$ werden definiert durch

  Definition 2. $F_{I(z)} =< A, FB, RB, 0 >$

  Es gibt Informationsflüsse zwischen Prozessen, externen Entitäten, Datenspeichern und Informationsräumen. Je nach Einsatzsituation können sie entweder erlaubte Informationsflüsse (A), verbotene Rückflüsse von Informationen (FB), freigegebene Informationsrückflüsse (RB) und verbotene Informationsflüsse (0) sein. Diese spezifische Attribute werden den Datenflüssen hinzugefügt. Datenflüsse werden durch Pfeile dargestellt, welche in Richtung des Flusses zeigen. Sie werden farblich oder durch ihre Struktur hervorgehoben. Datenflüsse $F_{I(z)}$, die innerhalb eines und desgleichen Informationsraums I(x) fließen, sind erlaubt, wenn $z \leq x$.

- Informationsräume I(z) sind die spezifischen Geheimhaltungsgrade, die Prozesse, Datenspeicher, Datenflüsse und zugehörige externe Entitäten umfassen, wobei I eine Reihe formaler Kategorien ist (z. B. „Nuclear“, „NATO“, „EU“, „DEU“ und „Crypto“) und (z) eine Reihe von Klassifizierungen oder Freigaben ist (z. B. „OFFEN“, „NUR-FÜR-DEN-DIENSTGEBRAUCH“, „VERTRAULICH“, „GEHEIM“ und „STRENG GEHEIM“). Um zwischen zwei Informationsräumen zu unterscheiden, wird I(x) und I(y) verwendet. Dabei sind x und y $\in$ Z. Informationsräume

werden durch Kreise dargestellt, die alle Elemente eines Informationsraumes in den Abbildungen umgeben.

Abbildung 5.1 stellt eine Situation dar, in der Daten innerhalb desselben Informationsraums gesendet werden. Ein Informationsaustausch ist innerhalb eines Bereichs öffentlicher oder offener Informationen möglich, sowie dort, wo das Prinzip „Kenntnis-nur-wenn-nötig“ (Need-to-know) angewendet wird [1]. Es gibt keine weiteren Einschränkungen innerhalb desselben Informationsraums. Dies sind zulässige Datenflüsse. Zulässige Datenflüsse $F_{I(z)}$ fließen vom Informationsraum I(x) zum Informationsraum I(y), während x ∈ Z, y = x und z = Klassifizierung.

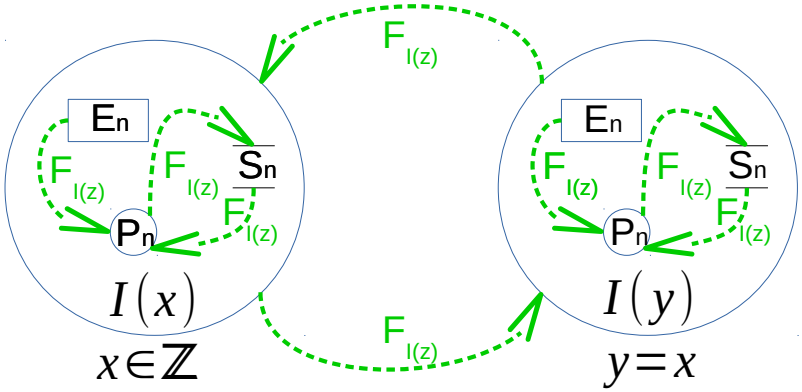

Abbildung 5.1.: Erlaubter Informationsfluss

Abbildung 5.2 zeigt die zweite Situation, in der Datenflüsse nur in eine Richtung zulässig sind. Ein Informationsrückfluss ist in diesem Fall verboten. Erlaubte Datenflüsse $F_{I(z)}$ in eine Richtung sind Ströme aus dem Informationsraum I(x), wobei x ∈ Z und z = Klassifizierung und z ≤ x, in einen höheren Informationsraum I(y), wobei y > x. Ein Hochsicherheitsgateway, wie z. B. eine Datendiode realisiert eine solche Verbindung [62]. Sie sind mit $F_{I(z)}$ gekennzeichnet.

Abbildung 5.3 veranschaulicht die dritte Situation, in welcher der Datenaustausch zwischen verschiedenen Informationsräumen nur möglich ist, wenn der Informationsrückfluss freigegeben wird. Der Datenfluss verläuft von einem höheren Geheimhaltungsgrad zu einem niedrigeren, aber nicht niedriger als OFFEN. Erlaubte Datenflüsse $F_{I(z)}$ mit freigegebenem Rückfluss sind Ströme vom Informationsraum I(x) zum Informationsraum I(y), wobei x ∈ Z, 0 ≤ y < x und z = Klassifizierung und z ≤ y. Ein Hochsicherheits-Gateway wie ein rot-schwarzes Gateway, das eine präzise Inhaltsüberwachung und Steuerung von Datenflüssen zwischen Netzwerken mit unterschiedlichen Geheimhaltungsgraden ermöglicht, implementiert eine solche Verbindung [75].

[1] Es wird nur innerhalb desselben Geheimhaltungsgrades und nur dann angewendet, wenn der Geheimhaltungsgrad höher als „VS-NUR-FÜR-DEN-DIENSTGEBRAUCH“ ist.

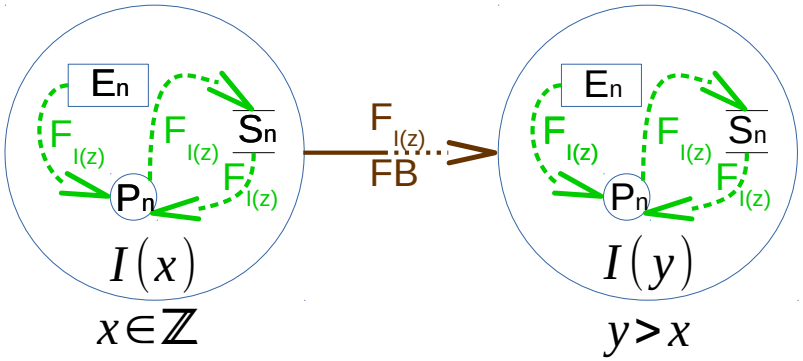

Abbildung 5.2.: Verbotener Rückfluss von Informationen

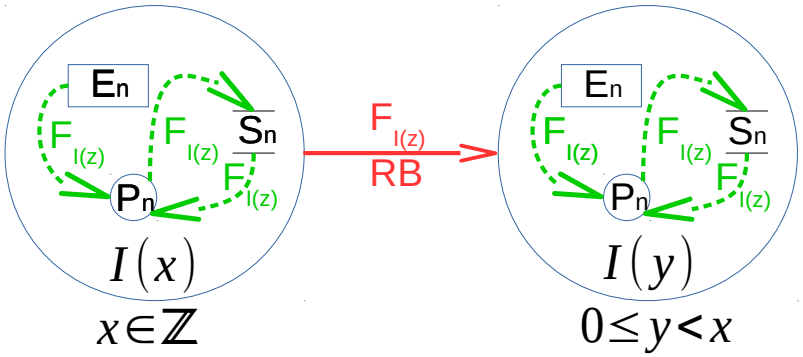

Abbildung 5.3.: Freigegebener Informationsrückfluss

Abbildung 5.4 zeigt die vierte Situation eines Datenaustauschs. Aber in diesem Fall ist der Datenfluss aus rechtlichen Gründen verboten. Es ist verboten, klassifizierte oder offene Informationen an ein öffentliches Netz zu senden. Verbotene Datenflüsse $F_{I(z)}$ sind Ströme vom Informationsraum I(x) zum Informationsraum I(y), wobei x $\in$ Z, x $>$ y, y $= -1$ (-1 repräsentiert das öffentliche Netz) und z = Klassifizierung und z $>$ y.

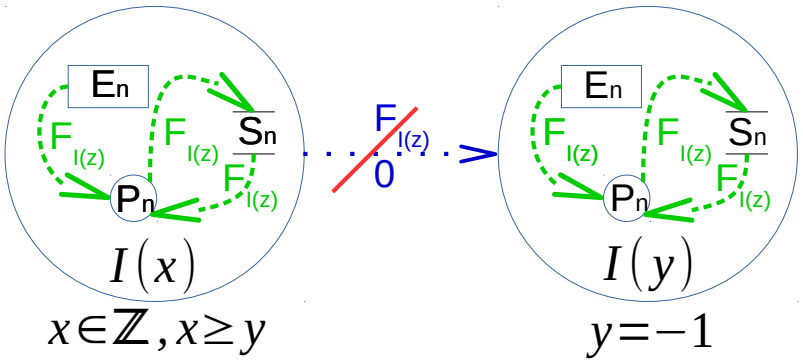

Abbildung 5.4.: Verbotener Informationsfluss

5.4. Analyse eines DFDsec

In diesem Abschnitt wird das DFDsec verwendet, um eine Analyse durchzuführen, die operationelle Netzknotenstrukturen dahingehend identifiziert, welche am stärksten von der Gefahr des Verlustes der Vertraulichkeit, Verfügbarkeit und Integrität ihrer eingestuften Informationen beim Datenaustausch zwischen Netzwerken mit unterschiedlichen Geheimhaltungsgraden betroffen sind. In dieser Analyse werden die drei grundlegenden Ziele der IT-Sicherheit [15]: Vertraulichkeit, Verfügbarkeit und Integrität mit den möglichen Geheimhaltungsgraden kombiniert.

Wie in Kapitel 2 dargestellt, gibt es verschiedene Berichte und Umfragen über Angriffstypen, Angriffsvektoren, Sektoren und Kosten von Verstößen. Aus diesen Berichten kann man schließen, welchen Risiken ein operationeller Netzknoten ausgesetzt ist. Dadurch ist es möglich ein Indexranking abzuleiten und zu definieren:

Definition 3. $INDRank =< P_{(n)}, NoC, EC, IND, Rank, * >$

where:

- P(n) ist der operationelle Netzknoten 1...n
- NoC sind die Anzahl der Verbindungen eines bestimmten Typs (ausgehende, eingehende oder beide).

- EC ist ein Bewertungskriterium in der Form eines Multiplikationsfaktors: Schweregrad (Vertraulichkeit), Angriffspotenzial (Verfügbarkeit) und Änderungsmöglichkeit (Integrität).
- IND ist der Vertraulichkeits-, Verfügbarkeits- oder Integritätsindex.
- Rang = 1..n
- *: EC*NoC = IND

Vertraulichkeit ist eine Eigenschaft, welche für Informationen gilt. Die Vertraulichkeit von Informationen zu schützen und zu wahren, bedeutet, sicherzustellen, dass sie nicht an unbefugte Personen weitergegeben werden [78]. Aus diesem Grund muss der Blick in Bezug auf Vertraulichkeitsverletzungen auf die ausgehenden Datenströme gerichtet werden. Die Verfügbarkeit ist ein Merkmal, das sich auf Werte (Assets) bezieht. Ein Asset ist verfügbar, wenn es für eine autorisierte Stelle zugänglich und bei Bedarf verwendbar ist [78]. Daraus folgt, dass bei der Verletzung der Verfügbarkeit eingehende Datenströme berücksichtigt werden müssen. Die Integrität von Informationen zu wahren, bedeutet, die Genauigkeit und Vollständigkeit von Informationen und die Methoden zu schützen, welche zu ihrer Verarbeitung und Verwaltung verwendet werden [78].

Je höher eine Information klassifiziert ist, desto sensibler ist sie und muss daher geschützt werden (Schweregrad) [115]. Daher ist es einfacher, die Verfügbarkeit anzugreifen (Angriffspotenzial) oder Informationen zu ändern (Änderungsmöglichkeit), wenn der Geheimhaltungsgrad niedriger ist als bei einer höheren Einstufung. Auf der anderen Seite ist eine geheime Information sicherlich interessanter, um manipuliert zu werden. Dies rechtfertigt Bemühungen, um den Zugang zu dieser Information zu verweigern oder sie zu ändern [152]. Daraus folgt, dass sensiblere Informationen stärker gefährdet sein könnten. Aus der Perspektive negativer Auswirkungen auf den Stakeholder wird der Schweregrad wie folgt bewertet (Geheimhaltungsgrad ≡ Multiplikationsfaktor):

- STRENG GEHEIM ≡ 6
- GEHEIM ≡ 5
- VS-VERTRAULICH ≡ 4
- VS-NUR-FÜR-DEN-DIENSTGEBRAUCH ≡ 3
- OFFEN ≡ 2
- Öffentlich ≡ 1

Je niedriger der Geheimhaltungsgrad und dessen Schutz, desto höher ist das Potenzial für einen erfolgreichen Angriff auf die Verfügbarkeit [76]. Alle Verbindungen könnten manipuliert werden, aber es ist einfacher, dass Informationen aus niedrigeren Quellen geändert werden können, da die Sicherheitsanforderungen proportional zum Geheimhaltungsgrad [115] steigen. Das Angriffspotenzial und die Änderungsmöglichkeit werden daher wie folgt bewertet:

- STRENG GEHEIM ≡ 1
- GEHEIM ≡ 2
- VS-VERTRAULICH ≡ 3
- VS-NUR-FÜR-DEN-DIENSTGEBRAUCH ≡ 4
- OFFEN ≡ 5
- Öffentlich ≡ 6

Tabelle 5.1.: Index-Ranking für operationelle Netzknoten

Op. Netzknoten	Anzahl der Verbindungen (NoC)	Bewertungskriterium (EC)	Index (IND)	Rang
P_n	Ausgehend	Schweregrad	Vertraulichkeitsindex	1..n
P_n	Eingehend	Angriffspotential	Verfügbarkeitsindex	1..n
P_n	Ausgehend und Eingehend	Änderungsmöglichkeit	Integritätsindex	1..n

Die Tabelle 5.1 fasst diese drei Indizes zusammen, um operationelle Netzknotenstrukturen zu identifizieren, die durch den Verlust von Vertraulichkeit, Verfügbarkeit und Integrität am meisten gefährdet sind. Die erste Spalte der Tabelle enthält die operationellen Netzknoten P(n), welche die zu analysierenden Elemente sind. Die zweite Spalte listet die Anzahl der Verbindungen (NoC) auf, welche den operationellen Netzknoten verlassen und/oder betreten. Die dritte Spalte enthält die Bewertungskriterien (EC), welche eins von den folgenden drei Kriterien sein können: Schweregrad (Vertraulichkeit), Angriffspotenzial (Verfügbarkeit) und Änderungsmöglichkeit (Integrität). Die vierte Spalte ist das Ergebnis der Spalten zwei und drei und enthält die Indizes für die drei Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität (EC*NoC=IND). Schließlich zeigt die fünfte Spalte das Ranking (den Rang) der operationellen Netzknoten, welche am stärksten gefährdet sind.

Nach der Identifizierung eines Rankings für diese drei Sicherheitsziele ist es nun möglich, diese Rankings der einzelnen operationellen Netzknoten in Abhängigkeit von der Bedeutung der einzelnen Sicherheitsziele zusammenzuführen, um einen Sicherheits-Bedeutungswert (Security importance value - (SIV)) für jeden Netzknoten zu erhalten. Die Gewichtung obliegt dem Fokus des Modellierers und muss von ihm festgelegt werden.

Wichtigkeitsmaße werden häufig dazu genutzt, um kritische Komponenten in modellierten Systemen zu identifizieren. Dies kann bei der Betrachtung von Zuverlässigkeiten von Komponenten durch die Birnbaum-Wichtigkeit geschehen [10].

Hier in diesem Fall wurden die Sicherheitsziele gleich gewichtet und die Gleichung lautet:

$$SIV = W_C * C + W_A * A + W_I * I \tag{5.1}$$

wobei $W_C = W_A = W_I = 0,3\overline{3}$ and C = Vertraulichkeitsranking, A = Verfügbarkeitsranking, I = Integritätsranking. Je niedriger die SIV, desto gefährdeter ist der operationelle Netzknoten. Daher sollten mögliche Sicherheitsmaßnahmen bei diesen Netzknoten zuerst getroffen werden.

5.5. Anwendungsfall in der Designphase

5.5.1. Beschreibung des Anwendungsfalls

Organisationen mit bestimmten operationellen Netzknotenstrukturen, die sich mit eingestuften Daten in verschiedenen Informationsräumen befassen, definieren Informationsaustauschanforderungen, um funktionale Anforderungen zu erhalten, welche ein zukünftiges Kommunikations- und Informationssystem erfüllen muss.

In diesem Abschnitt wird ein generisches Beispiel einer operationellen Netzknotenstruktur aus der Designphase analysiert. Dieses Beispiel wird als DFDsec dargestellt, um die Details des dynamischen Verhaltens aufzuzeigen und die Strukturgrenzen sowie deren entsprechende Geheimhaltungsgrade zu beschreiben. Die durchgeführte Analyse identifiziert diejenigen operationelle Netzknotenpunkte, welche am stärksten von der Gefahr des Verlustes von Vertraulichkeit, Verfügbarkeit und Integrität betroffen sind.

In dem exemplarischen generischen Anwendungsfall 5.5 gibt es vier Elemente der Prozessorganisation. Diese stellen die Prozesse (P) im Datenflussdiagramm dar:

- Ministerium (P1),
- Hauptquartier (P2),
- Führungskommando (P3) sowie das
- Team (P4) und zwei Elemente außerhalb der Prozessorganisation:
- das Internet (P5) und
- ein Angriffsvektor (P6).

Es gibt drei Informationsräume:

- DEU_{-1},
- DEU_1 und
- DEU_3.

Der Informationsraum DEU_{-1} besteht aus allen Prozessen (P1) - Ministerium, (P2) - Hauptquartier, (P3) - Führungskommando, (P4) - Team, (P5) - Internet, (P6) - Angreifer. Der Informationsraum DEU_1 enthält (P1) - Ministerium, (P2) - Hauptquartier, (P3) - Führungskommando, (P4) - Team. Der Informationsraum DEU_3 beinhaltet (P2) - Hauptquartier, (P3) - Führungskommando, (P4) - Team.

Jeder Prozess, der Datenflüsse mit dem Geheimhaltungsgrad DEU_{-1} hat, also öffentlich sind, befindet sich im Informationsraum DEU_{-1}. Jeder Prozess, der Datenflüsse mit dem Geheimhaltungsgrad DEU_1 hat, die DEU VS-NUR-FÜR-DEN-DIENSTGEBRAUCH sind, befindet sich im Informationsraum DEU_1. Jeder Prozess, der Datenflüsse mit dem Geheimhaltungsgrad DEU_3, also DEU GEHEIM, hat, befindet sich im Informationsraum DEU_3.

Das Ministerium erlässt für seine nachgeordneten Dienststellen strategische Richtlinien (F1, F2), die als DEU VS-NUR-FÜR-DEN-DIENSTGEBRAUCH eingestuft sind und daher dem Datenfluss das zusätzliche Attribut DEU_1 verleihen. Diese Einheiten entwickeln Pläne und Konzepte (F3, F4 - klassifiziert als DEU VS-NUR-FÜR-DEN-DIENSTGEBRAUCH) mit Regelungen für ihre untergeordneten Einheiten (z. B. Team). Sie können aber auch technische oder funktionale Konzepte versenden, die Richtlinien für weitere Einheiten sind. Diese Konzepte müssen möglicherweise vom Ministerium genehmigt werden.

Sensible Aufgaben oder Berichte (F5, F6, F7), die während einer Mission gesendet werden, werden als DEU GEHEIM eingestuft und erhalten das zusätzliche Attribut DEU_3. Berichte, die nach einer durchgeführten Mission (F8) gesendet werden, werden in diesem Anwendungsfall als DEU VS-NUR-FÜR-DEN-DIENSTGEBRAUCH klassifiziert und der Datenfluss erhält daher DEU_1 als zusätzliches Sicherheitsattribut.

Während ihrer Arbeit benötigen die verschiedene Einheiten möglicherweise Informationen aus dem öffentlichen Netz (F9, F11, F13, F15). Die angeforderten Informationen sind öffentlich (F10, F12, F14, F16). Datenflüsse erhalten daher das Attribut DEU_{-1}. Der Angreifer stellt das Problem dar. Dieser versucht geheime Informationen zu erhalten und z. B. in der Öffentlichkeit zu verbreiten (F17, F19, F21, F23). Dies kann ein bösartiger Insider oder ein Eindringling von außen sein. Seine Datenflüsse sind ebenfalls öffentlich und erhalten das Attribut DEU_{-1}. Wenn der Angreifer erfolgreich war und er Informationen zurückerhalten sollte, werden diese Informationen mindestens den Geheimhaltungsgrad OFFEN haben (F18, F20, F22, F24). In diesem Beispiel ist es DEU VS-NUR-FÜR-DEN-DIENSTGEBRAUCH. Daher erhält dieser Datenfluss das Attribut DEU_1.

Jeder Prozess hat ein- oder ausgehende Datenflüsse mit einem bestimmten Geheimhaltungsgrad. (P1) - Ministerium verfügt über vier eingehende und vier ausgehende Datenflüsse. Fünf von ihnen haben den Geheimhaltungsgrad DEU_1 und drei von ihnen den Klassifizierung DEU_{-1}. Daraus folgt, dass (P1) - Ministerium dem Informationsraum DEU_1 und dem Informationsraum DEU_{-1} hinzugefügt wurde. (P2) - Das Hauptquartier verfügt über drei eingehende und vier ausgehende Datenflüsse. Diese Datenflüsse haben drei verschiedene Geheimhaltungsgrade und daher wurde (P2) - Hauptquartier zu drei Informationsräumen DEU_{-1}, DEU_1 und DEU_3 hinzugefügt. (P3) - Führungskommando verfügt über fünf eingehende und vier ausgehende Datenflüsse. Diese haben

ebenfalls die drei verschiedenen Geheimhaltungsgrade DEU_{-1}, DEU_1 und DEU_3. (P3) - Führungskommando wurde zu drei Informationsräumen hinzugefügt. (P4) - Das Team hat vier ein- und vier ausgehende Datenflüsse mit den Geheimhaltungsgraden DEU_{-1}, DEU_1 und DEU_3 und wurde daher zu drei Informationsräumen hinzugefügt. In Abbildung 5.5 wird die Anzahl der Verbindungen auf die Verbindungen beschränkt, die sich zwischen den Informationsräumen befinden. Die Informationsflüsse innerhalb eines Informationsraumes wurden weggelassen. Das sind diejenigen, welche vom Informationsraum I(x) zum Informationsraum I(y) fließen, während x ∈ Z, y = x und z = Klassifizierung ist. In diesem Beispiel sind es die Datenflüsse mit dem Attribut DEU_3 (F5, F6, F7).

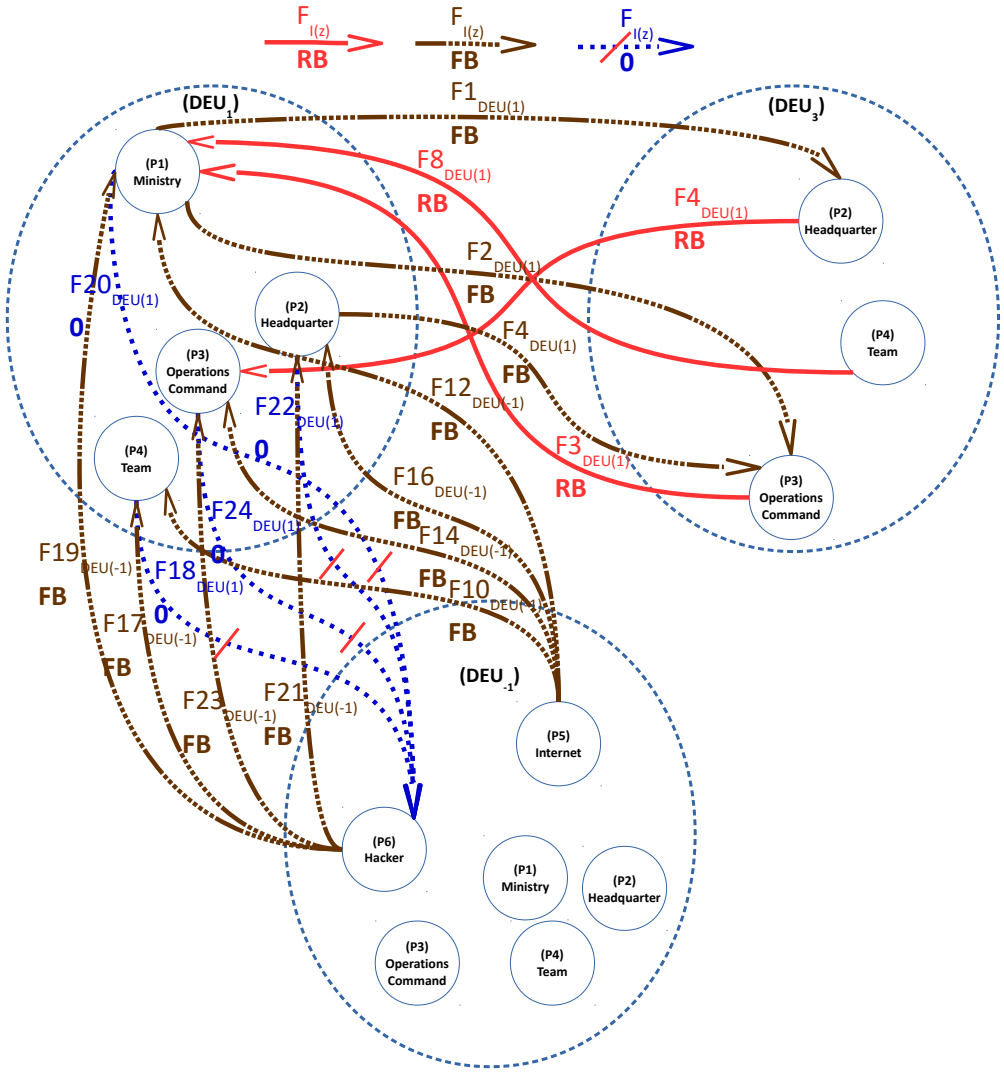

Abbildung 5.5.: DFDsec in der Designphase

Der Informationsfluss zwischen den Informationsräumen muss aufgrund von Sicherheitsvorschriften und des beschriebenen Problems (siehe Abschnitt 2.5), dass Verschlusssachen durch den Verlust von Vertraulichkeit, Verfügbarkeit und Integrität gefährdet sind, genauer betrachtet werden, insbesondere beim Austausch zwischen Netzwerken mit unterschiedlichen Geheimhaltungsgraden. Deshalb wurden sie in verschiedenen Farben hervorgehoben (braun, rot, blau mit roter Kreuzung):

- Daten fließen $F_I(z)$ vom Informationsraum I(x), wobei x ∈ Z und z = Klassifizierung und z ≤ x, in einen höherwertige Informationsraum I(y), wobei y > x braun hervorgehoben sind und das Attribut „FB“ = Verbotener Rückfluss hinzugefügt wird. In diesem Anwendungsfall sind dies (F1), (F2), (F4), (F10), (F12), (F14), (F16), (F17), (F19), (F21) und (F23).
- Datenflüsse $F_I(z)$ vom Informationsraum I(x) zum Informationsraum I(y), wobei x ∈ Z, 0 ≤ y < x und z = Klassifizierung und z ≤ y rot markiert sind und das Attribut „RB“ = Freigegebener Informationsrückfluss hinzugefügt wird. In unserem Anwendungsfall sind dies die Datenflüsse (F3), (F4), (F8).
- Daten fließen $F_I(z)$ vom Informationsraum I(x) zum Informationsraum I(y), wobei x ∈ Z, x ≥ y, y = −1 und z = Klassifizierung und z > y blau markiert, rot durchgestrichen und das Attribut „0“ = Verbotener Informationsfluss hinzugefügt wird.

5.5.2. Analyse des Anwendungsfalls

Nun können diejenigen operationellen Netzknoten identifiziert werden, die am meisten gefährdet sind, wenn sie ihre Vertraulichkeit, Verfügbarkeit und Integrität verlieren. Dazu werden zunächst die ausgehenden Datenflüsse der einzelnen operationellen Netzknoten betrachtet, um die Gefahr des Verlustes der Vertraulichkeit zu ermitteln (siehe Tabelle 5.2). (P1) hat drei ausgehende Datenflüsse, die alle vom Informationsraum DEU_1 zu den anderen Informationsräumen gehen. Der Schweregrad der Offenlegung von Informationen an eine nicht autorisierte Stelle ist einer von den folgende dreien. Es kann entweder 1 sein, was DEU_{-1} = Öffentlich entspricht, oder es kann 3 sein, was für DEU_1 = VS-NUR-FÜR-DEN-DIENSTGEBRAUCH steht, oder es kann 5 sein, was als DEU_3 = GEHEIM definiert ist. Da (P1) nur ausgehende Datenflüsse aus dem Informationsraum DEU_1 hat, beträgt die Schweregrad 3. Daher ist der Vertraulichkeitsindex das Ergebnis von dreimal drei, also neun. (P2) hat drei ausgehende Datenflüsse, zwei davon verlassen den Informationsraum DEU_1 und einer davon den Informationsraum DEU_3. Der entsprechende Schweregrad ist 3 und 5. Der aus der Gleichung EC*NoC=IND berechnete Vertraulichkeitsindex (siehe Abschnitt 5.4) ist das Ergebnis von zweimal drei plus einmal fünf, also elf. (P3) und (P4) haben zwei ausgehende Datenflüsse, von denen einer den Informationsraum DEU_1 und der andere den Informationsraum DEU_3 verlässt. Der damit verbundene Schweregrad ist 3 und 5. Daher ist der Vertraulichkeitsindex ein mal drei plus ein mal fünf, was in beiden Fällen acht ist. Dies bedeutet für ein Vertraulichkeitsranking, dass (P2) am meisten gefährdet ist, (P1) am zweithäufigsten gefährdet ist

und (P3) und (P4) gleichermaßen gefährdet sind, die Vertraulichkeit an eine nicht autorisierte Stelle zu verlieren. Die gleiche Berechnung kann für den Verfügbarkeits- und

Tabelle 5.2.: Vertraulichkeits-Ranking, Designphase

Operationeller Netzknoten	# ausgehender Verbindungen (NoC)	Schweregrad (EC)	Vertraulichkeitsindex (IND)	Rang
$P1$	(0/3/0)	(1/3/5)	$0+9+0=9$	2
$P2$	(0/2/1)	(1/3/5)	$0+6+5=11$	1
$P3$	(0/1/1)	(1/3/5)	$0+3+5=8$	3
$P4$	(0/1/1)	(1/3/5)	$0+3+5=8$	3

den Integritätsindex durchgeführt werden. Für die Verfügbarkeit müssen die eingehenden Datenflüsse der einzelnen operationellen Netzknoten und das Angriffspotenzial berücksichtigt werden, um die Gefahr eines Verfügbarkeitsverlustes zu ermitteln (siehe Tabelle 5.3).

Tabelle 5.3.: Verfügbarkeits-Ranking, Designphase

Operationeller Netzknoten	# eingehender Verbindungen (NoC)	Angriffspotenzial (EC)	Verfügbarkeitsindex (IND)	Rang
$P1$	(2/0/2)	(6/4/2)	$12+0+4=16$	2
$P2$	(2/1/0)	(6/4/2)	$12+4+0=16$	2
$P3$	(2/2/1)	(6/4/2)	$12+8+2=22$	1
$P4$	(2/0/0)	(6/4/2)	$12+0+0=12$	4

Wenn man alle Datenflüsse der einzelnen operationellen Netzknoten und die Änderungsmöglichkeit betrachtet, kann man die Gefahr eines Integritätsverlustes feststellen (siehe Tabelle 5.4). Nach der Identifizierung eines Rankings für die drei Sicherheitsziele ist es nun möglich, diese Rankings der einzelnen operationellen Netzknoten in Abhängigkeit von der Bedeutung der einzelnen Sicherheitsziele, dem Sicherheits-Bedeutungswert (SIV) der einzelnen operationellen Netzknoten zusammenzuführen.

Die Tabelle 5.5 zeigt das SIV-Ranking. Für (P1) und (P3) ist das SIV 1,65, für (P2) ist das SIV 1,98, für (P5) ist das SIV 3,63. Daraus folgt, dass (P1) und (P3) unter ausgewogener Gewichtung am meisten gefährdet sind. Diese Information kann nun dazu genutzt werden, für die operationellen Netzknoten (P1) und (P3) besondere Schutzmaßnahmen im künftigen System zu definieren. Dies können organisatorische, IT-technische oder auch baulich-physikalische Maßnahmen sein.

Tabelle 5.4.: Integritäts-Ranking, Designphase

Operationeller Netzknoten	# Verbindungen (NoC)	Änderungsmöglichkeit (EC)	Integritäts-Index (IND)	Rang
$P1$	(2/3/2)	(6/4/2)	12+12+4 = 28	1
$P2$	(2/3/1)	(6/4/2)	12+12+2 = 26	3
$P3$	(2/3/2)	(6/4/2)	12+12+4 = 28	1
$P4$	(2/1/1)	(6/4/2)	12 + 4 + 2 = 18	4

Tabelle 5.5.: Sicherheits-Bedeutungswert (SIV) Ranking, Designphase

Operationeller Netzknoten	Vertraulichkeits-Ranking	Verfügbar keits-Ranking	Integritäts-Ranking	SIV	Rang
$P1$	2	2	1	1,65	1
$P2$	1	2	3	1,98	3
$P3$	3	1	1	1,65	1
$P4$	3	4	4	3,63	4

5.6. Zusammenfassung

In diesem Kapitel wurde eine neue Methodik zur Modellierung von Datenflüssen eingeführt und eine Sicherheitsanalyse einer Organisationsstruktur aus der Designphase vorgestellt, die in einem Sicherheitsdatenflussdiagramm abgebildet wurde. Diese Darstellung ermöglicht die Identifizierung von Informationsräumen, was dabei hilft, die erlaubten und verbotenen Informationsflüsse innerhalb und zwischen diesen Informationsräumen zu verstehen. Das resultierende Modell heißt DFDsec. Das Modell ermöglicht eine Bedrohungsanalyse von Verbindungen, insbesondere zwischen den identifizierten Informationsräumen, um operationelle Netzknoten zu bestimmen, welche durch die Gefahr des Verlustes von Vertraulichkeit, Verfügbarkeit oder Integrität am stärksten gefährdet sind.

Die Analyse wurde mit einer operationellen Netzknotenstruktur und deren verbundenen Datenflüssen begonnen. Dabei wurden mögliche (gültige und ungültige) Pfade angegeben, über die Informationen zwischen den Netzknoten fließen können. Danach wurden alle Objekte eines Geheimhaltungsgrades in einem Informationsraum zusammengefasst. Anschließend wurden alle Verbindungen identifiziert, die zwischen den Informationsräumen verlaufen. Alle anderen Datenflüsse, welche innerhalb der Informationsräume fließen wurden reduziert. Schließlich wurden die Strukturen im Hinblick auf die Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität analysiert.

Dabei wurde ein Ansatz zur Quantifizierung der Sicherheitsrelevanz aller Netzknoten, basierend auf der gegebenen DFDsec-Struktur, diskutiert. Dies hilft, operationelle Netznoten in ihrer Bedeutung für notwendige Sicherheitsverbesserungen und Mitigati-

onsmaßnahmen zu ordnen und zu priorisieren. Unter ausgewogener Gewichtung führte dies dazu, dass bestimmte operationelle Netzknoten am meisten gefährdet sind. Deswegen sollten zunächst Sicherheitsmaßnahmen für diese Bereiche ergriffen werden.

Dieser Ansatz wurde in diesem Kapitel anhand eines Beispiels aus der Designphase veranschaulicht und kann bereits in der frühen Phase der Entwicklung angewendet werden. Im Kapitel 6 wird die Analyse weiterentwickelt, um ein Beispiel aus der Nutzungsphase (siehe Abschnitt 6.4) zu erörtern. Ferner wird die DFDsec-Methodik genutzt, um mit Hilfe von Protokolldaten, die während der Nutzungsphase eines realen IT-Systems entstanden sind, die Struktur und die Datenflüsse der darin enthalten operationellen Netzknoten zu analysieren und darzustellen.

Im Kapitel 6 wird sich der Problematik der Informationsflüsse von „oben“ nach „unten“ annehmen und Lösungen für die Erkennung der Verletzung der Integrität von Informationsräumen erläutern. Dies sind Bedrohungen aus der Phase 2 „Angriff auf das Ziel“. Kapitel 7 wird sich dann darauf aufbauend mit der Frage beschäftigen, wie man große Mengen an Protokolldaten reduzieren kann, um das unbefugte Eindringen in Informationsräume festzustellen.

6. Identifizierung von Informationsraumverletzungen mit Hilfe von anonymisierter Nachrichtenflussanalyse

Im letzten Kapitel wurde die Methodik „Sicherheitsdatenflussdiagramm (DFDsec)“ definiert und eine beispielhafte Analyse präsentiert. Dieser Ansatz kann in der konzeptionellen Phase, also bei der Definition von Anforderungen an ein künftiges System, verwendet werden. In diesem Kapitel wird nun mit Bezug auf die Forschungsfragen aus dem Abschnitt 2.7 und der DFDsec-Methodik eine Nachrichtenflussanalyse durchgeführt, um Verletzungen der Informationsraumgrenzen festzustellen.

- Wie kann man den Informationsfluss von oben (z. B. GEHEIM) nach unten (z. B. Öffentlich) feststellen?
- Wie kann man die Überwindung der physikalischen Trennung zwischen Informationsräumen feststellen?

Moderne Informationsinfrastrukturen und -organisationen stehen zunehmend vor dem Problem von IT-Sicherheits- und Datenschutzverletzungen sowie Cyberangriffen (siehe auch Kapitel 2). Eine traditionelle Methode zur Lösung dieses Problems sind Informationsräume wie „GEHEIM“, „VS-NUR-FÜR-DEN-DIENSTGEBRAUCH“ und „OFFEN“, die den Zugriff von Personen, Hard- und Software auf Datensätze regeln. Im Folgenden wird ein Ansatz vorgestellt, der Verstöße gegen Informationsräume durch eine automatisierte Nachrichtenflussanalyse findet. Dieser Ansatz berücksichtigt das Problem der Anonymisierung der Quellereignisprotokolle, wodurch das resultierende Datenflussmodell mit Experten und der Öffentlichkeit gemeinsam genutzt werden kann. Es werden die praktischen Auswirkungen der Anwendung des Ansatzes auf einen großen Datensatz einer Regierungsorganisation diskutiert und darüber hinaus wie die Anonymität des Konzepts formal validiert werden kann.

Die Struktur dieses Kapitels ist wie folgt: In Abschnitt 6.1 wird die Problemstellung und die Grundidee dieses Kapitels dargestellt. Im Abschnitt 6.2 werden die verwandten Arbeiten vorgestellt, insbesondere in Bezug auf die Analyse von Protokolldaten. Im Abschnitt 6.3 wird die Vorgehensweise zur Protokollierung von Daten im Datenflussmodell skizziert. Es folgt der Abschnitt 6.5, welcher erklärt und nachweist, dass die Daten durch den beschriebenen Ansatz hinreichend anonymisiert werden. Das Kapitel schließt mit einer kurzen Zusammenfassung im Abschnitt 6.6.

6.1. Ansatz

Die Untersuchung wird auf der Grundlage von Protokollen vergangener Informationsflüsse in einer Regierungsorganisation durchgeführt, die hier als einfache textuelle Protokolldateien von Mail-Servern vorliegen. Der ursprüngliche Rohdatensatz wird in ein Sicherheitsdatenflussdiagramm (DFDsec) umgewandelt, das einmalig, periodisch, manuell oder automatisiert generiert und untersucht werden kann. Ziel dieser Untersuchung ist es, Schwachstellen und unbekannte Angriffsvektoren in der Infrastruktur zu finden. Die spezielle Eigenschaft dieses Ansatzes ist die Anonymisierung der Quelldaten. Dies ist eine gängige Erwartung in Organisationen mit obligatorischen Informationsräumen, stellt aber im Allgemeinen das Gegenteil von frei zugänglicher Sicherheitsforschung dar. Die Anonymisierungsforderung verhindert in der Regel auch die Zusammenarbeit mit externen Beratern oder zwingt sie, starke rechtliche Geheimhaltungsvereinbarungen (Legal Non Disclosure Agreement - NDA) abzuschließen. In diesem Ansatz wird versucht, beide Themen gleichzeitig anzugehen.

6.2. Log-Daten und Datenflussdiagramme

Die automatisierte Erkennung von Verstößen gegen Informationsräume oder verdächtigen Aktivitäten im Allgemeinen ist ein klassisches Thema in der Sicherheitsforschung und -praxis. Ein frühes Beispiel aus den 80er Jahren ist das Haystack-System [127], welches dazu gedacht war, Eindringlinge in Luftwaffensysteme basierend auf atypischer Systemnutzung zu erkennen. Die Autoren haben sich bereits mit dem Problem eines „Ereignishorizonts“ beschäftigt, so dass die Überwachungsdaten vor der Weiterverarbeitung reduziert werden mussten.

Moderne Computersysteme erzeugen ständig große Mengen an Ereignisprotokollen. Diese Protokolle sind für Systemadministratoren gedacht, um den aktuellen Systemstatus zu verstehen und Probleme mit Systemausfallzeiten zu erkennen. Die Verwendung von Protokolldateien zum Auffinden von Zuverlässigkeitsvorfällen ist ein klassisches Thema im High-Performance-Computing (HPC). In der Vergangenheit gab es Versuche, dafür Mustererkennung [69], Data-Mining [130], [149], [158] Clustering [148], Support-Vektor-Maschinen (Stützvektormaschinen) [12], [74], oder Entscheidungsbaum-Lernen (decision tree learning) [114] zur Analyse großer Mengen an ursprünglichen Protokolldaten einzusetzen. Oliner et al. [102] nutzten zum Beispiel die Informationsentropie von Nachrichtenbegriffen, um fehlerbezogene Ereignisse in HPC-Protokollen zu finden.

Fast alle diese Ansätze konzentrieren sich auf Zuverlässigkeitsereignisse, wie z. B. Hardwarekomponentenausfälle, die durch Schweregrad-Marker in den Protokolldateien angezeigt werden. Es macht diese Ansätze für das Problem der Informationsraumverletzungen nicht direkt anwendbar, jedoch können die verfügbaren Ideen zur Reduzierung von Protokollinformationen direkt genutzt werden [32], [2], [122], [105]. Es werden auch Sicherheitsmetadaten in der Protokollanalyse verwendet, was in HPC-ähnlichen Systemen nicht üblich ist.

Kapitel 5 hat bereits gezeigt, dass die erweiterten Datenflussdiagramme helfen kön-

nen, die Beziehung zwischen Infrastrukturkomponenten und Informationsräumen auszudrücken [95]. Die daraus resultierenden Datenflussinformationen automatisiert untersucht werden, so dass Sicherheitsbedrohungen automatisch und zur Laufzeit erkannt werden können. Die Datenflussanalyse im Sicherheitskontext wird bereits für Systemaufrufe von Anwendungen [89], Netzwerkverkehr [131], [144], [72], virtuelle Laufzeit-Engines [53], Programm-Binaries [31] oder Programmcode [3] verwendet. Dieser Beitrag fokussiert sich auf die Erstellung von anonymisierten Datenflussdiagrammen, welche von menschlichen Auditoren innerhalb und außerhalb der Organisation überprüft werden können.

6.3. Von der Ereignisprotokollierung bis zur Datenflussanalyse

Um in militärischen und Regierungsorganisationen die Zusammenarbeit zwischen den Behörden zu verbessern und bei Bedarf externe Berater hinzuziehen zu können, ist es notwendig, klassifizierte Informationen so darzustellen, dass dies möglich ist. Dazu wurde ein Ansatz entwickelt, welcher anonymisierte Ergebnisse unter Nutzung der DFDsec (Kapitel 5) darstellt. Dieser Ansatz kombiniert die folgende Schritte (siehe auch Abbildung 6.1):

1. Ereignisprotokoll-Bereinigung
2. Auswertung von Nachrichtenpfaden
3. Modellgenerierung (Anonymisierung der Quelldaten unter Beibehaltung relevanter Sicherheitsinformationen und Umwandlung in ein Datenflussmodell)

Dieser Ansatz wurde auf den folgenden Datensatz einer großen staatlichen Organisation angewendet:

- Unstrukturierte, unbearbeitete Protokolle über die Netzwerkkommunikation für eine Reihe von Servern (siehe Tabelle 6.1)[1]
  - Zeitbereich: 01/16 - 11/16
  - Mehrere Textdateien pro Ordner, die jeweils eine bestimmte Zeitspanne abdecken.
  - Log-Einträge pro Datei im Textspaltenformat
  - Pro Log-Eintrag: Zeitstempel, eindeutiger Nachrichtenidentifikator, Sende-/Empfangsoperationen, Datengröße
- Liste der Netzknoten und ihre zugehörigen Geheimhaltungsgrade (Sicherheitseinstufung)

Inhalt und Art der ausgetauschten Daten sind für sich schon eine vertrauliche Information und können daher nicht im Rahmen dieser Arbeit diskutiert werden.

[1] Die Daten, die in der Tabelle spaltenweise dargestellt sind, sind in den Protokolldateien in einer Zeile. Aus Darstellungsgründen wurde dies geändert.

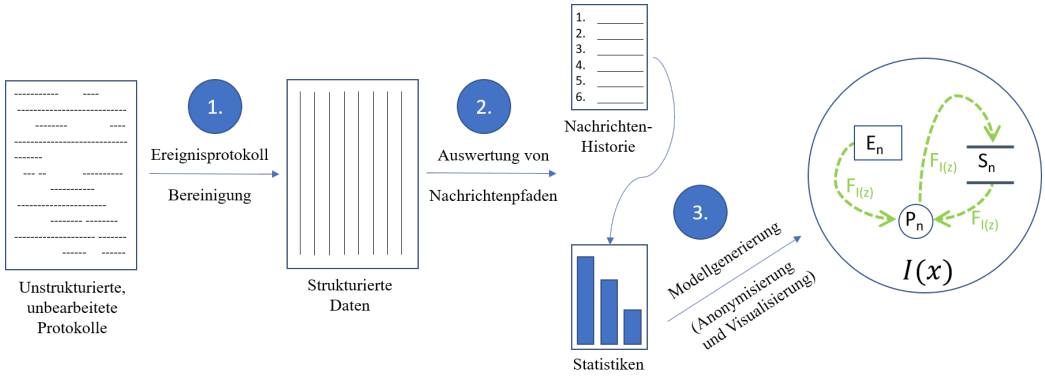

Abbildung 6.1.: Schritte zur Erkennung von Informationsraumverletzungen

Tabelle 6.1.: Beispiel für unbearbeitete Log-Daten

Ordnername:			Server SA		
Dateiname:			2016-01-01XXX.log		
01	00:02:12	Daten empfangen von	Server S_B	YYY Bytes	ID-ABC
01	00:02:12	Weitergeleitet zu	Server S_C		ID-ABC
01	00:02:12	Daten gesendet an	Server S_D	YYY Bytes	ID-ABC

6.3.1. Bereinigung von Ereignisprotokollen

Es wurden eine Reihe von Python-Skripten entwickelt, welche die ursprünglichen Protokolldateien linear analysieren und eine Datenbank mit den Kommunikationsaktivitäten der Netzknoten generieren. In diesem Schritt werden ungültige und unvollständige Informationselemente entfernt, wie z. B. Protokolleinträge mit fehlenden Informationen zur Klassifizierung von Nachrichten oder ungültigen Zeitstempeln. Beide Probleme wurden mit den Administratoren der Infrastruktur besprochen. Sie wurden mit Implementierungsfehlern begründet und nicht mit einem möglichen Angriffsversuch, die Logs zu bereinigen. Das Ergebnis dieses Normierungsschritts ist eine Reihe von Datensätzen, wie in Tabelle 6.2 dargestellt, wobei jeder die folgenden Informationen liefert:

- Spalte 1: Datum,
- Spalte 2: Zeit,
- Spalte 3: Netzknoten, der den Protokolleintrag erzeugt,
- Spalte 4: Datenoperation, die vom referenzierten Netznoten durchgeführt wird (Senden/Relais/Empfangen),
- Spalte 5: Datengröße der Nachricht,

- Spalte 6: Peernetzknoten,
- Spalte 7: Eindeutige Nachrichtenkennung (Nachrichten-ID).

Tabelle 6.2.: Beispiel-Ergebnis der Normierung

Date	Time	Server-Name	Daten-richtung	Byte-Größe	Server-Name	Nachrichten ID
2016-01-01	00:02:12	S_A	Empfangen von	YYY	S_B	ABC
2016-01-01	00:02:12	S_A	Weiter geleitet zu		S_C	ABC
2016-01-01	00:02:12	S_A	Gesendet an	YYY	S_D	ABC
...	...	...	...			

Es muss hierbei beachtet werden, dass das Senden von Nachrichten in zwei Varianten erfolgt: Senden, das durch den Netzknoten selbst ausgelöst wird, und Erfassen, das durch das Weiterleiten einer empfangenen Nachricht ausgelöst wird. Dies führt dazu, dass eine einzelne Empfangsaktivität von einem von den Netzknoten begründet werden kann, was aus dem Eintrag nicht direkt ersichtlich ist. Aus diesem Grund müssen die Nachrichtenpfade als Ganzes betrachtet werden.

6.3.2. Auswertung von Nachrichtenpfaden

Angesichts der Datensätze über die direkte Netzknoten-zu-Netzknoten-Interaktion sind nun die Nachrichtenpfade, welche sich über Relaisknoten erstrecken können, erkennbar. Dies kann einfach durch die Bündelung einzelner Übertragungsaktivitäten auf der Grundlage der eindeutigen Nachrichtenkennung erreicht werden. Es werden wiederum eine Reihe von Python-Skripten implementiert, da die Menge der Protokolldaten einen solchen Ansatz noch möglich macht. Für größere Datensätze können entsprechende skalierbare Analysetools auf Basis von NoSQL-Datenbanken eingesetzt werden.

Das Ergebnis ist eine Menge von Nachrichtentransfers, bei dem jeder Transfer die Menge der beteiligten Netzknoten enthält. Dies kann der Ausgangspunkt für eine Vielzahl von Analyseschritten sein. Im hier vorliegenden Ansatz wird die reine Netzknoten-zu-Netzknoten-Nachrichtenfrequenzstatistik genutzt. Zusammen mit den angegebenen Geheimhaltungsgraden der Netzknoten führt dies zu einem Datensatz, welcher die Interaktionsfrequenz von Netzknoten in verschiedenen oder gleichen Informationsräumen beschreibt. Zusammen mit der Gesamtzahl der Nachrichten ist es nun möglich, die Diagrammdarstellung für weitere Analysen zu generieren.

Die Tabelle 6.3 zeigt ein Beispiel für die resultierende Datendatei. Es ermöglicht, den Weg jeder Nachricht durch das Netzwerk zu bestimmen.

Tabelle 6.3.: Beispiel-Nachrichtenpfade

Nachrichten-ID	[	Liste der Serververbindungen			]
ABC:	[	'Server S_A	⇒	Server S_B',	
		'Server S_A	⇒	Server S_C',	
		'Server S_A	⇒	Server S_D'	]
...:	[	...	⇒	...	]

6.3.3. Modellgenerierung

Die Visualisierung der identifizierten Informationsaustauschströme erfolgt mit dem Ansatz *Sicherheitsdatenflussdiagramm (DFDsec)* aus Kapitel 5.

Das DFDsec-Diagramm wird automatisch aus den im letzten Schritt erzeugten Nachrichtenaustauschdaten erzeugt. Dies geschieht durch die Erstellung einer einzigen GraphML-Datei pro Datensatz. Diese Datei wird durch einen Auto-Layout-Algorithmus zum Bestimmen der Positionen der Modellelemente im Endbild modifiziert.

Eines der Ziele des in diesem Kapitel beschriebenen Ansatzes ist die anonymisierte und pseudonymisierte Darstellung sensibler Informationen in einem Sicherheitsmodell. Daher wurden die folgenden Anonymisierungsschritte durchgeführt:

- Der Zeitstempel des Nachrichtenaustauschs wird bei der Modellgenerierung nicht verwendet (Spalte 1 & 2).
- Servernamen werden in Pseudonyme übersetzt (Spalte 3).
- Nachrichtengröße und Nachrichtenkennung werden bei der Modellgenerierung nicht verwendet (Spalte 5 & 7).
- Datenflüsse zwischen Prozessen werden mit dem Anteil des Nachrichtenaustauschs zugerechnet, den sie zur Gesamtmenge des Datenaustauschs beigetragen haben.

Um die Modellkomplexität in der Praxis zu reduzieren, wird auf den Datenaustausch zwischen Knoten im selben Informationsraum verzichtet, wenn dieser weniger als 1% zum Gesamtdatenverkehr beiträgt. Die Idee dahinter ist, dass für einen potenziellen Angreifer hoch frequentierte Netzknoten wertvoller sind als spärlich genutzte Server. Ein offensichtlicher Grund dafür ist, dass erfolgreiche kryptografische Angriffe meist auf die Verfügbarkeit größerer Nachrichtenflüsse angewiesen sind. Informationsraumübergreifende Nachrichtenflüsse werden nicht ignoriert, da jeder einzelne Nachrichtentransfer auf eine mögliche Sicherheitsverletzung hinweisen kann.

Die Abbildung 6.2 zeigt ein DFDsec-Diagramm, welches aus dem realen Datensatz der Regierungsorganisation generiert wurde. Es zeigt, dass zwei verschiedene Informationsräume in der Nutzung sind, VS-NUR-FÜR-DEN-DIENSTGEBRAUCH (DEU_1) und GEHEIM (DEU_3). Jeder Informationsraum enthält mehrere operationelle Netzknoten (Sender-, Empfänger- oder Relay-Server). Zwischen diesen Knoten gibt es Informationsflüsse. Innerhalb des verwendeten Datensatzes stellte sich heraus, dass kein Nachrichtenaustausch über eine Informationsraumgrenze hinweg stattgefunden hat. Für das jeweilige Regierungssystem ist dies die erwartete und korrekte Funktionsweise.

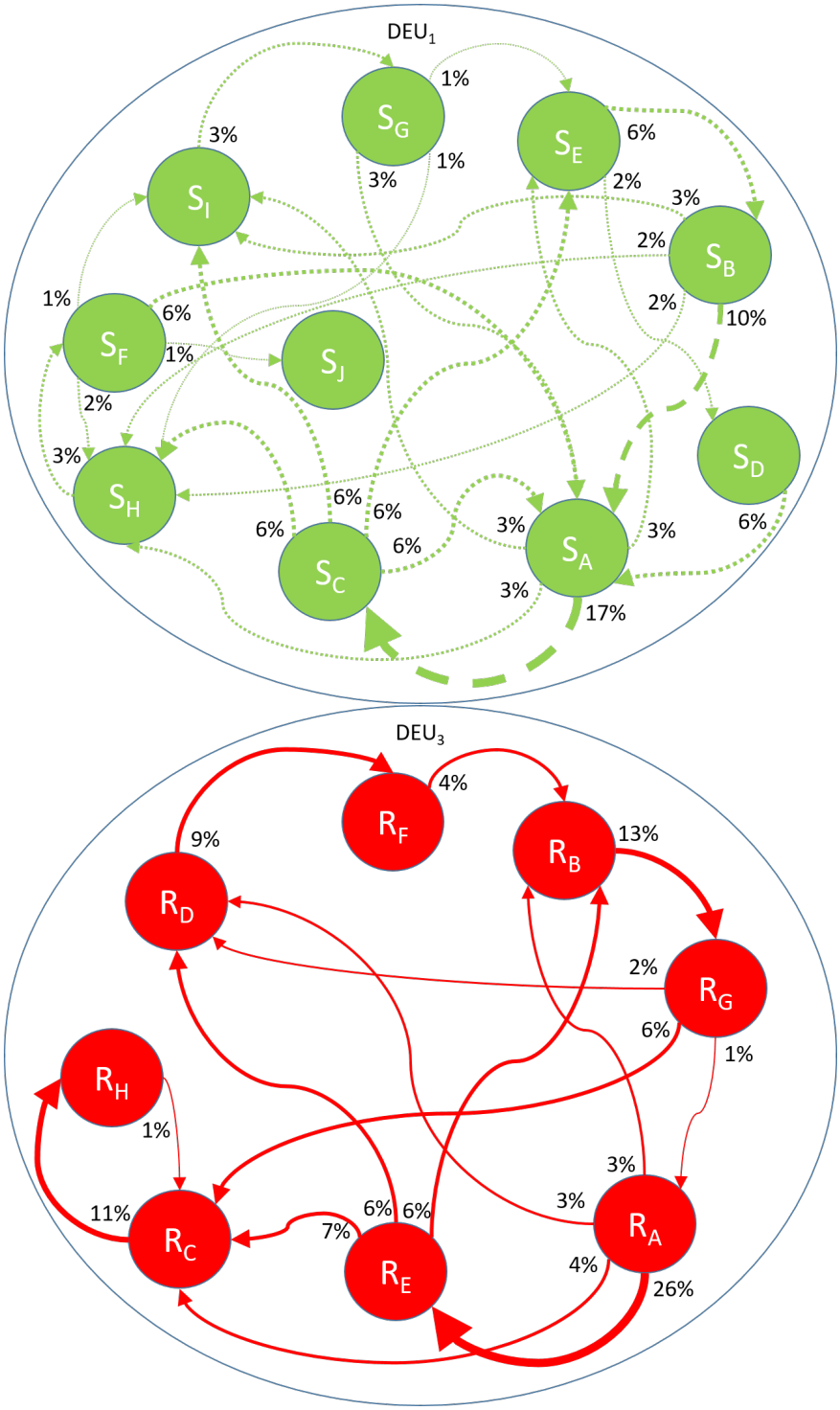

Abbildung 6.2.: DFDsec in der Nutzungsphase

Wenn eine DFDsec-Analyse einen Informationsraumübergang zeigt, hängt es von der Art der Quell- und Zielzone ab, wie bereits im Abschnitt 2.5 beschrieben, ob es sich dabei um ein Problem handelt. Ein typischer Ansatz wäre die wiederholte Untersuchung der Frage über die Zeit, z. B. durch periodische Generierung mehrerer DFDsec-Modelle und ein Vergleich derer. Damit könnte geklärt werden, ob die Überschreitung der Informationsraumgrenze zu normalen Geschäftszeiten mit einer zu erwartenden Nachrichtenfrequenz eine regelmäßige Aktivität ist oder ob es sich um eine Anomalie im Systembetrieb handelt. Die Analyse kann auch spezifische Eigenschaften der beteiligten Netzknoten berücksichtigen, wie z. B. deren Rolle in der Organisation.

Für den gegebenen Datensatz stellte sich heraus, dass der wichtigste operationelle Netzknoten S_A ist. 26 Prozent des Datenverkehrs dieses Knotens sind ausgehende Verbindungen und 31 Prozent des Verkehrs sind eingehende Verbindungen.

Im Informationsraum GEHEIM ist der wichtigste operationelle Netzknoten R_A. 36 Prozent des Datenverkehrs verlassen diesen Knoten. Im Gegensatz dazu hat dieser Knoten kaum eingehende Verbindungen.

Aus Angreifersicht scheinen diese beiden Knoten am interessantesten zu sein. Die meisten Informationsflüsse beginnen oder enden hier, so dass sie das größte Potenzial für die Sammlung von eingestuften Informationen haben. Aus Sicht des Verteidigers müssen IT-Sicherheitsmaßnahmen in erster Linie bei diesen beiden Knoten getroffen werden. Eine Idee wäre es, diese wichtigen Knoten redundant zu gestalten, so dass sie beispielsweise in hierarchischen Organisationen nicht mehr als einziges Relais für Nachrichten fungieren. Dies würde vertrauliche Informationen über mehrere Pfade in der Organisation verteilen, was es für einen Angreifer schwieriger macht, die relevanten Netzknoten im System zu identifizieren, welche einen Angriff wert sind.

Der wichtigste Informationsfluss innerhalb des Informationsraumes VS-NUR-FÜR-DEN-DIENSTGEBRAUCH ist die Verbindung S_A - S_C. Sie ist für 17 Prozent der Nachrichtenflüsse verantwortlich, gefolgt von der Verbindung S_B - S_A bei 10 Prozent. Der wichtigste Informationsfluss im Informationsraum GEHEIM ist die Verbindung R_A - R_E bei 26 Prozent, gefolgt von der Verbindung R_B - R_G bei 13 Prozent und der Verbindung R_C - R_H bei 11 Prozent.

Aus Sicht eines Angreifers sind dies diejenigen Verbindungen, welche für ein Man-in-the-Middle geeignet sind, z. B. durch Kompromittierung von Switches und Routern auf dem Netzwerkpfad zwischen den beiden Netzknoten. Aus defensiver Sicht wäre es daher sinnvoll, darüber nachzudenken, ob der Verkehr anders verteilt werden soll, um besonders stark ausgelastete Verbindungen, z. B. durch Lastverteilung [45], zu vermeiden oder das Verbindungsnetz entsprechend zu härten.

6.4. Weitergehende Analyse

In diesem Abschnitt werden die entstandenen DFDsec-Diagramm mithilfe der Methodik aus Abschnitt 5.4 analysiert. Bei der präsentierten Analyse ging es um die Identifizierung von operationellen Netzknotenstrukturen, die am stärksten von der Gefahr des Verlustes der Vertraulichkeit, Verfügbarkeit und Integrität betroffen sind. Aufgrund der Ausrich-

tung dieser Arbeit wird der Fokus dieser Analyse auf den IT-Sicherheitszielen Vertraulichkeit und Integrität sein. Ein wesentlicher Unterschied zwischen dieser Analyse und der Analyse aus Abschnitt 5.5.2 ist, dass hier die Datenflüsse innerhalb eines Informationsraumes analysiert werden und in der Analyse im Abschnitt 5.5.2 die Datenflüsse zwischen den Informationsräumen. Somit wird es ein Ranking für jeden Informationsraum geben. Ein weiterer Unterschied besteht darin, dass bei dieser Analyse zusätzlich gewichte Verbindungen existieren. Dieser Faktor kann genutzt werden, um die Methodik der Analyse aus Abschnitt 5.4 zu erweitern. Ein weiterer Unterschied ist, dass im Abschnitt 5.5.2 ein Anwendungsfall aus der Designphase beschrieben wurde und hier nun ein Anwendungsfall aus der Nutzung analysiert wird.

6.4.1. Beschreibung des Anwendungsfalls

Wie bereits im Abschnitt 6.3.3 dargestellt besteht das Beispiel aus zwei Informationsräumen DEU_1, was VS-NfD entspricht und DEU_3, was GEHEIM entspricht. DEU_1 besteht aus insgesamt 10 Prozessen, S_A - S_J. Der Informationsraum DEU_3 beinhaltet 8 Prozesse, R_A - R_H. Die Datenflüsse im Informationsraum DEU_1 haben alle den Geheimhaltungsgrad DEU_1. Die Datenflüsse im Informationsraum DEU_3 besitzen den Geheimhaltungsgrad DEU_3. Bei dieser Art von Datenflüssen handelt es sich um die gleichen Datenflüsse, wie sie in der Abbildung 5.1 im Abschnitt 5.3 definiert wurden. In Abbildung 6.2 wurden die Sicherheitsattribute in beiden Informationsräumen nicht dargestellt, da sie für den jeweiligen Informationsraum gleich sind. Da es sich bei dem untersuchten System um ein klassifiziertes System in der operativen Nutzung handelt, werden die Inhalte der Daten im Gegensatz zum Beispiel aus Abschnitt 5.5.1, die zwischen den einzelnen Prozessen ausgetauscht, nicht beschrieben. Es wird sich auf die Anzahl der Verbindungen und deren prozentuale Verteilung in Bezug auf ihre Menge beschränkt.

6.4.2. Analyse des Anwendungsfalls

Durch Nutzung der Methodik aus Abschnitt 5.4 werden nun diejenigen operationellen Netzknoten identifiziert, welche am meisten gefährdet sind, wenn sie ihre Vertraulichkeit und Integrität verlieren. Dazu werden zunächst die ausgehenden Datenflüsse der einzelnen operationellen Netzknoten betrachtet, um die Gefahr des Verlustes der Vertraulichkeit zu ermitteln (siehe Tabellen 6.4 - 6.10) und im Anschluss alle Verbindungen der operationellen Netzknoten, um die Gefahr eines Integritätsverlustes festzustellen (siehe Tabellen 6.6 - 6.12).

Informationsraum VS-NfD

Es wird mit der Analyse der Gefahr für den Verlust der Vertraulichkeit im Informationsraum DEU_1 (VS-NfD) begonnen. Zunächst wird die Analyse genauso durchgeführt, wie in Abschnitt 5.4 beschrieben, d.h. nur die Berücksichtigung der Anzahl der ausgehenden Verbindungen. Danach werden in einem zweiten Schritt die Auslastungen der Verbindung mit betrachtet. Tabelle 6.4 zeigt den ersten Schritt. In Spalte 1 befinden sich

die operationellen Netzknoten und in Spalte zwei die Anzahl der ausgehenden Verbindungen. In Spalte 3 ist das Evaluationskriterium für Vertraulichkeit, der Schweregrad. Dieser liegt im Informationsraum DEU_1 bei 3. Und schließlich befindet sich in Spalte 4 der Vertraulichkeitsindex und in Spalte 5 der Rang, also die Priorisierungsreihenfolge für spätere Maßnahmen, wenn die Vertraulichkeit im Vordergrund steht. Exemplarisch wird an einem operationellen Knoten das Verfahren erklärt. S_A hat 4 ausgehenden Verbindungen. Der Schweregrad bestimmt sich dadurch, dass diese Verbindungen innerhalb des Informationsraums DEU_1 verlaufen, also 3. Aus der Gleichung $EC * NoC = IND$ berechnet sich der Vertraulichkeitsindex von 12. Daraus ergibt sich der höchste Rang in der Tabelle.

Diesen Rang haben aber auch noch 3 weitere operationelle Netzknoten, S_B, S_C und S_F. Eine klare Priorisierung ist daraus nicht ableitbar. Dies wäre das Ergebnis, welches man aufgrund fehlender Nutzungsstatistiken in der Designphase erhalten würde. Diese Statistiken wurden bei diesem Anwendungsfall berechnet und daher werden nun in einem zweiten Schritt die bereits vorhandenen Auslastungsdetails verwendet. Das Ergebnis dieses Schrittes zeigt Tabelle 6.5. Exemplarisch wird der operationelle Netzknoten S_A genutzt, um das Verfahren darzustellen. S_A hat immer noch 4 ausgehenden Verbindungen. Diese werden diesmal mit ihrer Auslastung gewichtet. Somit ergibt sich für die Verbindungen (1*0,03)+(1*0,03)+(1*0,03)+(1*0,17), was 0,26 ergibt. Dies ist bereits im Abschnitt 6.3.3 als Analyseergebnis festgestellt worden. In der Tabelle 6.5 wurden die ausgehenden Verbindungen (NoC) unter Berücksichtigung der prozentualen Auslastung bereits zusammen gerechnet.

Der Schweregrad bleibt wie in Schritt 1 gleich. Aus der Gleichung $EC * NoC = IND$ berechnet sich nun der neue Vertraulichkeitsindex von 0,26*3, was 0,78 ergibt. Daraus ergibt sich der höchste Rang in der Tabelle. S_A ist diesmal der einzige Netzknoten auf diesem Rang. Diese Analyseänderung bestätigt das Ergebnis aus dem Abschnitt 6.3.3 und zeigt auch, dass sich eine in der Designphase festgelegte Priorisierung durch Auswertung von Nutzungsdaten ändern kann.

Die gleiche Berechnung kann für den Integritätsindex im Informationsraum DEU_1 durchgeführt werden. Hierbei werden nun alle Verbindungen, eingehende und ausgehende, berücksichtigt. Die Ergebnisse können den Tabellen 6.6 und 6.7 entnommen werden. In Spalte 1 befinden sich die operationellen Netzknoten und in Spalte zwei die Anzahl der Verbindungen bzw. die Anzahl unter Berücksichtigung ihrer Auslastung. Zur besseren Darstellung in der Tabelle wurden dabei die Ergebnisse dieses Schrittes bereits addiert. In Spalte 3 ist das Evaluationskriterium für Integrität, die Änderungsmöglichkeit. Diese liegt im Informationsraum DEU_1 bei 4. Schließlich befindet sich in Spalte 4 der Integritätsindex und in Spalte 5 der Rang, also die Priorisierungsreihenfolge für spätere Maßnahmen, wenn die Integrität im Vordergrund steht.

Nach der Identifizierung eines Rankings für die beiden Sicherheitsziele Vertraulichkeit und Integrität ist es nun möglich, diese Rankings der einzelnen operationellen Netzknoten in Abhängigkeit von der Bedeutung der einzelnen Sicherheitsziele zusammenzuführen, um den Sicherheits-Bedeutungswert (Security importance value - (SIV)) der jeweiligen Netzknoten zu erhalten. Die Tabelle 6.8 zeigt das SIV-Ranking. Grundlage bilden hierfür die erweiterten Analyseergebnisse der Tabellen 6.5 und 6.7. In Spalte 1 sind die opera-

Tabelle 6.4.: Vertraulichkeits-Ranking 1, Nutzungsphase für Informationsraum VS-NfD.

Operationeller Netzknoten	# ausgehender Verbindungen (NoC)	Schweregrad (EC)	Vertraulichkeits-Index (IND)	Rang
S_A	4	3	12	1
S_B	4	3	12	1
S_C	4	3	12	1
S_D	1	3	3	4
S_E	2	3	6	3
S_F	4	3	12	1
S_G	3	3	9	2
S_H	1	3	3	4
S_I	1	3	3	4
S_J	0	3	0	5

Tabelle 6.5.: Vertraulichkeits-Ranking 2, Nutzungsphase für Informationsraum VS-NfD.

Operationeller Netzknoten	# ausgehender Verbindungen (NoC)	Schweregrad (EC)	Vertraulichkeits-Index (IND)	Rang
S_A	$0,26$	3	$0,78$	1
S_B	$0,17$	3	$0,51$	3
S_C	$0,24$	3	$0,72$	2
S_D	$0,06$	3	$0,18$	6
S_E	$0,08$	3	$0,24$	5
S_F	$0,10$	3	$0,30$	4
S_G	$0,05$	3	$0,15$	7
S_H	$0,03$	3	$0,09$	8
S_I	$0,03$	3	$0,09$	8
S_J	0	3	0	10

Tabelle 6.6.: Integritäts-Ranking 1, Nutzungsphase für Informationsraum VS-NfD.

Operationeller Netzknoten	# Verbindungen (NoC)	Änderungsmöglichkeit (EC)	Integritäts-Index (IND)	Rang
S_A	9	4	36	1
S_B	5	4	20	3
S_C	5	4	20	3
S_D	2	4	8	9
S_E	5	4	20	3
S_F	5	4	20	3
S_G	4	4	20	3
S_H	7	4	28	2
S_I	5	4	20	3
S_J	1	4	4	10

Tabelle 6.7.: Integritäts-Ranking 2, Nutzungsphase für Informationsraum VS-NfD.

Operationeller Netzknoten	# Verbindungen (NoC)	Änderungsmöglichkeit (EC)	Integritäts-Index (IND)	Rang
S_A	$0,57$	4	$2,28$	1
S_B	$0,21$	4	$0,84$	3
S_C	$0,41$	4	$1,64$	2
S_D	$0,08$	4	$0,32$	8
S_E	$0,18$	4	$0,72$	5
S_F	$0,13$	4	$0,52$	7
S_G	$0,08$	4	$0,32$	8
S_H	$0,19$	4	$0,76$	4
S_I	$0,16$	4	$0,64$	6
S_J	$0,01$	4	$0,04$	10

tionellen Netzknoten, in Spalte 2 das Vertraulichkeitsranking des jeweiligen Netzknotens und in Spalte 3 das Integritätsranking dargestellt. In Spalte vier wird der SIV nach der abgewandelten Gleichung (Weglassen der Verfügbarkeit) $SIV = W_C * C + W_I * I$ aus Abschnitt 5.4 berechnet. Dabei sind die Sicherheitsziele gleich gewichtet.

Auch hier zeigt sich, dass die operationellen Netzknoten S_A, S_B und S_C unter ausgewogener Gewichtung am meisten gefährdet sind. Dies bestätigt die Analyse aus Abschnitt 6.3.3. Bei diesen Netzknoten können Schutzmaßnahmen (z. B. Lastverteilung), wie sie bereits dort diskutiert worden sind, angewendet werden.

Tabelle 6.8.: Sicherheits-Bedeutungswert (SIV) Ranking, Nutzungsphase für Informationsraum VS-NfD

Operationeller Netzknoten	Vertraulichkeits-Ranking	Integritäts-Ranking	SIV	Rang
S_A	1	1	1	1
S_B	3	3	3	3
S_C	2	2	2	2
S_D	6	8	7	7
S_E	5	5	5	4
S_F	4	7	5,5	5
S_G	7	8	7,5	8
S_H	8	4	6	6
S_I	8	6	7	7
S_J	10	10	10	10

Informationsraum GEHEIM

Für den Informationsraum DEU_3, also GEHEIM, können diese Berechnungen analog durchgeführt werden. Zunächst werden die Berechnung der Vertraulichkeitswerte und im Anschluss die Integritätswerte durchgeführt. Tabelle 6.9 zeigt die ersten Berechnungen. Diese sind vergleichbar mit denen, die in der Designphase durchgeführt werden. Es stechen hierbei drei operationelle Netzknoten (R_A, R_E und R_G) hervor. Diese drei Netzknoten sind nach dieser Berechnung für Sicherheitsmaßnahmen am höchsten zu priorisieren. Für den Rest ist die Tabelle wenig aussagekräftig, da eine wirkliche Priorisierung nicht gegeben ist.

In der Tabelle 6.10 ist die Berechnung der Vertraulichkeitswerte unter Berücksichtigung der prozentualen Auslastung abgebildet. Die Berechnung zeigt, dass R_A und R_E weiterhin die wichtigsten operationellen Netzknoten sind. Dahinter bietet sich ein differenziertes Lagebild, welches nun zeigt, dass der drittwichtigste Knoten R_B ist und R_G nur noch der fünftwichtigste Netzknoten ist. Die gleiche Berechnung wird für den Integritätsindex im Informationsraum DEU_3 durchgeführt. Unter Berücksichtigung aller

Tabelle 6.9.: Vertraulichkeits-Ranking 1, Nutzungsphase für Informationsraum GEHEIM.

Operationeller Netzknoten	# ausgehender Verbindungen (NoC)	Schweregrad (EC)	Vertraulichkeits-Index (IND)	Rang
R_A	4	3	12	1
R_B	1	3	3	3
R_C	1	3	3	3
R_D	1	3	3	3
R_E	3	3	9	2
R_F	1	3	3	3
R_G	3	3	9	2
R_H	1	3	3	3

Tabelle 6.10.: Vertraulichkeits-Ranking 2, Nutzungsphase für Informationsraum GEHEIM.

Operationeller Netzknoten	# ausgehender Verbindungen (NoC)	Schweregrad (EC)	Vertraulichkeits-Index (IND)	Rang
R_A	$0,36$	3	$1,08$	1
R_B	$0,13$	3	$0,39$	3
R_C	$0,11$	3	$0,33$	4
R_D	$0,09$	3	$0,27$	5
R_E	$0,19$	3	$0,57$	2
R_F	$0,04$	3	$0,12$	7
R_G	$0,09$	3	$0,27$	5
R_H	$0,01$	3	$0,01$	8

eingehenden und ausgehenden Verbindungen können die Ergebnisse den Tabellen 6.11 und 6.12 entnommen werden. Die erste Berechnung bringt hervor, dass die wichtigsten operationellen Netzknoten R_A und R_C sind. Für die restlichen ist das Bild indifferent. Für die zweite Berechnung konnte erneut eine Priorisierungsreihenfolge festgelegt werden. R_E ist der wichtigste Netzknoten, welcher gegen den Verlust der Integrität geschützt werden muss. Ihm folgt R_A, R_C und R_B.

Tabelle 6.11.: Integritäts-Ranking 1, Nutzungsphase für Informationsraum GEHEIM.

Operationeller Netzknoten	# Verbindungen (NoC)	Änderungsmöglichkeit (EC)	Integritäts-Index (IND)	Rang
R_A	5	4	20	1
R_B	4	4	16	3
R_C	5	4	20	1
R_D	4	4	16	3
R_E	4	4	16	3
R_F	2	4	8	4
R_G	4	4	16	3
R_H	2	4	8	4

Tabelle 6.12.: Integritäts-Ranking 2, Nutzungsphase für Informationsraum GEHEIM.

Operationeller Netzknoten	# Verbindungen (NoC)	Änderungsmöglichkeit (EC)	Integritäts-Index (IND)	Rang
R_A	$0,37$	4	$1,48$	2
R_B	$0,26$	4	$1,04$	4
R_C	$0,29$	4	$1,16$	3
R_D	$0,20$	4	$0,80$	6
R_E	$0,45$	4	$1,80$	1
R_F	$0,13$	4	$0,52$	7
R_G	$0,22$	4	$0,88$	5
R_H	$0,12$	4	$0,48$	8

Nun erfolgt abschließend die Berechnung des SIV für jeden einzelnen operationellen Netzknoten im Informationsraum GEHEIM. Diese kann der Tabelle 6.13 entnommen werden. Auch hier bleiben die Sicherheitsziele gleich gewichtet.

Die operationellen Netzknoten R_A und R_E sind unter ausgewogener Gewichtung am meisten gefährdet. Dies bestätigt ebenfalls die Analyse aus Abschnitt 6.3.3, wobei in

diesem Fall durch die starke Kommunikationsbeziehung zwischen R_A und R_E der Netzknoten R_E stärker in den Fokus rückt. Bei diesen Netzknoten können die gleichen Schutzmaßnahmen wie eine Lastverteilung mit den zuständigen Administratoren besprochen und geklärt werden, ob zusätzliche Maßnahmen erforderlich sind.

Tabelle 6.13.: Sicherheits-Bedeutungswert (SIV) Ranking, Nutzungsphase für den Informationsraum GEHEIM.

Operationeller Netzknoten	Vertraulichkeits-Ranking	Integritäts-Ranking	SIV	Rang
R_A	1	2	1,5	1
R_B	3	4	3,5	3
R_C	4	3	3,5	3
R_D	5	6	5,5	6
R_E	2	1	1,5	1
R_F	7	7	7	7
R_G	5	5	5	5
R_H	8	8	8	8

Bewertung der Analyse

Die dargestellte erweiterte Analyse hat gezeigt, dass sich die Priorisierungen von operationellen Knoten und deren dazugehörige Verbindungen von der Designphase bis zur Nutzungsphase ändern bzw. konkreter werden können. So können zum Beispiel zu Beginn der Entwicklung eines IT-Systems mehrere operationelle Netzknoten noch gleich gewichtet sein. Bei tatsächlicher Nutzung kristallisiert sich allerdings ein anderes Ergebnis heraus. Es ist somit erforderlich, kontinuierlich diese Art von Analysen durchzuführen, um den Gefahren des Verlustes der Vertraulichkeit und Integrität zu begegnen. Nach einer Analyse ist es möglich, die getroffenen Sicherheitsmaßnahmen zu überprüfen und gegebenenfalls anzupassen.

6.5. Anonymisierung

Eine Sicherheitsanalyse, die sich auf ungefilterte eingestufte Daten stützt, erzeugt wieder eine eingestufte Instanz. Sie kann selten direkt an Dritte weitergegeben werden. Die Herausforderung in der täglichen Arbeit besteht daher darin, solche Daten auszutauschen, ohne die Offenlegung von klassifizierten Infrastrukturdetails auf der einen Seite zu gefährden und auf der anderen Seite den Nutzen des Aufwands nicht zu sehr einzuschränken.

Während der DFDsec-Ansatz dazu beiträgt, dass bereinigte Ergebnisse noch nützlich sind, bleibt die Frage offen, ob das Wissen über die klassifizierte Infrastruktur wirklich

geschützt ist. Es reicht nicht aus, den veröffentlichten Datensatz zu reduzieren und auf das Beste zu hoffen, sondern es muss eine objektive und wiederholbare Überprüfung durchgeführt werden, um diese Eigenschaft zu validieren.

Eine Möglichkeit zur Bewertung eines Anonymisierungsansatzes wurde von Samarati und Sweeney beschrieben. Ihr Modell heißt *k-Anonymität*. Ein veröffentlichter Datensatz wird als k-anonym deklariert, wenn identifizierende Informationen eines einzelnen Knotens, wie z. B. ein Servername, ununterscheidbar von mindestens k-1 ähnlichen Entitäten ist [121], [132]. Ein größeres k bedeutet einen höheren Grad an Anonymisierung. Das Ergebnis ist die Überzeugung von 1/k, dass eine korrekte Verknüpfung von korrelierendem klassifiziertem Wissen nicht möglich ist.

Das Modell wurde später um die Idee der l-Diversität (l-diversity) [92] und t-Verbundenheit (t-closeness) [88] erweitert. Diese Erweiterungen und der ursprüngliche Ansatz verhindern die Möglichkeit einer Deanonymisierung, welche sich aus einem unsortierten Matching-Angriff (unsorted matching attack), temporalen Angriffen oder komplementären Release-Angriffen (complementary release attacks) ergeben könnten [59]. Diese Erweiterungen beheben spezifische Probleme der k-Anonymität, wie den Homogenitätsangriff (Homogeneity attacks) oder den Angriff mit Hintergrundwissen (background knowledge attack) [92].

Für den in diesem Kapitel beschriebenen Ansatz wird die *k-Anonymität* verbessert, indem 5 der 7 ursprünglichen Datenspalten weglassen werden. Nur der sendende Server und der empfangende Server bleiben in ihrer ursprünglichen Bedeutung erhalten. k wird hier durch die geringste Anzahl von Serververbindungen zwischen zwei Servern im Nachrichtenflussdatensatz bestimmt. Aus der Sicht von Anonymisierungsangriffen deckt der Ansatz dieser Arbeit die folgenden Sicherheitsbedrohungen ab:

Beim *unsortierten Matching-Angriff* werden die Datenspalten getrennt und in der gleichen Reihenfolge offenbart. Auf diese Weise können die ursprünglichen Daten wiederhergestellt werden. Dieser Angriff wird in diesem Konzept verhindert, indem nur zwei der ursprünglichen Spalten veröffentlicht werden. Darüber hinaus basiert die Sortierung in der veröffentlichten Diagrammdarstellung auf der Nachrichtenfrequenz von Netzknoten zu Netzknoten, welche variieren kann. Dadurch ändert sich die Reihenfolge der Einträge automatisch.

Der *temporale Angriff* nutzt die Tatsache aus, dass Datensammlungen dynamisch sind. Das Hinzufügen, Ändern oder Entfernen von Einträgen kann die k-Anonymität des Analyseergebnisses beeinflussen. Dieser Angriff wird verhindert, indem die gemeinsamen Attribute (Pseudonym-Servernamen) bei der Veröffentlichung aktualisierter oder erweiterter Analyseergebnisse nicht geändert werden. Nachfolgende Versionen eines DFDsec-Diagramms müssen daher die gleichen Server-Pseudonyme wie bisher wiederverwenden.

Im Falle des *komplementären Angriffs* können verschiedene Releases von Teilmengen der Basisdatei zu unterschiedlichen Anonymisierungen führen, welche jeweils der k-Anonymität entsprechen. Durch die Kombination der jeweiligen Publikationen wird die k-Anonymität wieder aufgehoben. Dieser Angriff wird verhindert, indem alle nachfolgenden Versionen eines Analyseergebnisses auf der Grundlage des ursprünglichen Ergebnisses erstellt werden. Dies wird durch die Verwendung immer gleicher Spaltenattribute (Empfangs- und Sende-Server) und Spalteninhalte für unveränderte Daten gewährleistet.

Die einzige Änderungsvariable für die Aktualisierung von DFDsec sollte die Nachrichtenfrequenz und die Menge der zu modellierenden Prozesse sein.

Homogenitätsangriffe basieren auf der Idee, dass es Gruppen von Datenelementen, hier Modellelemente, gibt, welche alle das gleiche sensible Attribut haben. Dieser Angriff wird in diesem Konzept verhindert, indem die sensiblen Attribute (z. B. Nachrichten-ID oder Servername) für das endgültige veröffentlichte Modell einfach nicht verwendet werden. Zusätzliche Vielfalt, wie in [92] vorgeschlagen, ist daher nicht erforderlich.

Der *Angriff mit Hintergrundwissen* nutzt die Tatsache aus, dass ein Angreifer trotz k-Anonymität durch zusätzliches Wissen Dateninhalte eindeutig zuordnen kann. In diesem Ansatz wird Hintergrundwissen dadurch verhindert, dass alle sensiblen Attribute weggelassen werden und die eingestuften Daten physisch von den öffentlichen Daten getrennt sind. Es werden nur Daten veröffentlicht, welche für den externen Support erforderlich sind, nach dem in [104] beschriebenen Filter-in-Prinzip.

6.6. Zusammenfassung

In diesem Kapitel wurde ein Ansatz zur Identifizierung von Verletzungen der Informationsraumgrenzen mittels automatisierter Nachrichtenaustauschanalyse diskutiert. Die Bestimmung kritischer Informationsflüsse führt zur Identifizierung sensibler operationeller Netzknoten, die hochriskante Ziele für Sicherheitsangriffe darstellen. Da die Rohdatenprotokolle und die Analyseergebnisse selbst eingestufte Informationen sind, wurde ein einfacher Anonymisierungsansatz für die Originaldaten vorgeschlagen. Dabei wurde das Potenzial bekannter Anonymisierungsangriffe diskutiert.

Die Analyse von Daten eines Jahres aus der Praxis zeigte, dass das untersuchte System bei guter Gesundheit ist. Verletzungen der Informationsraumgrenzen konnten nicht festgestellt werden. Die Visualisierung mit reduzierten DFDsec-Diagrammen erwies sich als eine praktikable Methode für Regierungsorganisationen mit hohen Anforderungen an den Datenschutz. Die Verwendung anonymisierter DFDsec-Modelle ermöglicht den Austausch der Analyseergebnisse mit externen Sicherheitsberatern und Führungskräften, die eine niedrigere Sicherheitsklassifizierung aufweisen.

Im folgende Kapitel werden die hier genutzten Protokolldaten für weitergehendende Analysen verwendet. Die Daten werden so reduziert, dass aus einer reinen Offline-Analyse eine Online-Analyse ermöglicht wird, mit der z. B. eine Anomalieerkennung durchgeführt werden kann. Dabei wird unter anderem zeitliche Kausalität des Nachrichtenaustauschs berücksichtigt.

7. Grobe Protokolle - Ein Ansatz zur Datenreduktion für Protokolldateien

Im letzten Kapitel wurde eine automatisierte Nachrichtenaustauschanalyse zur Identifizierung von Verletzungen der Informationsraumgrenzen präsentiert. Unter Nutzung des Sicherheitsdatenflussdiagramm (DFDsec) aus Kapitel 5 wurden die Ergebnisse der Analyse von Rohdatenprotokollen anonymisiert dargestellt. In diesem Kapitel wird sich mit der Frage beschäftigt, wie man sehr große Mengen an Protokolldaten so reduzieren kann, dass die zeitnahe Verarbeitung erfolgen und trotzdem das unbefugte Eindringen in Informationsräume mit ausreichender Sicherheit festgestellt werden kann.

Moderne, skalierbare Informationssysteme erzeugen einen konstanten Strom von Protokolleinträgen, um ihre Aktivitäten und ihren aktuellen Zustand zu beschreiben. Diese Daten werden zunehmend für die Online-Anomalieanalyse verwendet, so dass Zuverlässigkeitsprobleme, wie z. B. Sicherheitsvorfälle, im laufenden Betrieb erkannt werden können. Aufgrund der ständigen Skalierung vieler solcher Systeme ist die Menge der verarbeiteten Protokolldaten ein wesentlicher Aspekt, der bei der Wahl eines Anomalie-Erkennungsansatzes zu berücksichtigen ist. In diesem Kapitel wird eine neue Idee zur Reduzierung von Protokolldaten vorgestellt, welche als „Grobe Protokolle“ bezeichnet werden. Dabei wird die Theorie der groben Mengen (rough sets) nach Pawlak [106] zur Reduzierung der Anzahl der Attribute verwendet, die in Protokolldaten zur Darstellung von Ereignissen im System gesammelt werden. Der Ansatz wurde in einer großen Fallstudie getestet. Die Experimente zeigten, dass die von diesem Ansatz vorgeschlagenen Möglichkeiten zur Datenreduktion auch dann gültig bleiben, wenn die Protokollinformationen aufgrund von Anomalien im System geändert werden.

Die Struktur dieses Kapitels ist wie folgt: Abschnitt 7.1 beschreibt das zugrunde liegende Problem und die Grundidee des Ansatzes. Die Abschnitte 7.2 und 7.3 präsentieren verwandte Arbeiten, insbesondere im Hinblick auf die gewählte Unsicherheitstheorie. In Abschnitt 7.4 wird die Vorgehensweise skizziert, die auf Log-Daten mit der Methode von Groben Protokollen angewendet wird. Es folgt der Abschnitt 7.5, der das Ergebnis der Fallstudie zeigt. Abschnitt 7.6 behandelt speziell die Stabilität des gewählten Ansatzes. Das Kapitel schließt mit einer kurzen Zusammenfassung im Abschnitt 7.7.

7.1. Problem und Grundidee

In einer immer komplexer werdenden modernen Informationstechnologie (IT)-Landschaft werden immer mehr Systeme für neue oder verbesserte Funktionalität und Effizienz verbunden. Dieser unvermeidliche Trend macht die Online-Sicherheitsaufsicht zu einer Herausforderung in allen IT-Systemen von Unternehmen und Behörden. Mit

dem immer größer werdenden Umfang und der zunehmenden Komplexität dieser Systeme ist es heute eine gängige Praxis, automatisierte Sicherheitsabwehrmechanismen aufzubauen, welche autonom und konstant im Hintergrund arbeiten. Diese Mechanismen überwachen das Systemverhalten, erkennen Anomalien und reagieren entsprechend mit Alarmen oder automatisierten Gegenmaßnahmen.

Jede Anomalie-Erkennung erfordert einen konstanten Strom von Systemzustandsinformationen, die auf verdächtige Merkmale analysiert werden müssen. Ein gemeinsames Datenformat für diese Art von Informationen sind Protokolldateien, eine textuelle Darstellung relevanter Systemereignisse, welche üblicherweise von der Serversoftware und dem Betriebssystem selbst erzeugt werden. Die Menge der Protokolldaten, die in großen Systemen für diese Zwecke gesammelt werden, ist mittlerweile ein relevantes Thema für sich.

In diesem Kapitel wird eine neue Methode zur Reduzierung der Menge der Protokolldaten vorgeschlagen, welche für die Online-Analyse und die Erkennung von Anomalien benötigt werden. Dabei wird auf einen Ansatz der Unsicherheitstheorie namens *Grobe Mengen* gebaut, der es ermöglicht, Logdaten zu verkleinern, indem grob redundante Attribute in Logfile-Einträgen entfernt werden. Die entfernbaren Attribute werden durch eine einmalige Analyse vorhandener Protokolldaten identifiziert, welche die logische Beziehungen zwischen den im Systemprotokoll aufgezeichneten Systemattributen findet. Grobe Attribute werden dann zu einem repräsentativen Attribut zusammengefasst. Das Ergebnis sind „Grobe-Protokolle“, die das Systemverhalten auf eine unscharfe, aber dennoch repräsentative Weise beschreiben. Der Ansatz wird mit einem umfangreichen Datensatz aus der Praxis getestet.

7.2. Anomalieerkennung

Die Erkennung von Anomalien bezieht sich auf das Problem, Muster in Daten zu finden, welche nicht dem erwarteten Verhalten entsprechen. Die zu untersuchenden Daten lassen sich in Sequenzdaten (z. B. Zeitseriendaten, Proteinsequenzen und Genomsequenzen), räumliche Daten (Fahrzeugverkehrsdaten oder ökologische Daten) und Diagrammdaten unterscheiden. Es gibt auch verschiedene Arten von Anomalien: Punktanomalien, Kontextanomalien und kollektive Anomalien [30].

Das Auffinden von Ausreißern oder Anomalien in Daten wurde bereits im 19. Jahrhundert statistisch untersucht [47]. Im Laufe der Jahre wurden verschiedene Anomalie-Erkennungstechniken (klassifikationsbasiert, basierend auf dem nächtsgelegenen Nachbarn, clusterbasiert, statistisch, informationstheoretisch und spektral) in verschiedenen Forschungsbereichen entwickelt, wie z. B. Einbruchserkennung (intrusion detection), Betrugserkennung, medizinische Anomalieerkennung, Erkennung von Industrieschäden, Bildverarbeitung, textuelle Anomalieerkennung und Sensornetzwerke [30].

Die Verwendung von Protokolldateien zur Erkennung von Anomalien in IT-Systemen wurde in mehreren Bereichen untersucht, insbesondere im High-Performance Computing mit zehntausenden Knoten [101]. Diese Versuche beinhalten die Berücksichtigung von Message-Timing [90], Data-Mining-Ansätzen [91], [130], [149], [102], Pattern-Learning-

Konzepten [69] oder graphenbasierten Ansätzen [119].

Um riesige Mengen von Systemprotokolldateien zu reduzieren und zu analysieren, gibt es verschiedene bekannte Methoden wie die Mustererkennung [69], Data-Mining [130], [149], [158], Clustering [148], Support-Vektor-Maschinen [12], [74], Entscheidungsbaum-Lernen [113] oder Normalisierung [32], [80], [122].

7.3. Grobe Mengen

Dieser Ansatz zur Generierung von groben Protokollen basiert auf dem größeren Forschungsfeld des *unperfekten Wissens*. Es wird von verschiedenen Wissenschaften untersucht. Philosophen, Mediziner, Logiker, Mathematiker und Informatiker verwenden entsprechende mathematische Theorien, wie die bekannte Fuzzy-Set-Theorie [160] oder die Dempster-Shafer-Theorie [125], um unsicheres Wissen auszudrücken.

Die Theorie der groben Mengen (rough sets) wurde von Pawlak [106] erfunden und wird inzwischen in verschiedenen Bereichen eingesetzt, wie z. B. bei der Vorhersage von Flugzeugkomponentenausfällen [109]. Im Gegensatz zu anderen Theorien sind in der Theorie der Groben Mengen keine zusätzlichen oder vorläufigen Informationen über Daten erforderlich, wie z. B. Wahrscheinlichkeiten, Wahrscheinlichkeitszuweisungen oder Möglichkeitsdeklarationen [107].

Ausgangspunkt für grobe Mengen ist die klassische mathematische Idee von Mengen und Elementen. In der Standardschulmathematik ist jedes Element Teil einer Menge oder nicht. Die Forschung über unvollkommenes Wissen lockert nun diese Idee und definiert den Begriff der Teilmitgliedschaft eines Elements zu einer Menge. Dies ist sehr hilfreich, wenn es beispielsweise um vage Konzepte wie die menschliche Sprache (mehr oder weniger ein Mitglied) oder medizinische Symptome geht.

Die Theorie der groben Mengen stellt jede Informationsmenge als Entscheidungstabelle dar. Die Spalten repräsentieren die Attribute ($a \in A$) des zu untersuchenden Systems, die Zeilen sind verschiedene Instanzen ($i \in I$) von Attributwerten, die im System aufgetreten sind.

Jedes Attribut ist entweder ein Bedingungsattribut oder ein Entscheidungsattribut. Ein einfaches Beispiel wäre eine Reihe von medizinischen Symptomen, die als Bedingungsattribut behandelt werden, während die Krankheit als einziges Entscheidungsattribut angesehen wird. Mit unvollkommenem Wissen kann es vorkommen, dass verschiedene oder sogar widersprüchliche Symptome für eine Reihe von Instanzen bzw. Patienten zu derselben Krankheit führen. Es kann auch vorkommen, dass die gleichen Symptome für verschiedene Krankheiten in verschiedenen Reihen stehen. Ein anderes Beispiel wurde durch Tröger [142] für die Verlässlichkeitsanalyse eines Web-Servers beschrieben. Die Bedingungsattribute sind die Beobachtungen, ob es sich um eine große Anfrage an den Webserver handelt und wie dieser ausgelastet ist. Das Entscheidungsattribut ist die Feststellung, ob der Server infolge der Bedingungen abgestürzt ist.

Ein Entscheidungsattribut hängt vollständig von einer Reihe von Bedingungsattributen ab, wenn alle Entscheidungsattributwerte eindeutig durch alle Bedingungsattributwerte beschrieben werden. Wenn nur ein Teil der Entscheidungsattribute durch die

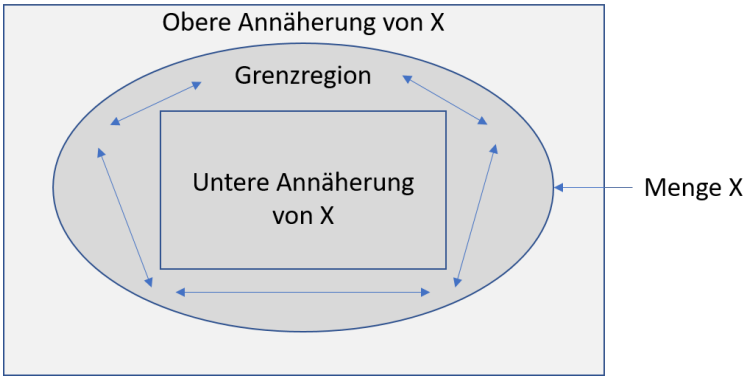

Abbildung 7.1.: Grobe Mengen

Bedingungsattribute beschrieben werden kann, ist die Abhängigkeit unvollständig.

Instanzen, welche die gleichen Besonderheiten aufweisen, gelten als ununterscheidbar und bilden Äquivalenzklassen, die als *elementare Mengen* bezeichnet werden. Durch die Identifizierung von elementaren Mengen können Informationsmengen vor der weiteren Analyse reduziert werden. Dies ist ein zeit- und speicherintensiver algorithmischer Ansatz, welcher für die Reduzierung von Protokolldateien nicht geeignet ist.

Einige Instanzen (Zeilen) in der Entscheidungstabelle können zu demselben Wert im Entscheidungsattribut führen. Dies wird als Konzept X bezeichnet, z. B. eine bestimmte Krankheit. Die untere Annäherung von X ist eine Teilmenge von Instanzen, welche sicher die Bildung von Zielentscheidungsattributwerten beschreibt. Die obere Annäherung von X ist eine Teilmenge, die alle Möglichkeiten beschreibt, die Zielentscheidungsattributwerte zu erreichen.

Der Unterschied zwischen unterer und oberer Annäherung ist die Grenzregion (siehe Abbildung 7.1). Eine leere Grenzregion zeigt, dass die grobe Informationsmenge *crisp* ist, was bedeutet, dass es keine Unsicherheit in der Entscheidungstabelle für die gegebenen Entscheidungsattribute gibt und dass die Informationsmenge genau ist. In allen anderen Fällen wird die Menge als *grob* bezeichnet und die untere und obere Annäherung sind, wie in Abbildung 7.1 dargestellt, ungleich (erkennbar an dem durch Pfeile gekennzeichneten Bereich).

Für eine gegebene grobe Menge ist es möglich, den *Abhängigkeitsgrad* von Entscheidungsattributen von einer Menge von Bedingungsattributen zu berechnen. Diese Analyse stützt sich wiederum auf das Wissen über die unteren und oberen Annäherungen. Der Abhängigkeitswert, welche zwischen 0 und 1 ist, beschreibt den Anteil der Entscheidungsattributwerte, welche durch die Bedingungsattributwerte richtig klassifiziert werden können. Eine Attributabhängigkeit von 1 zeigt, dass jeder Entscheidungsattributwert eindeutig von den Werten der Bedingungsattribute abgeleitet werden kann. Dieses spezielle Konzept ist die Grundlage für den hier dargestellen Ansatz von groben Protokollen.

7.4. Beschreibung des Ansatzes

Dieser Ansatz basiert auf der Idee, Systemprotokolldateien als Entscheidungstabelle im Sinne der Theorie der groben Mengen zu behandeln. Es wird angenommen, dass die verschiedenen gemeinsamen Attribute in Protokolldateien, wie Zeitstempel oder Dringlichkeit, eine gewisse vage Korrelation zueinander aufweisen.

Ein einfaches Beispiel sind die Log-Einträge für einen Mailserver, der periodisch einen Newsletter an eine Reihe von Empfängern sendet. Die kontaktierten Ziel-Mailserver, die Ursprungs-E-Mail-Adresse und vielleicht sogar der Zeitpunkt des Versands werden sicherlich grob miteinander korrelieren. Es wird keine klare Beziehung geben, da die Liste der Empfänger oder der Zeitpunkt des Sendens leicht variieren kann, aber ein absichtlicher ungenauer Blick auf die Protokolldaten kann einige wahrhaftige Verbindungen offenbaren.

Unter der Annahme, dass einige der Attribute „nah genug“ zueinander sind, kann nun entschieden werden, solche grob redundanten Attribute aus den Protokolldaten zu entfernen. Die Motivation für eine solche Datenreduktion können Techniken zur Erkennung von Anomalien sein, wie z. B. maschinelles Lernen. Wichtig dabei ist, dass die Idee der groben Protokolle nicht auf die Art der Daten zugeschnitten sein darf, da sie nur auf die Symbole wirkt, aus denen sich die Attributwerte zusammensetzen. Es ist daher möglich, eine bestimmte Menge von Protokolldateien aus beliebigen Systemen auf schwache Attributabhängigkeiten zu analysieren und redundante Informationen vor der Weiterverarbeitung mit einer systemspezifischen Anomalievorhersagetechnik zu entfernen.

Der Ansatz funktioniert wie folgt:

- Kandidaten $a \in A$ für Kombinationen von Bedingungs- und Entscheidungsattributen basierend auf der Datensemantik finden.
- Zeilen mit unvollständigen Attributdaten entfernen.
- Diskretisierung von kontinuierlichen Werten durchführen, so dass Symbole abgeleitet werden können.
- Untere und obere Annäherung der groben Menge für jedes a bestimmen.
- Attributabhängigkeit für jedes a bestimmen.
- Attribute mit hohen Abhängigkeiten entfernen.

Wenn das untersuchte System ein regelmäßiges oder sogar zyklisches Verhalten aufweist, sollte es möglich sein, Kandidaten a mit hohen Abhängigkeitswerten zu finden, die über einen bestimmten Untersuchungszeitraum stabil bleiben. Für solche Kandidaten kann dann entschieden werden, Teile der Attribute aus dem Protokollinformationssatz zu entfernen, so dass die Datenmenge, welche für die Anomalieerkennung verwendet werden soll, deutlich kleiner wird.

7.5. Fallstudie

Der Ansatz wurde mit einem 10 GB Datensatz von Protokolldateien aus einem realen Server-Netzwerk getestet, das in einer sicherheitskritischen Regierungsumgebung arbeitet. Die Server tauschen intern Daten aus und führen Protokolle ihrer Aktivitäten zur Identifizierung von Sicherheitsvorfällen. Die Protokolle erstrecken sich über einen Zeitraum von 11 Monaten und enthalten 195.923.988 Log-Einträge. Jeder Eintrag bietet die gleiche Menge von Attributen: Datum, Uhrzeit, Sender, Empfänger, Art der Nachrichtenübertragung (Aktion, z. B. Senden/Empfangen) und Nachrichtengröße.

7.5.1. Implementierung der Analyse

Die Analyse der groben Mengen wurde mit dem RoughSets-Paket für System-R (R-Script) durchgeführt. Das Aufrufen des R-Scripts, das Zusammenführen der Ergebnisse und die graphische Darstellung der Ergebnisse wurden mit Python-Scripten realisiert. Um die Gesamtlaufzeit der Experimente von Tagen auf Stunden zu reduzieren, wurde eine benutzerdefinierte Parallelisierungsstrategie angewendet. Die Umsetzung der Parallelisierung erfolgt in Python über die Funktionen der multiprocessing Bibliothek. Diese sorgen dafür, dass mehrere Prozesse gleichzeitig ablaufen können. Zusätzliche hat die Pool-Funktion eine asynchrone Variante. Die Ergebnisse werden dabei zurückgeben, sobald sie berechnet worden sind und nicht, wenn alle Prozesse fertig sind. Dies hat den Vorteil, dass man unmittelbar mit den Ergebnisse weiter arbeiten kann, z. B. Berechnung von Statistiken (siehe Abschnitt 7.5.2). Die asynchrone Variante wurde durch den folgenden Funktionsaufruf implementiert:

```
pool.apply_async(run_analysis, (src_path, dest_path))
```

Die dabei integrierte Funktion „run_analysis“ startet dann das R-Script rekursiv über die zu untersuchende Verzeichnisstruktur. Das Analyse-Script besteht aus zwei Funktionen, welche die Abhängigkeiten berechnen:

```
function.dependency <- function(data, cond_attr, dec_attr,
nominal_attr)
function.fuzzydependency <- function(data, cond_attr,
dec_attr, nominal_attr)
```

Die Funktionen werden mit vier Variablen aufgerufen und führen die im Abschnitt 7.4 dargestellten Schritte des Ansatzes durch. Zunächst wird die Entscheidungstabelle über die Funktion „SF.asDecisionTable“ aufgebaut. Dies geschieht mit der Zuweisung:

```
decision.table <- SF.asDecisionTable(dataset = data,
decision.attr = dec_attr)
```

Danach werden die unvollständigen Daten durch die Funktion „MV.missingValueCompletion“ entfernt. Daraus entsteht eine aktualisierte Entscheidungstabelle. In R sieht dieser Schritt wie folgt aus:

```
indx = MV.missingValueCompletion(decision.table,
type.method = "deletionCases")
decision.table2 <- SF.applyDecTable(decision.table,
indx)
```

Nun folgend wird die Diskretisierung mit Hilfe der Funktion „D.discretization.RST“ durchgeführt. Die Diskretisierung erzeugt die Unterscheidbarkeit zwischen Objekten. Daraus entsteht erneut eine aktualisierte Entscheidungstabelle, welche im R-Quelltext wie folgt umgesetzt wird:

```
discr <- D.discretization.RST(decision.table2,
type.method = "unsupervised.quantiles",
nOfIntervals = 1)
decision.table3 <- SF.applyDecTable
(decision.table2, discr)
```

Jetzt folgt als nächster Schritt vor der Berechnung der oberen und unteren Annäherung sowie des Abhängigkeitsgrades, die Berechnung der elementaren Mengen, also der Instanzen, welche die gleichen Besonderheiten aufweisen und als nicht unterscheidbar gelten. Dies ist in R folgt durch die Funktion „BC.IND.relation.RST“ implementiert:

```
IND <- BC.IND.relation.RST(decision.table3,
feature.set = cond_attr)
```

Nun kann man durch die Bestimmung der elementaren Mengen die untere und obere Annäherung („BC.LU.approximation.RST“), also die „groben Mengen“ ermitteln. Damit ist es möglich die Abhängigkeitsgrade durch die Funktion „BC.positive.reg.RST“ zu berechnen. Diese wurde in R wie folgt implementiert.

```
roughset <- BC.LU.approximation.RST
(decision.table3, IND)
region = BC.positive.reg.RST
(decision.table3, roughset)
```

Die Funktion „function.fuzzydependency“ unterscheidet sich von der Funktion „function.dependency“ dahingehend, dass beim Schritt der Berechnung der elementaren Mengen andere Funktionen, nämlich die äquivalenten Fuzzy-Funktionen genutzt werden. Dabei wird jeder Zahlenwert in einen symbolischen Wert umgewandelt, um die Unterscheidbarkeit zwischen Objekten zu ermöglichen [44]. Für alle Kandidaten a, die das Größenattribut enthielten, war diese Umwandlung erforderlich. In R sieht die Implementierung dieser Schritt wie folgt aus:

```
IND.cond <- BC.IND.relation.FRST
(decision.table3, attributes = cond_attr)
IND.dec  <- BC.IND.relation.FRST
(decision.table3, attributes = dec_attr)
roughset <- BC.LU.approximation.FRST
```

```
(decision.table3, IND.cond, IND.dec)
region = BC.positive.reg.FRST
(decision.table3, roughset)
```

Konkret für den vorliegenden Anwendungsfall bedeutet dies, dass in einem ersten Schritt die Kandidaten $a \in A$ für Bedingungs- und Entscheidungsattributkombinationen in dem Anwendungsszenario definiert worden sind. Die Spalte Datum und Uhrzeit kann zusammen als Zeitstempel betrachtet werden, der jeden einzelnen Protokolleintrag eindeutig identifiziert. Es ist möglich, einen Zeitstempel als Bedingungsattribut in das Kandidaten-Tupel aufzunehmen. Dies würde es ermöglichen, zeitabhängige Entscheidungsattribute zu identifizieren. Allerdings bestand jedoch das praktische Problem, dass 10 GB Logdaten einfach zu viel sind für eine der bestehenden Analyse-Implementierungen von groben Mengen. Daher wurde entschieden, die Zeitstempelspalten aus der Analyse der groben Mengen in der Fallstudie zu entfernen. Stattdessen wurden diese Informationen verwendet, um die Protokolldaten in Blöcke pro untersuchte Stunde aufzuteilen. Für jede Stunde in den insgesamt 11 Monaten wurden die Attributabhängigkeiten für alle ausgewählten Kandidaten berechnet und so konnte festgestellt werden, ob sich die Attributabhängigkeiten im Laufe der Zeit ändern.

Die restlichen Attribute waren Sender, Empfänger, Aktion (z. B. Senden/Empfangen) und Größe. Basierend auf Gesprächen mit den zuständigen Administratoren über die Systemsemantik wurden folgende Kandidaten ($C1$ - $C10$) für Bedingungsattribute und deren abhängiges Entscheidungsattribut entwickelt:

- $C1$: Aktion ⇒ Empfänger
- $C2$: Sender ⇒ Aktion
- $C3$: Sender ⇒ Empfänger
- $C4$: Aktion, Empfänger ⇒ Sender
- $C5$: Sender, Aktion ⇒ Empfänger
- $C6$: Sender, Empfänger ⇒ Aktion
- $C7$: Sender ⇒ Größe
- $C8$: Sender, Empfänger ⇒ Größe
- $C9$: Sender, Empfänger, Aktion ⇒ Größe
- $C10$: Empfänger ⇒ Größe

7.5.2. Ergebnisse der Analyse

In Abbildung 7.2 sind die Abhängigkeitswerte für die verschiedenen Attributkombinationskandidaten $C1$ bis $C10$ im Zeitverlauf dargestellt. Die y-Achse stellt dabei die Abhängigkeitswerte, welche sich zwischen 0 und 1 befinden können, dar. Die x-Achse enthält die untersuchten Monate von Januar bis November.

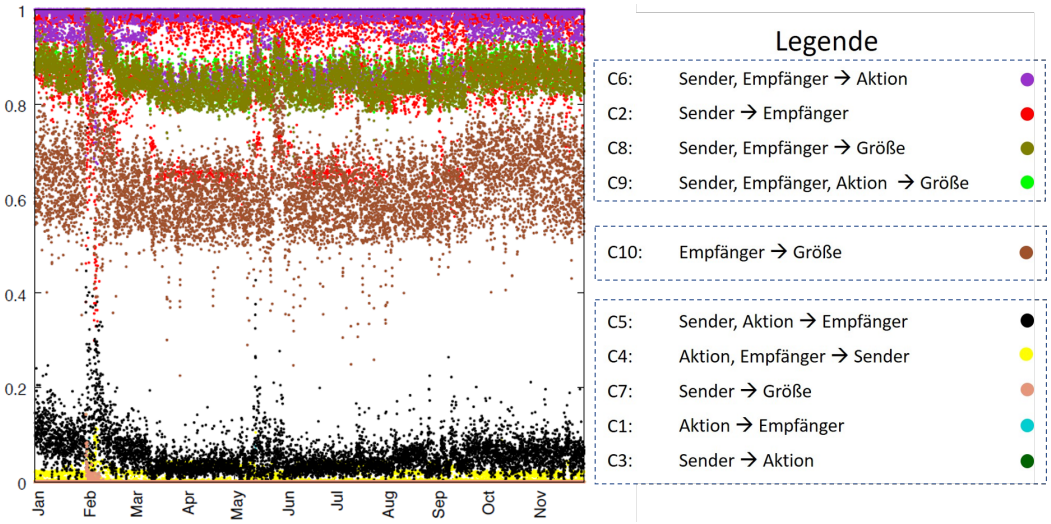

Abbildung 7.2.: Attributabhängigkeiten über die Zeit

Die numerischen Ergebnisse zeigen, dass für $C1$, $C3$, $C4$, $C5$ und $C7$ fast keine Attributabhängigkeit angegeben ist, so dass sie nicht aus dem Datensatz entfernt werden können. Dies sind die Punktwolken im unteren Bereich der Abbildung 7.2.

Für $C10$ wird eine mittlere Attributabhängigkeit über die Zeit angegeben. Dies ist die braune Punktwolke im mittleren Bereich der Abbildung 7.2. Der Mittelwert der Abhängigkeit für $C10$ beträgt 0,621, mit einer Standardabweichung von 0,078. In solchen Fällen hängt es vom Druck zur Datenreduktion ab, ob ein solcher Abhängigkeitswert hoch genug ist, um z. B. die Empfängerinformationen aus allen Protokolldaten zu entfernen.

Für die Daten der Fallstudie war es möglich, einige hohe Attributabhängigkeiten mit den Kombinationen $C2$, $C6$, $C8$ und $C9$ zu identifizieren. In der Abbildung sind diese Abhängigkeiten im oberen Teil dargestellt.

Die größten Abhängigkeiten im Zeitablauf sind für $C6$ angegeben. Diese haben einen Mittelwert von 0,975 und eine Standardabweichung von 0,043.

Für $C2$ ist der Mittelwert 0,890 und die Standardabweichung 0,104. Diese Kombination von Attributen zeigt auch eine große Streuung, der kleinste Wert beträgt 0,299 und der größte Wert 0,998.

Die drittgrößte Abhängigkeit ist $C9$. Der Mittelwert dieser Kombination ist 0,860 und die Standardabweichung 0,038. Die Abhängigkeit ist über den gesamten Zeitraum sehr konstant, nur im Februar ist sie etwas höher. Hier ist der Mittelwert 0,908 und die Standardabweichung 0,052.

Die Untersuchung von Attributabhängigkeiten und deren transitiven Beziehungen über das ganze Jahr hinweg führt zu dem Schluss, dass die Kombination von Sender und Empfänger ein sehr guter Indikator für die Art einer Datenübermittlung ist, insbesondere im Hinblick auf die Art und Menge der übertragenen Daten. Es wäre daher sinnvoll, die **Größe** und die **Aktion**sinformationen aus den Protokolldaten herauszu-

lassen, da die Kombination von Sender- und Empfängerinformationen etwa die gleiche Informationsmenge darstellt. Ein Anomalie-Erkennungsmechanismus könnte sich auf diese Attributkombination konzentrieren und gleichzeitig andere Teile zur Verbesserung der eigenen Leistung weglassen.

7.6. Stabilität mit Anomalien

Da die ursprüngliche Motivation für dieses Kapitel die Datenreduktion zur Online-Anomalieerkennung war, wird es zu einer interessanten Frage, ob sich die Attributabhängigkeiten ändern, wenn die Protokolldaten beginnen, Hinweise für einen solchen Fall zu enthalten.

Es wurden drei Anomalie-(oder Fehler-)Injektionsszenarien erstellt. Alle drei Szenarien stammen von realen Sicherheitsbedrohungen für das zu untersuchende System:

- Neue Nachrichtenübertragung zwischen bekannten Sendern und Empfängern
- Neue Sender- oder Empfänger
- Änderungen der übertragenen Datenmenge für bestehende Verbindungen

Die Szenarien decken dabei eine Vielzahl von Bedrohungen, welche im Kapitel 4 und im Anhang A dargestellt sind, aus verschiedenen Teilbereichen der Organisation ab. So sind die Bereiche Infrastruktur, IT-System, Netze, Anwendungen und Informationsräume betroffen. Folgende Bedrohungen aus der „Phase 2: Angriff auf das Ziel“ können dabei beispielsweise Ursache für diese Angriffszenarien sein:

- Infrastruktur
  - Einsatz gefälschter Komponenten (Verkabelung) [16]
  - Wiretapping [13], [110]
- IT-System
  - Eindringen in IT-Systeme [16]
  - Missbrauch von IT-Systemen [16], [43], [112], [84]
- Netze
  - Eindringen durch Netzwerkverbindungen [13], [43]
  - Hijacking von Netz-Verbindungen [16]
- Anwendungen
  - Kryptographieangriffe [16], [43], [70], [112], [83]
  - Manipulation von Software [16], [5], [153]
  - Schadsoftware/-programme [1], [16], [11], [13], [35], [43], [56], [112], [81], [83], [94], [66], [65], [110], [120]

  - Spoofing/Identitätsdiebstahl [16], [5], [35], [43], [70], [112], [81], [65], [133], [120], [153]
  - E-mail [16], [43], [112], [81], [83], [94], [110]
    - Mitlesen von E-mails [16]
    - Vortäuschen eines falschen Absenders [16]

- Informationsräume
  - Informationsfluss von oben (z. B. GEHEIM) nach unten (z. B. Öffentlich) [6]
  - Überwindung der physikalischen Grenzen zwischen Informationsräumen
  - Unbefugtes Eindringen in Informationsräume
  - Verändern von Daten während der Übertragung [84]
  - Verstöße gegen den Grundsatz „Kenntnis nur wenn nötig“

Ebenfalls spielen Bedrohungen aus der „Phase 3: Ausweitung der Rechte“ eine Rolle:

- Manipulation von IT-Systemen (Teilbereich IT-System) [16], [5], [43]
- Nutzung von internen Netzverbindungen für laterale Bewegungen (Teilbereich Netze) [43]
- Manipulation der Geheimhaltungsgrade (Teilbereich Informationsräume)

Bei den verschiedenen Angriffsszenarien wurden zwei Monate, Februar und April, mit genau dem gleichen Analyseansatz (vgl. Abschnitt 7.4) untersucht. Allerdings wurden modifizierte Protokolldateien erzeugt, die die jeweilige Anomalie enthielten.

7.6.1. Anomalieszenario „Duplikation“

Im ersten Szenario werden einige Datenübertragungen von einem Angreifer dupliziert, um diese Daten auf einem gefährdeten Einzelrechner im System zu sammeln. In einer ersten Version (V1) dieses Szenarios werden alle ausgehenden Daten von einem bestimmten Host (mit beliebigem Empfänger) zusätzlich auf einen kompromittierten, aber bekannten zweiten Host übertragen. Mit dieser Modifikation wurden insgesamt 271.576 neue Log-Einträge erzeugt. In der zweiten Version (V2) des Duplikationsszenarios werden die ausgehenden Daten nur dann auf den kompromittierten Host kopiert, wenn sie für einen bestimmten Empfänger bestimmt sind. Diese Änderung führte zu 170.140 neuen Log-Einträgen.

Das Ergebnis des ersten Szenarios ist, dass sich die Abhängigkeiten für den Anwendungsfalldatensatz entweder gar nicht oder nur geringfügig ändern. Dies ist in der Abbildung 7.3 für den Monat Februar und Abbildung 7.4 für den Monat April dargestellt. Die y-Achse umfasst die Abhängigkeitswerte zwischen 0 und 1 und die x-Achse die Tage des untersuchten Monats. Hierbei ist erkennbar, dass sich weiterhin für $C1$, $C3$, $C4$, $C5$ und $C7$ fast keine, für $C10$ mittlere und für $C2$, $C6$, $C8$ und $C9$ hohe Attributabhängigkeiten

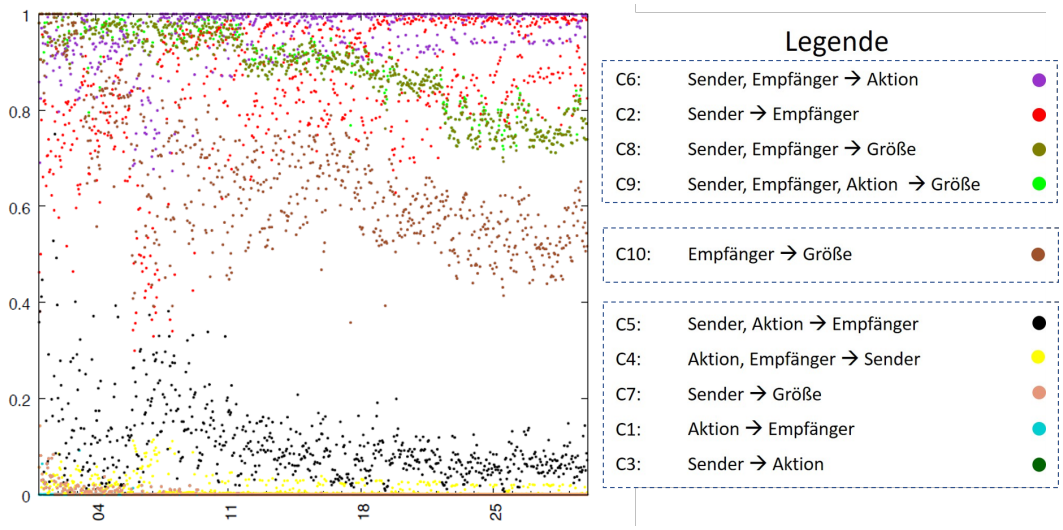

Abbildung 7.3.: Anomalieszenario „Duplikation“, Version 1, Februar

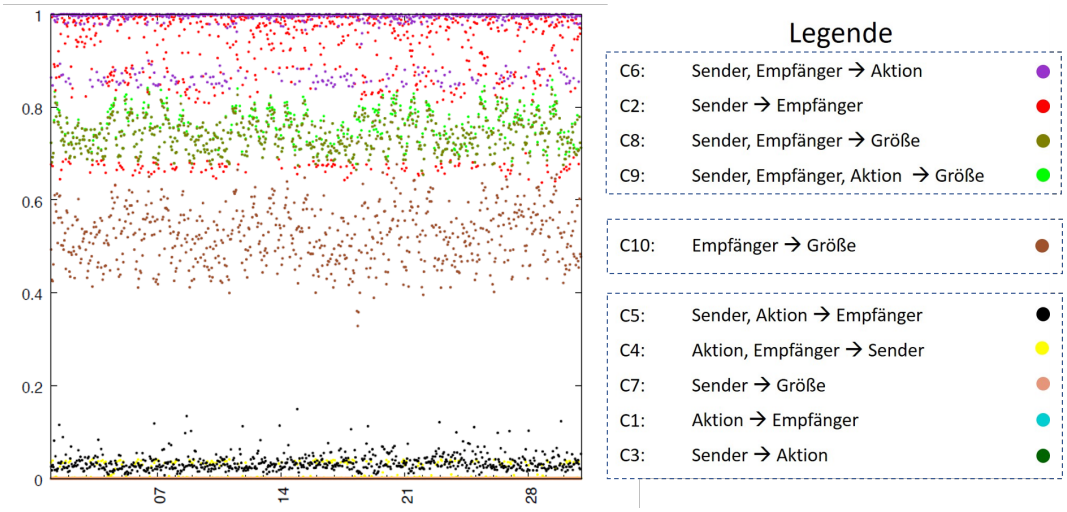

Abbildung 7.4.: Anomalieszenario „Duplikation“, Version 1, April

feststellen lassen. Dabei ist auffallend, dass im Februar die gleichen Schwankungen der Attributabhängigkeit vorhanden sind, wie sie auch in Abbildung 7.2 für die unveränderten Protokolldaten zu sehen sind.

Nennenswerte Änderungen ergaben sich für die Kandidaten $C8$, $C9$ und $C10$. $C8$ und $C9$ sind aus dem oberen Bereich und $C10$ ist aus dem mittleren Bereich der Abbildungen 7.3 und 7.4. Die numerischen Änderungen wurden daher in der Tabelle 7.1 beschrieben. In Spalte 1 der Tabelle befindet sich die betrachtete Zeitspanne und in Spalte 2 - 4 sind die Kandidaten $C8$ - $C10$. Die Berechnungen der durchschnittlichen Attributabhängigkeiten wurden dabei für die unmodifizierten Protokolldateien des ganzen Jahres, der Monate Februar und April sowie für die modifizierten Protokolldateien des Szenarios „Duplikation“ in den unterschiedlichen Versionen der Monate Februar und April berechnet.

Die Abhängigkeiten der Version 2 des Duplikationsszenarios sind höher als die der Version 1 (beispielsweise beträgt die Abhängigkeit für die Attributkombination „Sender, Empfänger ⇒ Größe“ im April Version 1: 0,741 und bei der Version 2: 0,771). Dies ist darauf zurückzuführen, dass weniger zusätzliche Verbindungen aufgebaut werden.

Das Gesamtbild der Attributabhängigkeit ändert sich aufgrund dieser Art von Anomalie nicht wesentlich (beispielsweise liegt die Abhängigkeit für die Attributkombination „Sender, Empfänger ⇒ Größe“ im ganzen Jahr (0,855) zwischen den Werten des Februars und des Aprils (unabhängig von den Versionen), so dass jede Entscheidung zur Datenreduktion, die auf Attributabhängigkeiten basiert, weiterhin möglich ist.

Tabelle 7.1.: Durchschnittliche Attributabhängigkeit im Anomalieszenario „Duplikation“

Zeitspanne	$C8$: Sender, Empfänger ⇒ Größe	$C9$: Sender, Empfänger, Aktion ⇒ Größe	$C10$: Empfänger ⇒ Größe
Ganzes Jahr, unmodifiziert	0,855	0,860	0,621
Februar, unmodifiziert	0,904	0,908	0,666
Februar V1, modifiziert	0,881	0,884	0,647
Februar V2, modifiziert	0,889	0,892	0,654
April, unmodifiziert	0,830	0,835	0,596
April V1, modifiziert	0,741	0,746	0,521
April V2, modifiziert	0,771	0,775	0,547

7.6.2. Anomalieszenario „Neuer Knoten“

Im zweiten Szenario wurde ein völlig neuer Netzknoten im System als Anomalie simuliert. Dabei wurde eine einzige, aber häufig verwendete Verbindung zwischen zwei Maschinen ausgewählt und einen Man-in-the-Middle-Knoten eingeführt, der den gesamten Datenverkehr abfängt. Insgesamt wurden durch diese Modifikation 206.332 Log-Einträge durch zwei neue Einträge ersetzt.

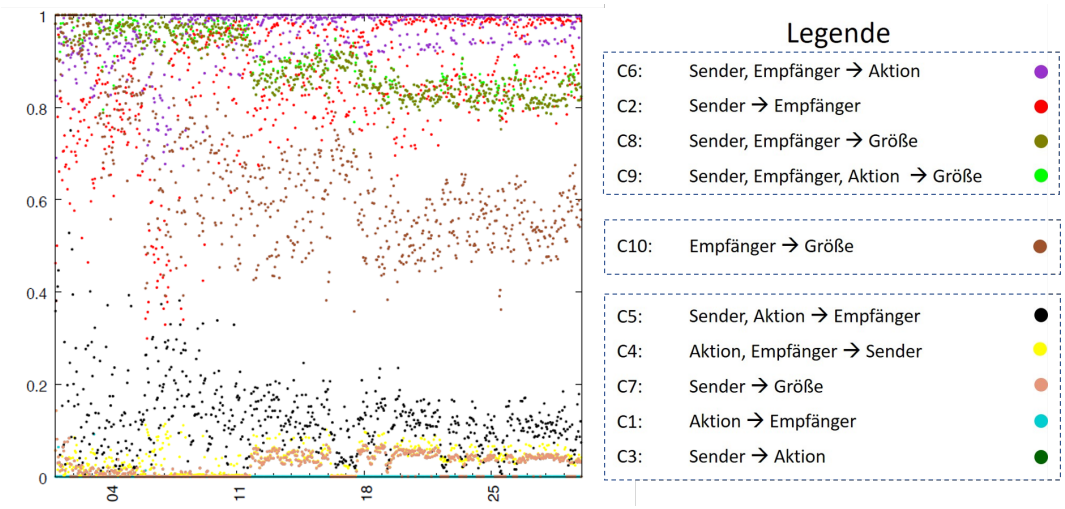

Abbildung 7.5.: Anomalieszenario „Neuer Netzknoten“, Februar

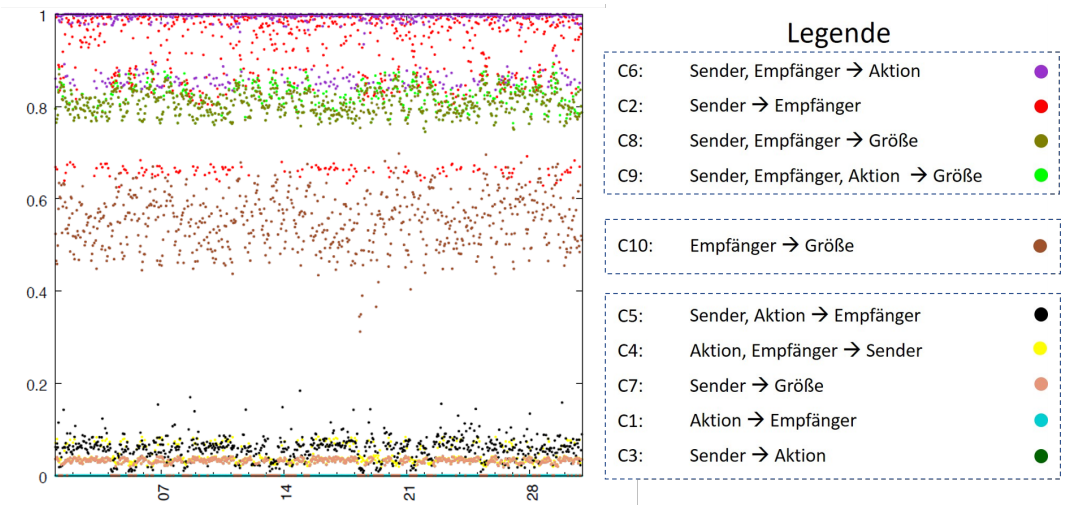

Abbildung 7.6.: Anomalieszenario „Neuer Netzknoten“, April

Dabei ist zu beachten, dass das Identifizieren von bösartigen neuen Netzknoten in Protokolldateien nicht in allen praktischen Systemen realistisch ist. Man könnte hier

davon ausgehen, dass die untersuchten Logdateien von Layer-7-Switches stammen, die tatsächlich neue Zwischenknoten im Rahmen ihrer Logging-Aktivitäten melden würden.

Das Ergebnis dieses Szenarios ist nahezu das gleiche wie im ersten. Die Abhängigkeiten für die $C1$ - $C10$ ändern sich entweder ein wenig oder gar nicht. Abbildung 7.5 und Abbildung 7.6 visualisieren die Ergebnisse.

Nennenswerte Änderungen ließen sich wieder für die Kandidaten $C8$ - $C10$ feststellen. Daher wurden diese in der Tabelle 7.2 festgehalten. Die Tabelle enthält für diese Kandidaten Berechnungen der durchschnittlichen Attributabhängigkeiten für die unmodifizierten Protokolldateien des ganzen Jahres, der Monate Februar und April sowie für die modifizierten Protokolldateien des Szenarios „Neuer Netzknoten“ der Monate Februar und April. Das Gesamtbild der Attributabhängigkeit ändert sich wegen dieser Anomalie ebenfalls nicht. Die Vergleichswerte das ganzen Jahres liegen weiterhin zwischen denen des Februars und des Aprils (z. B. Attributkombination „Sender, Empfänger ⇒ Größe“: Februar (0,888) > Ganzes Jahr (0,855) > April (0,808)). Für dieses Anomalieszenario ist allerdings erkennbar, dass die Änderung der Protokolldateien weniger Auswirkungen auf die Abhängigkeiten der Kandidaten $C1$ - $C10$ als das Anomalie-Szenario „Duplikation“ (vgl. Abschnitt 7.6.1) hatte. Dies zeigt sich insbesondere an den Werten des Aprils.

Tabelle 7.2.: Durchschnittliche Attributabhängigkeit im Anomalieszenario „Neuer Netzknoten“

Zeitspanne	$C8$: Sender, Empfänger ⇒ Größe	$C9$: Sender, Empfänger, Aktion ⇒ Größe	$C10$: Empfänger ⇒ Größe
Ganzes Jahr, unmodifiziert	0,855	0,860	0,621
Februar, unmodifiziert	0,904	0,908	0,666
Februar, modifiziert	0,888	0,891	0,631
April, unmodifiziert	0,830	0,835	0,596
April, modifiziert	0,808	0,813	0,550

7.6.3. Anomalieszenario „Datengröße“

Im dritten Szenario wurde die Menge der übertragenen Daten für bestehende Datenverbindungen in unregelmäßigen Abständen geändert. Dies soll einen Piggyback-Angriff simulieren, bei dem ein bösartiger Eindringling Daten aus dem System schmuggelt, indem er bestehende Datenverbindungen nutzt.

Um dieses Szenario zu simulieren, wurden modifizierte Protokolldaten erzeugt, indem

die Menge der zu übertragenden Daten für fünf ausgewählte Kombinationen von Sender und Empfänger zufällig um einen Faktor zwischen 1,5 und 5,0 verändert wurden. Dies führte zur Änderung von 496.444 Log-Einträgen.

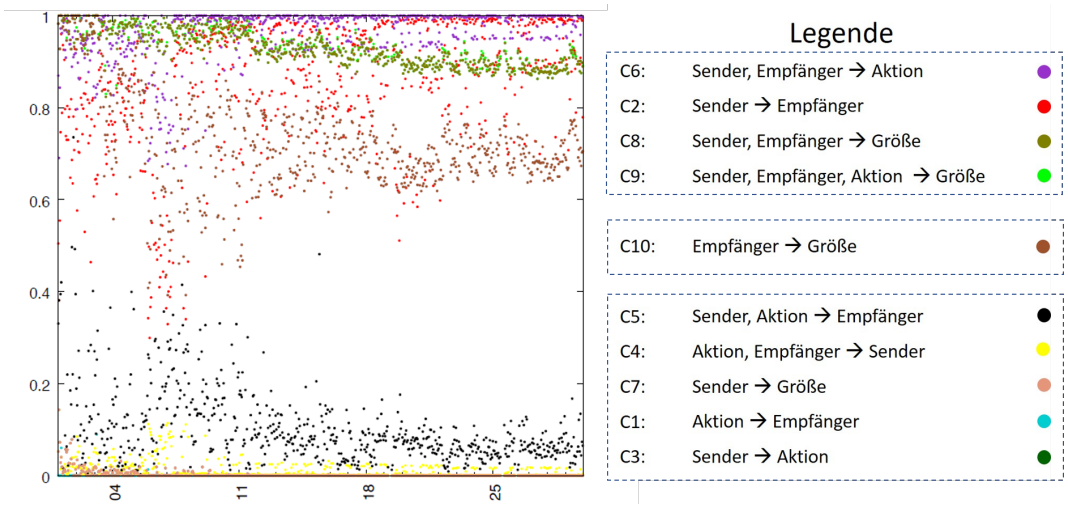

Abbildung 7.7.: Anomalieszenario „Datengröße“, Februar

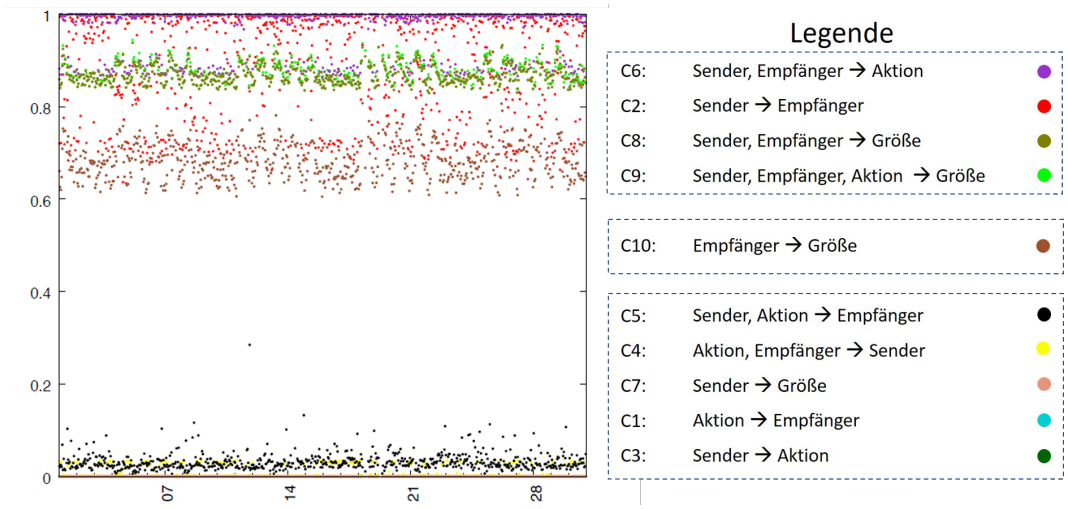

Abbildung 7.8.: Anomalieszenario „Datengröße“, April

Das Ergebnis dieses Szenarios ist, dass mit zunehmender Nachrichtengröße die Abhängigkeiten, die ein Größenattribut beinhalten, etwas höher werden als die der Originaldaten. Dies ist in Abbildung 7.7 und Abbildung 7.8 zu sehen. Die ursprünglich in den unteren Bereichen liegenden Abhängigkeiten ($C1$, $C3$, $C4$, $C5$ und $C7$) stiegen etwas an, die mittlere Abhängigkeit ($C10$) und die hohen Abhängigkeiten ($C2$, $C6$, $C8$, $C9$) nahmen stärker zu. Nennenswerte Änderungen sind auch in der Tabelle 7.3 enthalten.

Szenario 3 zeigte, dass Änderungen in der Nachrichtengröße Auswirkungen auf die Attributabhängigkeit haben, aber nur in einem Umfang, der sich nicht auf die Trennung zwischen hohen, mittleren und niedrigen Attributkombinationen auswirkt. Man kann daher zu dem Schluss kommen, dass für alle drei untersuchten Anomalieszenarien eine Wahl zur Attributentfernung auf der Grundlage der Analyse der groben Mengen die im System gegebenen Anomalien nicht beeinträchtigt hätte.

Tabelle 7.3.: Durchschnittliche Attributabhängigkeit im Anomalieszenario „Datengröße“

Zeitspanne	$C8$: Sender, Empfänger ⇒ Größe	$C9$: Sender, Empfänger, Aktion ⇒ Größe	$C10$: Empfänger ⇒ Größe
Ganzes Jahr, unmodifiziert	0,855	0,860	0,621
Februar, unmodifiziert	0,904	0,908	0,666
Februar, modifiziert	0,928	0,930	0,725
April, unmodifiziert	0,830	0,835	0,596
April, modifiziert	0,869	0,872	0,683

7.7. Zusammenfassung

In diesem Kapitel wurden grobe Protokolle vorgestellt. Dies ist ein Konzept zur Reduzierung von Protokolldaten (Faktor 1 zu 10.000), die von großen Anomalieerkennungseinrichtungen verwendet werden. Die ausführlichen Tests mit einem realen Datensatz zeigten, dass die vorgeschlagene Methode einen stabilen Hinweis darauf gibt, welches Attribut in den Protokolldaten am ehesten redundant ist. Dies gilt auch dann, wenn die Daten beginnen, Anzeichen einer Systemanomalie zu enthalten. Angesichts dieser Stabilität scheint es sicher zu sein, Attribute aus der hohen Abhängigkeitsklasse in Online-Anomalie-Erkennungsansätzen zu entfernen, da sie keinen Nutzen für die Darstellung des Systemverhaltens bieten.

Der Vorteil der vorgeschlagenen Methode liegt in ihrer Allgemeingültigkeit. Aufgrund der fundierten theoretischen Grundlagen kann es auf jede Art von Systemereignisprotokoll angewendet werden, das sich auf Attribute und deren symbolische Werte beschränkt. Die Semantik des Systems ist nur einmal relevant, um die zu testenden Kombinationen von Kandidatenattributen auf ihre Abhängigkeit hin auszuwählen. Danach ist der gesamte Ansatz datenagnostisch.

8. Zusammenfassung, Fazit und Ausblick

8.1. Zusammenfassung und Fazit

Der Gegenstand dieser Arbeit ist die strukturierte Sicherheitsanalyse komplexer verteilter IT-Umgebungen, die Verschlusssachen (VS)/Staatsgeheimnisse verarbeiten, wie zum Beispiel in militärischen oder Regierungsorganisationen. Das besondere an diesen IT-Umgebungen ist das Konzept der Informationsräume, in denen verschiedene Datenelemente, wie z. B. Papierdokumente und Computerdateien, entsprechend ihrer Sicherheitsempfindlichkeit eingestuft werden, z. B. „STRENG GEHEIM“, „GEHEIM“, „VS-NUR-FÜR-DEN-DIENSTGEBRAUCH“ und „OFFEN“. Die Besonderheit dieser Arbeit ist der Zugang zu eingestuften Informationen aus verschiedenen Informationsräumen und der Prozess der Freigabe dieser. Jede in der Arbeit entstandene Veröffentlichung wurde mit Angehörigen in der Organisation besprochen, gegengelesen und freigegeben, so dass keine eingestuften Informationen an die Öffentlichkeit gelangen.

In der Arbeit wurde erläutert, dass Vertraulichkeits- und Integritätsverluste gesamtgesellschaftliche Probleme sind und Regierungsnetze und Netzes des Militärs, in denen Verschlusssachen und Staatsgeheimnisse verarbeitet werden, permanent Ziel von Angriffskampagnen sind. Die IT-Sicherheitsziele Vertraulichkeit und Integrität werden, wie einige Beispiele zeigen, nicht erfüllt. Ursache dafür sind Bedrohungen, die auf die Infrastruktur, IT-Systeme, Netze, Anwendungen, Menschen und Informationsräume dieser IT-Umgebungen einwirken.

Im Kapitel 3 und 4 wurden diese Bedrohungen untersucht und mit Hilfe von verwandten Arbeiten klassifiziert. Dabei wurde ein geeignetes Modell für Organisationen entwickelt, das insbesondere für militärische und Regierungsorganisationen verwendbar ist und hierbei das Konzept der Informationsräume berücksichtigt. Dieses Modell ist an verschiedene Organisationen anpassbar und kann verwendet werden, um Einblicke in die Bedrohungswelt zu gewinnen. Es ermöglicht, Strategien zur Risikominderung für einzelne Teilbereiche einer Organisation zu entwickeln. Das Modell ist vollständig und klar definiert, wenn es alle Teilbereiche einer Organisation und alle Phasen eines Angriffs auf diese Bereiche sowie Klassifizierungskriterien enthält, die festlegen, welche Bedrohungen in jeder Kategorie platziert werden sollten.

In den Kapiteln 5 bis 7 wurden Bedrohungen des Modells aus dem Teilbereich der Informationsräume aufgegriffen und implementierte Lösungen präsentiert. Zunächst wurde in Kapitel 5 eine Sicherheitsanalyse einer Organisationsstruktur vorgestellt, die in einem Sicherheitsdatenflussdiagramm abgebildet wurde. Diese Darstellung begünstigt die Identifizierung von Informationsräumen, welche helfen, die erlaubten und verbotenen Informationsflüsse innerhalb und zwischen diesen Informationsräumen zu verstehen. Das resultierende Modell heißt DFDsec. Das Modell ermöglicht eine Bedrohungsanalyse

von Verbindungen, insbesondere zwischen den identifizierten Informationsräumen, um operationelle Netzknoten zu bestimmen, die durch die Gefahr des Verlustes von Vertraulichkeit, Verfügbarkeit oder Integrität am stärksten gefährdet sind. Dabei wurde ein Ansatz zur Quantifizierung der Sicherheitsrelevanz aller Netzknoten, basierend auf der gegebenen DFDsec-Struktur, diskutiert. Dies hilft, operationelle Netznoten in ihrer Bedeutung für notwendige Sicherheitsverbesserungen und Maßnahmen zur Risikominderung zu ordnen und zu priorisieren. Dieser Ansatz kann bereits in der frühen Phase der Entwicklung angewendet werden.

Im Kapitel 6 wurde die DFDsec-Methodik genutzt, um mit Hilfe von Protokolldaten, welche während der Nutzungsphase eines realen IT-Systems entstanden sind, die Struktur und die Datenflüsse der darin enthalten operationellen Netzknoten darzustellen. An dieser Stelle wurde ein Ansatz zur Identifizierung von Verletzungen der Informationsraumgrenzen mittels automatisierter Nachrichtenaustauschanalyse diskutiert. Die Bestimmung kritischer Informationsflüsse führt zur Identifizierung sensibler, operationeller Netzknoten, die hochriskante Ziele für Sicherheitsangriffe darstellen. Hierbei wurde der Ansatz zur Quantifizierung aus Kapitel 5 um die prozentuale Auslastung der Informationsflüsse erweitert. Der präsentierte Ansatz wurde somit einerseits in der Designphase und andererseits in der Nutzungsphase an beispielhaften IT-Umgebungen verwendet. Er hat gezeigt, dass eine Priorisierungsreihenfolge für IT-Sicherheitsmaßnahmen für verschiedene operationelle Netzknoten sich zwischen diesen Phasen ändern kann. Grund dafür ist die tatsächliche Auslastung der verschiedenen Informationsflüsse.

Da die Rohdatenprotokolle und die Analyseergebnisse selbst eingestufte Informationen sind, wurde ein Anonymisierungsansatz für die Originaldaten vorgeschlagen. Dabei wurde das Potenzial bekannter Anonymisierungsangriffe diskutiert. Die Analyse von Daten eines Jahres aus der Praxis zeigte, dass das untersuchte System keine Verletzungen der Informationsraumgrenzen aufzeigte. Die Visualisierung mit reduzierten DFDsec-Diagrammen erwies sich als eine praktikable Methode für Regierungsorganisationen mit hohen Anforderungen an den Datenschutz. Die Verwendung anonymisierter DFDsec-Modelle ermöglicht den Austausch der Analyseergebnisse mit externen Sicherheitsberatern und Führungskräften, die eine niedrigere Sicherheitsklassifizierung aufweisen.

Im Kapitel 7 wurden die Protokolldaten für weitergehende Analysen verwendet. Die Daten wurden so reduziert, dass aus einer reinen Offline-Analyse eine Online-Analyse ermöglicht wurde, mit der z. B. eine Anomalieerkennung durchgeführt werden kann. Dabei wird unter anderem die zeitliche Kausalität des Nachrichtenaustauschs berücksichtigt. Diese Methodik heißt grobe Protokolle. Dies ist ein Konzept zur Reduzierung von Protokolldaten, die von großen Anomalieerkennungseinrichtungen verwendet werden. Die ausführlichen Tests mit einem realen Datensatz zeigten, dass die vorgeschlagene Methode einen stabilen Hinweis darauf gibt, welches Attribut in den Protokolldaten am ehesten redundant ist. Dies gilt auch dann, wenn die Daten beginnen, Anzeichen einer Systemanomalie zu enthalten. Angesichts dieser Stabilität scheint es sicher zu sein, Attribute aus der hohen Abhängigkeitsklasse in Online-Anomalie-Erkennungsansätzen zu entfernen, da sie keinen Nutzen für die Darstellung des Systemverhaltens bieten. Die Methode kann wegen der soliden, theoretischen Grundlagen für jede Art von Systemereignisprotokoll genutzt werden, welches sich auf Attribute und deren symbolische Werte

beschränkt. Zur Identifizierung der Abhängigkeiten der zu testenden Kombinationen von Kandidatenattributen ist die Semantik des Systems nur einmal relevant. Danach kann der gesamte Ansatz ohne die zugrundeliegenden Details des Systems verwendet werden.

Zusammengefasst kann festgestellt werden, dass diese Arbeit verschiedene wissenschaftliche Beiträge zur Bedrohungsanalyse militärischer Informationstechnik unter Berücksichtigung des Konzepts der Informationsräume liefert. Die entwickelten Methoden und Verfahren können durch ihr Zusammenwirken über den gesamten Lebenszyklus von der Designphase bis zur Nutzungsphase von militärischer Informationstechnik genutzt werden.

In der Designphase kann durch die Analyse von Bedrohungen und die Nutzung des Sicherheitsdatenflussdiagramms (DFDsec) eine erste Priorisierung von operationellen Netzknoten und deren dazugehörigen Verbindungen innerhalb verschiedener Informationsräume erfolgen. In der Nutzungsphase kann sich durch Identifizierung von Informationsraumverletzungen und die Reduzierung von Attributen in Protokolldaten („ grobe Protokolle“) der Fokus von bereits getroffenen Sicherheitsmaßnahmen ändern, um den Gefahren des Verlustes der Vertraulichkeit, der Integrität und der Verfügbarkeit zu begegnen. Abhängig von der Art der Daten kann es dabei möglich sein, die groben Protokolle als direkten Ansatz zur Erkennung von Anomalien zu verwenden. Die zugrunde liegende Annahme hier wäre, dass sich die Attributabhängigkeiten signifikant ändern können, wenn die Systemanomalie die Protokolldaten stark genug beeinflusst. In diesem Fall wäre es möglich, eine Änderung der Attributabhängigkeiten als Warnzeichen für strukturelle Probleme im System zu behandeln, etwa aufgrund von Sicherheits- oder Verfügbarkeitsvorfällen.

Die anonymisierte Darstellung durch die Sicherheitsdatenflussdiagramme (DFDsec) ermöglicht über den gesamten Lebenszyklus den Austausch mit externen Experten außerhalb der Organisation. Die Dissertation leistet damit einerseits einen Beitrag zur Netzwerksicherheit, darüber hinaus zeigt sie durch die ganzheitliche Betrachtung einzelner Bestandteile, und hierbei insbesondere die Beachtung der Informationsräume von Regierungs- oder militärischen Organisationen, einen neuen Blickwinkel auf. Die Arbeit bietet einen geschlossenen Rahmen, auf den andere Verfahren, wie z. B. aus dem Bereich der künstlichen Intelligenz, des Sicherheitsbewusstseins (Awareness) und der Erkennung von Anomalien, aufsetzen können.

8.2. Ausblick

Im Rahmen der Dissertation sind Ideen aufgekommen, die nicht Bestandteil dieser Arbeit sind, aber geeignet sind in künftigen Untersuchungen analysiert zu werden. Diese sind:

- Die Sicherstellung der Integrität gegen das Einschleusen falscher Inhalte in eingestufte Dokumente. Künftige Arbeiten könnten sich mit der Inhaltsüberprüfung beschäftigen. Dies ist aus Sicht des Autors ein großes Problemfeld. Hier wären Untersuchungen im Bereich Fehlerkorrektur-Codes, Data Mining, Meta-Daten oder Signaturen möglich.

- Die Sicherstellung der korrekten Auswahl von Geheimhaltungsgraden. Unklassifizierte oder falsch eingestufte Informationen führen zur ungewollten Preisgabe/Geheimnisverrat oder unbeabsichtigtem Teilen von vertraulichen Informationen mit anderen (inkl. Außenstehenden). Daher ist es notwendig, dass die Korrektheit des Geheimhaltungsgrad bei der Bearbeitung von Dokumenten oder E-mails verifiziert wird. Denkbare Lösungen aus Sicht des Autors sind ebenfalls die Inhaltsüberprüfungen, aber auch neue Ausbildungsmethoden.

- Zukünftige Arbeiten, die sich aus dem Kapitel 5 ableiten lassen. Vorstellbar wären weitere Analysen der Struktureigenschaften in der Datenflussdarstellung, z. B. quantitative Analyseansätze, bei dem Datenflusskanten mit Angriffspotenzialen parametrisiert werden. Dies würde eine noch genauere Identifizierung von anfälligen Netzknoten ermöglichen.

Das Themenfeld der Netzwerksicherheit unterliegt einem ständigen und starkem Wandel. Es werden einerseits neue Angriffsmethoden und andererseits neue Sicherheitsmethoden/-verfahren entwickelt. Daher müssen die Beiträge dieser Dissertation laufend überprüft und gegebenenfalls angepasst werden. Diese Anpassungsmöglichkeiten sind ebenfalls nicht Bestandteil dieser Dissertation:

- Das Bedrohungsmodell aus Kapitel 4 muss die aktuellen Angriffstechniken berücksichtigen, um das Modell auf dem neuesten Stand zu halten. Dabei können identifizierte Bedrohungen anderer Autoren automatisiert mit diesem Modell verknüpft werden, um die Zuordnung von Bedrohungen für die Komponenten der Organisation und die Phasen eines Angriffs zu erleichtern. Dieser Automatismus würde es einfacher machen, eine Bedrohungsanalyse zu wiederholen, unabhängig davon, welche Person es klassifiziert.

- Ein Thema, dass sich aus den Erkenntnissen des Kapitels 6 und Kapitel 7 ergibt, ist die Erkennung von Anomalien. Hierbei könnten neben weiteren Offline-Analysen auch zusätzliche Onlineanalysen zur Überwachung der Infrastruktur entwickelt werden. Dabei ist es unerlässlich vorhandene oder neu entwickelte Online-Tools, in die in dieser Arbeit entstandenen Methoden und Verfahren zu integrieren.

- Die experimentellen Ergebnisse aus den Kapiteln 6 und 7 werden sich höchstwahrscheinlich ändern, wenn sich die Menge und Art der ursprünglichen Protokolldaten ändert. Es wäre daher interessant, die gleiche Art von Fallstudie mit anderen Protokolldatensätzen durchzuführen, um die Methoden zu verfeinern und zu generalisieren.

- Ferner ist es absolut natürlich, dass in Zukunft weitere Strategien zur Risikominderung für die identifizierten Bedrohungen in den Informationsräumen entwickelt werden können. Diese gilt es zu beobachten und mit den in dieser Dissertation entwickelten Ideen zu verknüpfen, um daraus noch effizientere Maßnahme identifizieren zu können.

Literaturverzeichnis

[1] Aycock, J. *Computer Viruses and Malware.* Springer Science + Business Media LLC, ISBN 978-0-387-30236-2, 1. edition, 2006.

[2] Azodi, A., Jaeger, D., Cheng, F., and Meinel, C. *Event Normalization Through Dynamic Log Format Detection.* https://www.researchgate.net/, 2014.

[3] Baca, D. *Identifying Security Relevant Warnings from Static Code Analysis Tools through Code Tainting.* In ARES, pages 386–390. IEEE Computer Society, 2010.

[4] Baier, H., Magraf, M., Gärtner, S., and Ossenbühl, S. *Modul IT-Sicherheit.* https://www.dasec.h-da.de/, 2015. [Online; Zugriff am 20. Januar 2019].

[5] Barnum, S. *Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description*, 2008.

[6] Bell, D. E. and LaPadula, L. J. *Secure computer system: Unified Exposition and Multics Interpretation.* Technical Report ESD-TR-75-306, MITRE Corp., Bedford, MA., 1976.

[7] Biba, J. K. *Integrity Considerations for Secure Computer Systems.* https://ban.ai/multics/doc/a039324.pdf, 1977.

[8] Bibliographisches Institut GmbH. *Duden - Die deutsche Rechtschreibung.* Dudenverlag Berlin Mannheim Zürich, ISBN 978-3-411-04017-9, 2017.

[9] Bild. *GEHEIM-AKTE AFGHANISTAN - In diesem Marder starb ein deutscher Soldat.* https://www.bild.de/, 2011. [Online; Zugriff am 20. Januar 2019].

[10] Birnbaum, Z. W. *On the importance of different components in a multicomponent system.* Technical Report No. 54, Laboratory of Statistical Research, Department of Mathematics, Seattle, Washington, Mai 1968.

[11] Bishop, M. *Computer Security - Art and Science.* Addison-Wesley, ISBN 0-201-44099-7, 2003.

[12] Bose, R. P. J. C. and Aalst, W. M. P. van der . *Discovering signature patterns from event logs.* In IEEE Symposium on Computational Intelligence and Data Mining, CIDM 2013, Singapore, 16-19 April, pages 111–118, DOI:10.1109/CIDM.2013.6597225, 2013.

[13] Bosworth, S., Kabay, M.E., and Whyne, E. *Computer Security Handbook*, volume 1. John Wiley & Sons, Inc., Hoboken, New Jersey, ISBN 978-0-470-32722-7, 5. edition, 2009.

[14] Brewer, D. F. C. and Nash, M. J. *The Chinese Wall security policy.* In Proceedings. 1989 IEEE Symposium on Security and Privacy, pages 206–214, DOI:10.1109/SECPRI.1989.36295, Mai 1989.

[15] Bundesamt für Sicherheit in der Informationstechnik. *BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS.* Bundesanzeiger-Verlag, Bad Godesberg, Deutschland, 2008.

[16] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutzkataloge - 15. Ergänzungslieferung.* Bundesanzeiger-Verlag, Köln, Deutschland, 2016.

[17] Bundesamt für Sicherheit in der Informationstechnik. *Die Lage der IT-Sicherheit in Deutschland 2017.* https://www.bsi.bund.de/, 2017. [Online; Zugriff am 20. Januar 2019].

[18] Bundesamt für Sicherheit in der Informationstechnik. *Die Lage der IT-Sicherheit in Deutschland 2018.* https://www.bsi.bund.de/, 2018. [Online; Zugriff am 20. Januar 2019].

[19] Bundesamt für Sicherheit in der Informationstechnik. *Register aktueller Cyber-Gefährdungen und -Angriffsformen.* https://www.allianz-fuer-cybersicherheit.de/, 2018. [Online; Zugriff am 19. Januar 2019].

[20] Bundesamt für Sicherheit in der Informationstechnik and secunet Security Networks AG. *Sichere Inter-Netzwerk Architektur (SINA).* https://www.bsi.bund.de/, 2002. [Online; Zugriff am 26. Januar 2019].

[21] Bundesministerium der Justiz und für Verbraucherschutz. *Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz - SÜG) vom 20. April 1994 (BGBl. I S. 867), zuletzt geändert durch Artikel 4 des Gesetzes vom 18.07. 2017 (BGBl. I S. 2732)*, 2017.

[22] Bundesministerium der Justiz und für Verbraucherschutz. *Grundgesetz für die Bundesrepublik Deutschland, Ausfertigungsdatum 23.05.1949, zuletzt geändert durch Artikel 1 des Gesetzes vom 13. Juli 2017 (BGBl. I S. 2347)*, 2017.

[23] Bundesministerium der Justiz und für Verbraucherschutz. *Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618)* , 2017.

[24] Bundesministerium der Justiz und für Verbraucherschutz. *Telekommunikationsgesetz (TKG), Ausfertigungsdatum 22.06.2004 (BGBl. I S. 1190), zuletzt geändert*

durch Artikel 10 Absatz 12 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618), 2017.

[25] Bundesministerium der Verteidigung. *IT-Sicherheit in der Bundeswehr.* Zentrale Dienstvorschrift, Bundesministerium der Verteidigung, Berlin, Deutschland, 2016.

[26] Bundesministerium der Verteidigung. *Konzeption der Bundeswehr.* Konzeption, Bundesministerium der Verteidigung, Berlin, Deutschland, 2018.

[27] Bundesministerium des Innern. *Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung - VSA).* Allgemeine Verwaltungsvorschrift, Bundesministerium des Innern, Berlin, Deutschland, 2007.

[28] Bundesregierung Deutschland. *Weißbuch 2016 - Zur Sicherheitspolitik und zur Zukunft der Bundeswehr.* Konzeption, Bundesregierung Deutschland, Berlin, Deutschland, 2016.

[29] Bundesverfassungsgericht. *Urteil des Ersten Senats vom 27. Februar 2008, - 1 BvR 370/07 - Rn. (1-333).* https://www.bundesverfassungsgericht.de/, 2008.

[30] Chandola, V., Banerjee, A., and Kumar, V. *Anomaly Detection: A Survey.* ACM Comput. Surv., 41(3):15:1–15:58, DOI:10.1145/1541880.1541882, Juli 2009.

[31] Chen, Z., Juan Wang, X., and Xin Zhang, X. *Dynamic Taint Analysis with Control Flow Graph for Vulnerability Analysis*, Oktober 2011.

[32] Cheng, F., Sapegin, A., Gawron, M., and Meinel, C. *Analyzing Boundary Device Logs on the In-memory Platform.* In 17th IEEE International Conference on High Performance Computing and Communications, HPCC 2015, 7th IEEE International Symposium on Cyberspace Safety and Security, CSS 2015, and 12th IEEE International Conference on Embedded Software and Systems, ICESS 2015, New York, NY, USA, August 24-26, pages 1367–1372. IEEE, DOI:10.1109/HPCC-CSS-ICESS.2015.284, 2015.

[33] CISCO. *Annual Cybersecurity Report.* Report, CISCO, Februar 2018.

[34] Clark, D. D. and Wilson, D. R. *A Comparison of Commercial and Military Computer Security Policies.* IEEE Symposium on Security and Privacy, page 184, DOI:10.1109/SP.1987.10001, 1987.

[35] Clough, J. *Principles of Cybercrime.* Cambridge University Press, ISBN 978-1-107-03457-0, 2. edition, 2015.

[36] CNN. *Every single Yahoo account was hacked - 3 billion in all.* http://money.cnn.com/, 2013. [Online; Zugriff am 19. Januar 2019].

[37] CWE. *Common Weakness Enumeration (CWE)*, 2018.

[38] CyberEdge Group. *2018 Cyberthreat Defense Report*. Report, CyberEdge Group, März 2018.

[39] DeMarco, T. *Structured Analysis and System Specification*. In Yourdon, Edward Nash, editor, Classics in Software Engineering, pages 409–424. Yourdon Press, Upper Saddle River, NJ, USA, 1979.

[40] Denning, D. E. *A Lattice Model of Secure Information Flow*. Commun. ACM, 19(5):236–243, DOI:10.1145/360051.360056, Mai 1976.

[41] Denning, D. E. and Denning, P. J. *Certification of Programs for Secure Information Flow*. Commun. ACM, 20(7):504–513, DOI:10.1145/359636.359712, Juli 1977.

[42] Deutsches Institut für Normung. *Zuverlässigkeitsmanagement - Teil 3.1: Anwendungsleitfaden (DIN EN 60300-3-1)*, Mai 2005.

[43] Donaldson, S. E., Siegel, S. G., Williams, C. K., and Aslam, A. *Enterprise Cybersecurity - How to Build a Successful Cyberdefense Program Against Advanced Threats*. Apress, ISBN 978-1-4302-6082-0, 2015.

[44] Dubois, D. and Prade, H. *Rough Fuzzy Sets and Fuzzy Rough Sets**. International Journal of General Systems, 17(2-3):191–209, DOI:10.1080/03081079008935107, 1990.

[45] Eager, D. L., Lazowska, E. D., and Zahorjan, J. *Adaptive load sharing in homogeneous distributed systems*. IEEE Transactions on Software Engineering, 12:662–675, DOI:10.1109/TSE.1986.6312961, Mai 1986.

[46] Eckstein, C. *Preventing data leakage: A risk based approach for controlled use of the use of administrative and access privileges*. White Paper, SANS Institute, August 2015.

[47] Edgeworth, F.Y. *XLI. On discordant observations*. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 23(143):364–375, DOI:10.1080/14786448708628471, 1887.

[48] ENISA. *ENISA Threat Landscape Report 2017*. http://www.enisa.europa.eu/, 2018.

[49] Europäische Kommission. *Information Technology Security Evaluation Criteria (ITSEC) - Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom*. Standard, Europäische Kommission, Juni 1991.

[50] Europäisches Parlament und Europäischer Rat. *Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtwidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung*. https://eur-lex.europa.eu/, Juni 2016.

[51] European Commission. *Commission Decision of 29 November 2001 amending its internal Rules of Procedure (notified under document number C(2001) 3031).* https://publications.europa.eu/, 2001.

[52] European Parliament Directorate General for Internal Policies Police Department A: Economic and Scientific Policy. *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts.* Report, European Parliament, September 2013.

[53] Feng, B., Zhang, M., Xu, G., Niu, X., and Hu, Z. *Runtime protecting system for java applications with dynamic data flow analyzing.* In 2010 2nd International Conference on Future Computer and Communication, volume 2, pages V2–408–V2–411, DOI:10.1109/ICFCC.2010.5497460, Mai 2010.

[54] Forbes. *Equifax's Enormous Data Breach Just Got Even Bigger.* https://www.forbes.com/, 2017. [Online; Zugriff am 19. Januar 2019].

[55] FU-Berlin. *IT-Sicherheit - Grundwerte.* http://www.fu-berlin.de/, 2019. [Online; Zugriff am 20. Januar 2019].

[56] Fuhrberg, K. *Internet-Security - Browser, Firewalls and Encryption.* Carl Hanser Verlag München Wien, ISBN 3-446-21333-3, 2000.

[57] Gabler. *Gabler - Wirtschaftslexikon.* Springer Fachmedien Wiesbaden, ISBN 978-3-658-19570-0, 2018.

[58] Gane, C. and Sarson, T. *Structured Systems Analysis: Tools and Techniques.* McDonnell Douglas Systems Integration Company, ISBN 0930196007, 1977.

[59] Ganta, S. R., Kasiviswanathan, S. P., and Smith, A. *Composition Attacks and Auxiliary Information in Data Privacy.* In Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '08, pages 265–273, New York, NY, USA. ACM, ISBN 978-1-60558-193-4, DOI:10.1145/1401890.1401926, 2008.

[60] Gaycken, S. *Studienbrief 3 Phänomenologie von Cybercrime.* https://m.esmt.org, Dezember 2013.

[61] Gemalto. *Data Breach Discoveries from the Breach Level Index - Data Privacy and New Regulations Take Center Stage - 2018 First Half Review.* Report, Gemalto, Oktober 2018.

[62] Genua Gmbh. *Datendiode vs-diode.* https://www.genua.de/, 2016. [Online; Zugriff am 19. Januar 2019].

[63] Gerić, S. and Hutinski, Ž. *Information System Security Threats Classification.* Journal of information and organizational sciences, 31:51–61, 2007.

[64] Gordon, P. *Data Leakage - Threats and Mitigation.* White Paper, SANS Institute, Oktober 2007.

[65] Gustin, J. F. *Cyber Terrorism - A Guide for Facility Managers.* The Fairmount Press, ISBN 0-88173-442-X, 2004.

[66] Guttmann, B. and Roback, E. A. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800-12, National Institute of Standards and Technology, 1995.

[67] Harrison, W. S., Hanebutte, N., Oman, P. W., and Alves-Foss, J. *The MILS Architecture for a Secure Global Information Grid.* The Journal of Defense Software Engineering, pages 20–24, 2005.

[68] Haystax Technology. *Insider Attacks - Industry Survey.* Report, Haystax Technology, 2017.

[69] Hellerstein, J. L., Ma, S., and Perng, C.-S. *Discovering actionable patterns in event data.* IBM Systems Journal, 41(3):475–493, DOI:10.1147/sj.413.0475, 2002.

[70] Hellmann, R. *IT-Security - An Introduction.* DE Gruyter Oldenbourg, ISBN 978-3-11-049483-9, 2018.

[71] Helmuth, C., Westfeld, A., and Sobirey, M. *Mikro-SINA - Eine mikrokernbasierte Systemarchitektur für sichere Systemkomponenten.* Standard, Technische Universität Dresden & secunet Security Networks AG, Deutschland, 2003.

[72] Hofstede, R., Pras, A., Sperotto, A., and Rodosek, G. D. *Flow-Based Compromise Detection: Lessons Learned.* IEEE Security Privacy, 16(1):82–89, DOI:10.1109/MSP.2018.1331021, Januar 2018.

[73] Identity Theft Resource Center. *Data Breaches.* https://www.idtheftcenter.org/, 2018.

[74] I.Fronza, Sillitti, A., Succi, G., Terho, M., and Vlasenko, J. *Failure prediction based on log files using Random Indexing and Support Vector Machines.* Journal of Systems and Software, 86(1):2–11, DOI:10.1016/j.jss.2012.06.025, 2013.

[75] Infodas GmbH. *SDoT Security Gateway 6.0.* https://www.infodas.de/, 2017. [Online; Zugriff am 19. Januar 2019].

[76] InfoWatch. *Global Data Leakage Report, H1 2018.* Report, InfoWatch, Dezember 2018.

[77] International Organization for Standardization. *ISO 26262 Road vehicles - Functional safety - Part 3: Concept phase.* Standard, International Organization for Standardization, Genf, CH, 2011.

[78] International Organization for Standardization. *ISO 27001 Information technology - Security techniques - Information security management systems Overview and vocabulary.* Standard, International Organization for Standardization, Genf, CH, 2013.

[79] International Organization for Standardization. *ISO 9000:2015-11 Qualitätsmanagementsysteme - Grundlagen und Begriffe.* Standard, International Organization for Standardization, Genf, CH, 2015.

[80] Jaeger, D., Azodi, A., Cheng, F., and Meinel, C. *Normalizing Security Events with a Hierarchical Knowledge Base.* In WISTP, volume 9311 of Lecture Notes in Computer Science, pages 237–248. Springer, 2015.

[81] Jakobsson, M. and Myers, S. *Phishing and Countermeasures - Understanding the Increasing Problem of Electronic Identity Theft.* John Wiley & Sons, Inc., Hoboken, New Jersey, ISBN 978-0-471-78245-2, 2007.

[82] Jouini, M., Rabai, L.B.A., and Aissa, A.B. *Classification of Security Threats in Information Systems.* In ANT/SEIT, volume 32 of Procedia Computer Science, pages 489–496. Elsevier, 2014.

[83] Kammermann, M. and Campo, M. *CompTIA Security+.* mitp, ISBN 978-3-8266-5522-7, 1. edition, 2011.

[84] Kersten, H. *Sicherheit in der Informationstechnik - Einführung in die Computersicherheit.* R. Oldenburg München, Wien, ISBN 3-486-21873-5, 1991.

[85] Laprie, J. *Dependability: Basic Concepts and Terminology.* Springer-Verlag Wien, ISBN 978-3-7091-9172-9, 1998.

[86] Lawrence, J. D. *Software safety hazard analysis.* Division of Reactor Controls and Human Factors, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission : Supt. of Docs., U.S. G.P.O. [distributor] Washington, DC, UCRL-ID-122514, 1996.

[87] Leveson, N. *Engineering a Safer World: Systems Thinking Applied to Safety.* Engineering systems. MIT Press, ISBN 978-0-262-01662-9, 2011.

[88] Li, N. and Li, T. *t-Closeness: Privacy Beyond k-Anonymity and l-Diversity.* In In Proc. of IEEE 23rd International Conference on Data Engineering (ICDE'07, volume 7, pages 106–115, 2007.

[89] Li, P., Park, H., Gao, D., and Fu, J. *Bridging the Gap between Data-Flow and Control-Flow Analysis for Anomaly Detection.* In 2008 Annual Computer Security Applications Conference (ACSAC), pages 392–401, DOI:10.1109/ACSAC.2008.17, Dezember 2008.

[90] Liang, Y., Zhang, Y., Sivasubramaniam, A., Sahoo, R. K., Moreira, J., and Gupta, M. *Filtering failure logs for a BlueGene/L prototype.* In 2005 International Conference on Dependable Systems and Networks (DSN'05), pages 476–485, DOI:10.1109/DSN.2005.50, Juni 2005.

[91] Ma, S. and Hellerstein, J. L. *Mining Partially Periodic Patterns With Unknown Periods From Event Stream.* In Chen, D. and Cheng, X., editors, Pattern Recognition and String Matching, pages 353–377. Springer US, Boston, MA, 2002.

[92] Machanavajjhala, A., Gehrke, J., Kifer, D., and Venkitasubramaniam, M. *L-diversity: privacy beyond k-anonymity.* In 22nd International Conference on Data Engineering (ICDE'06), pages 24–24, DOI:10.1109/ICDE.2006.1, April 2006.

[93] Mah, P. *7 Social Engineering Scams and How to Avoid Them.* https://www.cio.com/.../7-social-engineering-scams-and-how-to-avoid-them.html, Februar 2015. [Online; Zugriff am 20. Januar 2019].

[94] McClure, S., Scambray, J., and Kurtz, G. *Hacking Exposed Network Security Secrets & Solutions.* McGraw-Hill, ISBN 0-07-226081-5, 5. edition, 2005.

[95] Meinig, M. and Meinel, C. *Securing the Flow - Data Flow Analysis with Operational Node Structures.* In Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, Funchal, Madeira - Portugal, Januar 22-24, pages 241–250, DOI:10.5220/0006570302410250, Januar 2018.

[96] Meinig, M., Sukmana, M. I. H., Torkura, K. A., and Meinel, C. *Holistic Strategy-Based Threat Model for Organizations.* In Proceedings of the 10th International Conference on Ambient Systems, Networks and Technologies, (ANT 2019), Leuven, Belgien, April 29- Mai 02, April-Mai 2019.

[97] Meinig, M., Tröger, P., and Meinel, C. *Finding Classification Zone Violations with Anonymized Message Flow Analysis.* In Proceedings of the 5th International Conference on Information Systems Security and Privacy, ICISSP 2019, Prag, Tschechien, Februar 23-25, pages 284–292, DOI:10.5220/0007352602840292, Februar 2019.

[98] Meinig, M., Tröger, P., and Meinel, C. *Rough Logs - A Data Reduction Approach for Log Files.* In Proceedings of the 21st International Conference on Enterprise Information Systems (ICEIS 2019), Heraklion, Kreta - Griechenland, Mai 03-05, Mai 2019.

[99] Mitnick, K. D. and Simon, W. L. *Art of Deception - Controlling the Human Element of Security.* Wiley Publishing, Inc., ISBN 0-471-23712-4, 2002.

[100] Myers, A. C. and Liskov, B. *A Decentralized Model for Information Flow Control.* In Proceedings of the Sixteenth ACM Symposium on Operating Systems Principles, SOSP '97, pages 129–142, New York, NY, USA. ACM, ISBN 0-89791-916-5, DOI:10.1145/268998.266669, 1997.

[101] Oliner, A. and Stearley, J. *What Supercomputers Say: A Study of Five System Logs.* In IEEE Proceedings of International Conference on Dependable Systems and Networks (DSN'07), pages 575–584. IEEE Computer Society, ISBN 0-7695-2855-4, 2007.

[102] Oliner, A. J., Aiken, A., and Stearley, J. *Alert Detection in System Logs.* In Eighth IEEE International Conference on Data Mining, pages 959–964, DOI:10.1109/ICDM.2008.132, Dezember 2008.

[103] Oxford University Press. *Oxford Dictionary of English.* Oxford University Press, ISBN 978-0-19-957112-3, 2010.

[104] Pang, R. and Paxson, V. *A High-level Programming Environment for Packet Trace Anonymization and Transformation.* In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '03, pages 339–351, New York, NY, USA. ACM, ISBN 1-58113-735-4, DOI:10.1145/863955.863994, 2003.

[105] Pantola, V. A., Yatco, F. R., and Pineda, J. D. *Normalization of Logs for Networked Devices in a Security Information Event Management System*, August 2010.

[106] Pawlak, Z. *Rough sets.* International Journal of Parallel Programming, 11(5):341–356, DOI:10.1007/BF01001956, 1982.

[107] Pawlak, Z. *Some Issues on Rough Sets*, 2004.

[108] Peikari, C. and Chuvakin, A. *Security Warrior.* O'Reilly, ISBN 3-89721-376-1, 1. edition, 2004.

[109] Pena, J. M., Létourneau, S., and Famili, F. *Application of Rough Sets Algorithms to Prediction of Aircraft Component Failure.* In Advances in Intelligent Data Analysis: Third International Symposium (IDA-99), volume 1642 of LNCS. Springer Verlag, Amsterdam, The Netherlands, August 1999.

[110] Pfleeger, C. P., Pfleeger, S. L., and Margulies, J. *Security in Computing.* pearson education, ISBN 978-0-13-408504-3, 5. edition, 2015.

[111] Ponemon Institute. *2018 Cost of a Data Breach Study: Global Overview.* Report, Ponemon Institute, August 2018.

[112] Rao, U.H. and Nayak, U. *The InfoSec Handbook - An Introduction to Information Security.* Apress Media, ISBN 978-1-4302-6382-1, 5. edition, 2014.

[113] Reidemeister, T., Jiang, M., and Ward, P. A. S. *Mining unstructured log files for recurrent fault diagnosis.* In Proceedings of the 12th IFIP/IEEE International Symposium on Integrated Network Management, IM 2011, Dublin, Ireland, 23-27 May 2011, pages 377–384. IEEE, DOI:10.1109/INM.2011.5990536, 2011.

[114] Reidemeister, T., Jiang, Miao, and Ward, P. A. S. *Mining unstructured log files for recurrent fault diagnosis.* In 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops, pages 377–384, DOI:10.1109/INM.2011.5990536, Mai 2011.

[115] Rodgers, C. *Data Classification: Why is it important for Information Security?* http://www.infosecisland.com/, April 2012. [Online; Zugriff am 20. Januar 2019].

[116] Rost, N. *Peak Oil-Studie der Bundeswehr und ihre Bedeutung für Kommunen.* https://www.peak-oil.com/, 2010. [Online; Zugriff am 20. Januar 2019].

[117] Ruf, L., Thorn, A., Christen, T., Gruber, B., and Portmann, R. *Threat Modeling in Security Architecture - The Nature of Threats.* https://www.isss.ch/, 2008.

[118] Rushby, J. M. *Design and Verification of Secure Systems.* In Proceedings of the Eighth ACM Symposium on Operating Systems Principles, SOSP '81, pages 12–21, New York, NY, USA. ACM, ISBN 0-89791-062-1, DOI:10.1145/800216.806586, 1981.

[119] Salfner, F. and Tröger, P. *Predicting Cloud Failures Based on Anomaly Signal Spreading.* In 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Boston. Juni 2012.

[120] Salomon, D. *Foundations of Computer Security.* Springer-publishers London, ISBN 978-1-84628-193-8, 2006.

[121] Samarati, P. and Sweeney, L. *Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression.* Tech. rep. SRI-CSL-98-04, SRI Computer Science Laboratory, Palo Alto, CA, 1998.

[122] Sapegin, A., Jaeger, D., Azodi, A., Gawron, M., Cheng, F., and Meinel, C. *Hierarchical object log format for normalisation of security events.* In IAS, pages 25–30. IEEE, 2013.

[123] Schmidt, K., Tröger, P., Kroll, H.-M., Bünger, T., Krueger, F., and Neuhaus, C. *Adapted Development Process for Security in Networked Automotive Systems.* SAE Int. J. Passeng. Cars - Electron. Electr. Syst., 7:516–526, DOI:10.4271/2014-01-0334, April 2014.

[124] Security, Risk Based. *Data Breach Quick View Report.* https://pages.riskbasedsecurity.com/, 2018.

[125] Shafer, G. *A Mathematical Theory of Evidence.* Princeton University Press, 1976.

[126] Shostack, A. *Experiences Threat Modeling at Microsoft.* In MODSEC@MoDELS, volume 413 of CEUR Workshop Proceedings. CEUR-WS.org, Januar 2008.

[127] Smaha, S. E. *Haystack: an intrusion detection system.* In [Proceedings 1988] Fourth Aerospace Computer Security Applications, pages 37–44, DOI:10.1109/ACSAC.1988.113412, September 1988.

[128] Snow, B. *We need assurance!* In Proceedings of the 21st Annual Computer Security Applications Conference, IEEE Computer Society, pages 3–10, DOI:10.1109/CSAC.2005.63, Dezember 2005.

[129] Spiegel. *Geheime Bundeswehrstudie - Militärplaner halten Zerfall der EU für denkbar.* https://www.spiegel.de/, 2017. [Online; Zugriff am 20. Januar 2019].

[130] Stearley, J. *Towards informatic analysis of Syslogs.* In 2004 IEEE International Conference on Cluster Computing (CLUSTER 2004), September 20-23 2004, San Diego, California, USA, pages 309–318, DOI:10.1109/CLUSTR.2004.1392628, 2004.

[131] Su, L., Yao, Y., Li, N., Liu, J., Lu, Z., and Liu, B. *Hierarchical Clustering Based Network Traffic Data Reduction for Improving Suspicious Flow Detection.* In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pages 744–753, DOI:10.1109/TrustCom/BigDataSE.2018.00108, August 2018.

[132] Sweeney, L. *K-anonymity: A Model for Protecting Privacy.* Int. J. Uncertain. Fuzziness Knowl.-Based Syst., 10(5):557–570, DOI:10.1142/S0218488502001648, Oktober 2002.

[133] Swiderski, F. and Snyder, W. *Microsoft Professional Threat Modeling.* Microsoft Press, ISBN 0-7356-1991-3, 2004.

[134] Tagesspiegel. *Das Beichtgeheimnis.* https://www.tagesspiegel.de/, 2008. [Online; Zugriff am 20. Januar 2019].

[135] The Guardian. *Facebook says Cambridge Analytica may have gained 37m more users' data.* https://www.theguardian.com/, 2018. [Online; Zugriff am 19. Januar 2019].

[136] The OWASP Foundation. *OWASP Top 10 - 2017 - The Ten Most Critical Web Application Security Risks.* https://www.owasp.org/, 2017.

[137] Torkura, K. A., Sukmana, M. I. H., Meinig, M., Cheng, F., Meinel, C., and Graupner, H. *A threat modeling approach for cloud storage brokerage and file sharing systems.* In NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, pages 1–5, DOI:10.1109/NOMS.2018.8406188, April 2018.

[138] Torkura, K. A., Sukmana, M. I. H., Meinig, M., Kayem, A. V. D. M., Cheng, F., Graupner, H., and Meinel, C. *Securing Cloud Storage Brokerage Systems Through Threat Models.* In 2018 IEEE 32nd International Conference

on Advanced Information Networking and Applications (AINA), pages 759–768, DOI:10.1109/AINA.2018.00114, Mai 2018.

[139] Torr, P. *Demystifying the threat modeling process.* IEEE Security Privacy, 3(5):66–70, DOI:10.1109/MSP.2005.119, September 2005.

[140] TrendLabs^{SM}. *2017 Midyear Security Roundup.* Report, Trendlabs, September 2017.

[141] TrendLabs^{SM} APT Research Team. *Spear-Phishing E-Mail: die beliebteste APT-Angriffstechnik.* Forschungspapier, Trendlabs, Dezember 2012.

[142] Tröger, P. *Unsicherheit und Uneindeutigkeit in Verlässlichkeitsmodellen.* Springer Fachmedien Wiesbaden, ISBN 978-3-658-23341-9, 2018.

[143] Trustwave. *2018 Trustwave Global Security Report.* Report, Trustwave, April 2018.

[144] Tzur-David, S., Dolev, D., and Anker, T. *MULAN: Multi-Level Adaptive Network Filter.* In Security and Privacy in Communication Networks - 5th International ICST Conference, SecureComm 2009, Athens, Greece, September 14-18, 2009, Revised Selected Papers, volume 19, pages 71–90. Springer, DOI:10.1007/978-3-642-05284-2_5, 2009.

[145] UK Department for Digital, Culture, Media and Sport. *Cyber Security Breaches Survey 2018: Statistical Release.* Report, UK Department for Digital, Culture, Media and Sport, April 2018.

[146] Universität Giessen. *Ziele der IT-Sicherheit.* https://www.uni-giessen.de/, 2019. [Online; Zugriff am 20. Januar 2019].

[147] Upguard. *US Air Force Suffers Massive Data Breach.* https://www.upguard.com/, 2017. [Online; Zugriff am 19. Januar 2019].

[148] Vaarandi, R. *A data clustering algorithm for mining patterns from event logs.* In in IEEE IPOM'03 Proceedings, pages 119–126. IEEE, DOI:10.1109/IPOM.2003.1251233, 2003.

[149] Vaarandi, R. *A Breadth-First Algorithm for Mining Frequent Patterns from Event Logs.* In Intelligence in Communication Systems, (IFIP)International Conference, (INTELLCOMM) 2004, Bangkok, Thailand, November 23-26, 2004, Proceedings, pages 293–308, DOI:10.1007/978-3-540-30179-0_27, 2004.

[150] Verisign. *Verisign Distributed Denial of Service Trends Report - Volume 5, Issue 1 - 1st Quarter 2018.* Report, Verisign, Juni 2018.

[151] Verizon. *2017 Data Breach Investigations Report.* Report, Verizon, 2017.

[152] Verizon. *2018 Data Breach Investigations Report - 11th Edition.* Report, Verizon, März 2018.

[153] WASC. *WASC Threat Classification - Version 2.00*. http://www.webappsec.org/, 2010.

[154] Washington Post. *eBay asks 145 million users to change passwords after data breach*. https://www.washingtonpost.com/, 2014. [Online; Zugriff am 19. Januar 2019].

[155] Washington Post. *Government alleges former NSA contractor stole astonishing quantity of classified data over 20 years*. https://www.washingtonpost.com/, 2016. [Online; Zugriff am 19. Januar 2019].

[156] Wiesauer, A. and Sametinger, J. *A Security Design Pattern Taxonomy based on Attack Patterns - Findings of a Systematic Literature Review*. In SECRYPT, pages 387–394. INSTICC Press, DOI:10.5220/0002232503870394, 2009.

[157] Wilshusen, G. C. *Cybersecurity - Actions Needed to Strengthen U.S. Capabilities*. Report, United States Government Accountability Office, Februar 2017.

[158] Yamanishi, K. and Maruyama, Y. *Dynamic Syslog Mining for Network Failure Monitoring*. In Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining, KDD '05, pages 499–508, New York, NY, USA. ACM, ISBN 1-59593-135-X, DOI:10.1145/1081870.1081927, 2005.

[159] Yourdon, E. *Modern Structured Analysis*. Yourdon Press, Upper Saddle River, NJ, USA, ISBN 0-13-598624-9, 1989.

[160] Zadeh, L. A. *Fuzzy Sets*. Information and Control, 8(3):338–353, DOI:10.1016/S0019-9958(65)90241-X, 1965.

[161] Zeit. *Bundestags-Hack - Merkel and the Fancy Bear*. https://www.zeit.de/, 2015. [Online; Zugriff am 19. Januar 2019].

Anhang

A. Bedrohungsmodell

A.1. Infrastruktur

Phase 1: Informationsgewinnung

- Ausspähen von Informationen (Rückschlüsse auf internen Aufbau der Infrastruktur durch Betrachtung von außen)
- Verkabelung - Ausstrahlung (Radiation, Emanation) [110]
- Räume/Gebäude - Unkontrollierte Ausbreitung der Funkwellen [16]

Phase 2: Angriff auf das Ziel

- Energieversorgung/Klimatisierung [83], [66]
- Räume/Gebäude [16], [5], [66], [120]
  - Abhören [16]
    - Abhören von Räumen mittels Rechner mit Mikrofon und Kamera [16]
    - Abhören von Räumen über TK-Endgeräte [16]
    - Abhören von Raumgesprächen über mobile Endgeräte [16]
  - Einsatz gefälschter Komponenten [16]
  - Seitenkanalangriffe (z. B. auf eingebettete Systeme) [16], [120]
    - Elektromagnetische Ausstrahlung [120]
    - Passive Reconnaissance [120]
  - Unbefugtes Eindringen in Räumlichkeiten (Physische Sicherheit umgehen, z. B. elektronische Schlösser) [16], [5]
- Verkabelung [16], [13], [84], [66], [110]
  - Abhören von Leitungen [16]
    - Abhören von Telefongesprächen und Datenübertragungen [16]
    - Manipulation von Leitungen [16]
  - Datenlogger in interner Verkabelung (z. B. durch Reinigungsfirma)
  - Einsatz gefälschter Komponenten (Verkabelung) [16]
  - Einschleusen von Daten in die Übertragungsstrecke [84]
  - Unzulässige Kabelverbindungen [16], [110]
  - Übersprechen [16]

  - Wiretapping [13], [110]

Phase 3: Ausweitung der Rechte

- Keylogger im Kabelkanal
- über Anwendungen, IT-Systeme, Netze

Phase 4: Zielerreichung

- Zugriff auf Anwendungen, IT-Systeme, Netze

A.2. IT-System

Phase 1: Informationsgewinnung

- Abfangen kompromittierender Strahlung [16], [110]
- Ausspähen von Informationen/Spionage [16]
- Footprinting [5]
- Physikalischer Zugriff (Fraud and Theft) [16], [5], [112], [66], [65], [108], [120]
  - Diebstahl von IT-Systemen [16], [5], [112], [65]
    - Am häuslichen Arbeitsplatz (Telearbeit) [16]
    - Bei mobiler Nutzung des IT-Systems [16]
  - Verlust von IT-Systemen (z. B. beim Versand, unterwegs) [16]
- Reverse Engineering [16], [108]
- Schultersurfen [13], [112], [108]

Phase 2: Angriff auf das Ziel (Allgemeine Bedrohungen)

- Eindringen in IT-Systeme (z. B. über Kommunikationskarten) [16]
- Missbrauch von IT-Systemen [16], [43], [112], [84]
  - Bewusste Fehlbedienung von Schutzschränken (z. B. aus Bequemlichkeit) [16]
  - Bomb [43]
    - Laser Bomb (single critical computer or infrastructure component) [43]
    - Smart Bomb (single IT-System) [43]
    - Sniper Bomb (Angriff auf single person's accounts or computers) [43]
  - Einschleusen von Daten in die Übertragungsstrecke [84]
  - Erlangung physischen Zugangs (z. B. auf Switche) [16]
  - Gefährdung bei Wartungs-/Administrierungsarbeiten [16]
  - Missbrauch der Informationen von mobilen Endgeräten [16]

  - Missbrauch von SIM-Karten [16]
  - Physikalischer Eingriff in IT-System (z. B. eingebettetes System) [16]
  - Unberechtigter Anschluss von IT-Systemen an ein Netz [16], [43]
  - Vertraulichkeitsverlust schützenswerter Informationen [16]
- Fehlfunktion von IT-Systemen (Geräten oder Systemen) [16]
- MAC-Spoofing [16]

Phase 2: Angriff auf das Ziel (Spezielle Bedrohungen)

- Adapter, Router, Switch, Hub, TK-Anlage [16], [94], [66]
  - Erlangung physischen Zugangs auf SAN-Switches [16]
  - Manipulation von ARP-Tabellen [16]
  - Missbrauch von Leistungsmerkmalen von TK-Anlagen [16]
  - Unberechtigter Zugang zu den aktiven Netzkomponenten [16]
  - Unsichere Default-Einstellungen auf Routern und Switches [16]
  - Vertraulichkeitsverlust von in TK-Anlagen gespeicherten Daten [16]
  - Zugriff auf Informationen anderer Mandanten durch WWN-Spoofing [16]
- Drucker/Multifunktionsgeräte [16]
  - Auswertung von Restinformationen in Druckern, Kopierern und Multifunktionsgeräten [16]
  - Komplexität von Druckern, Kopierern und Multifunktionsgeräten [16]
  - Unzureichender Schutz der Kommunikation bei Druckern und Multifunktionsgeräten [16]
- Fax [16]
  - Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes [16]
  - Auswertung von Restinformationen in Faxgeräten und Faxservern [16]
  - Fehlerhafte Faxübertragung [16]
  - Manipulation von Adressbüchern und Verteillisten [16]
  - Unbefugtes Lesen von Faxsendungen [16]
  - Unbefugte Nutzung eines Faxgerätes oder eines Faxservers [16]
  - Vortäuschen eines falschen Absenders bei Faxsendungen [16]
- Kryptomodul [16]
  - Manipulation eines Kryptomoduls [16]
  - Unautorisierte Benutzung eines Kryptomoduls [16]
- Mobile Endgeräte (Mobiltelefone, Telefone VOIP, Laptop, Smartphone, Tablet, USB-Stick, MP3-Player) [16], [43], [112], [120]

  - Abhören von Mobiltelefonaten [16]
  - Abhören von Raumgesprächen über Mobiltelefone [16]
  - Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen [16]
  - Automatische Erkennung von Wechseldatenträgern [16]
  - BYOD [43]
  - Datendiebstahl über mobile Datenträger/Endgeräte [16]
  - Einschleusen von GSM-Codes in Endgeräte mit Telefonfunktion [16]
  - Manipulation von Mobiltelefonen [16]
  - Missbrauch frei zugänglicher Telefonanschlüsse [16]
  - Schwachstellen beim Einsatz von VoIP-Endgeräten [16]
  - Unberechtigte Datenweitergabe über Mobiltelefone [16]
  - Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten [16]
  - Unberechtigtes Kopieren der Datenträger [16]
  - Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs [16]
  - Unzureichende Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs [16]
  - Verbreitung von Schadprogrammen über mobile Datenträger [16]
- Server [16]
  - Erweiterte Rechte durch Programmdialoge auf Terminalservern [16]
  - Manipulation von Daten und Werkzeugen beim Patch- und Änderungsmanagement [16]
  - Unsichere Default-Einstellungen bei Speicherkomponenten [16]
- Zubehör (z. B. Tastatur) [120]
  - Acoustic Keyboard Eavesdropping [120]
- Speicher [16]
  - Manipulation der Konfiguration einer Speicherlösung [16]
  - Manipulation von Daten über das Speichersystem [16]
  - Nutzung gemeinsamer Speicherbereiche, Register, Statusbericht [84]
  - Unsichere Default-Einstellungen bei Speicherkomponenten [16]
  - Verlust der Vertraulichkeit durch storagebasierte Replikationsmethoden [16]
- Virtualisierung [16]

  - Kompromittierung des Hypervisor virtueller IT-Systeme [16]
  - Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen [16]
  - Missbrauch von Virtualisierungsfunktionen [16]
  - Überwindung der logischen Netzseparierung [16]
  - Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes [16]
  - Unberechtigtes Wiedereinspielen von Snapshots [16]

Phase 3: Ausweitung der Rechte

- Manipulation von IT-Systemen (Hardware, z. B. während der Supply Chain) [16], [5], [43]
  - Manipulation während der Herstellung [5]
  - Manipulation während der Auslieferung [5]

Phase 4: Zielerreichung

- Integritätsverlust/Tampering der IT-Systeme [16], [133]
- Vertraulichkeitsverlust der IT-Systeme [16], [133]

A.3. Netze

Phase 1: Informationsgewinnung

- Abhören/Sniffing/Traffic Injection [5], [56], [112], [65], [108], [110]
- Analyse [16], [70], [108]
  - Analyse des Nachrichtenflusses [16], [70]
  - Netzanalysetools [16]
  - Vertraulichkeitsverlust schützenswerter Informationen [16]

Phase 2: Angriff auf das Ziel (Allgemeine Bedrohungen)

- Eindringen durch Netzwerkverbindungen [13], [43]
  - abgehende z. B. von Servern/Clients des internen Netzwerk [43]
  - eingehende/ausgehende Netzwerkverbindungen von Servern, die mit dem Internet verbunden sind [43]
- Gate Crashing [43]
- Hijacking von Netz-Verbindungen [16]
- Manipulation von Managementparametern [16]
- Unberechtigte Ausführung von Netzmanagement-Funktionen [16]

Phase 2: Angriff auf das Ziel (Spezielle Bedrohungen)

- Angriffe auf Protokolle [16], [5], [56], [70], [81], [83], [110], [120]
  - ARP-Spoofing [83]
  - FTP (z. B. FTP Bounce Attack) [56]
  - IP [16], [56], [81], [83], [120]
    - IP-Fragmentierung [56]
      - Tiny Fragment Attack [56]
      - Overlapping Fragment Attack [56]
    - IP-Spoofing [16], [56], [81], [83], [120]
  - ICMP-Protokolls (z. B. Redirect Attack) [16], [56]
  - TCP/IP (z. B. Angriffe auf z/OS-Systeme oder TCP Hijacking) [16], [56], [110]
  - TLS [70]
    - TLS Manipulation der Verhandlungsphase [70]
    - TLS Änderung der Verschlüsselung [70]
  - UDP (z. B. Portscanning) [56]
- Bluetooth [16]
  - Erstellung von Bewegungsprofilen unter Bluetooth [16]
  - Missbrauch der Bluetooth-Profile [16]
  - Schwachstellen in der Bluetooth-Implementierung [16]
  - Unzureichende oder fehlende Bluetooth-Sicherheitsmechanismen [16]
- DNS [16], [56], [112], [83], [110], [120]
  - Ausnutzen dynamischer DNS-Updates [16]
  - Cache-Poisoning [110]
  - DNS-Hijacking [16], [110]
  - DNS Information Leakage [16]
  - DNS-Spoofing [16], [56], [83], [120]
  - Fehlerhafte Konfiguration eines DNS-Servers [16]
  - Top-Level Domain Angriffe [110]
- LAN [16], [56], [110]
  - Eindringen und Manipulation über die Kommunikationsschnittstelle von eingebetteten Systemen [16]
  - Kompromittierung der Protokolldatenübertragung bei zentraler Protokollierung [16]
  - Manipulationen über den ISDN-D-Kanal [16]

  - Manipulation von Managementparametern [16]
  - Manipulation von Routen (Routing Detours) [16]
  - Missbrauch des Source-Routing [16]
  - Missbrauch von Spanning Tree [16]
  - Portscanning [56], [110]
  - Überwindung der Grenzen zwischen VLANs [16]
  - Unberechtigte Ausführung von Netzmanagement-Funktionen [16]
  - Ungenügende Absicherung der SOAP-Kommunikation [16]
- VOIP [16], [94]
  - Fehlerhafte Konfiguration der VoIP-Middleware [16]
  - Fehlerhafte Konfiguration von VoIP-Komponenten [16]
- VPN [16], [83]
  - Erlauben von Fremdnutzung von VPN-Komponenten [16]
  - Fehlerhafte Administration von VPNs [16]
  - Fehlverhalten bei der Nutzung von VPN-Diensten [16]
  - Nutzung des VPN-Clients als VPN-Server [16]
  - Ungeeignete Nutzung von Authentisierungsdiensten bei VPNs [16]
  - Unsichere Konfiguration der VPN-Clients für den Fernzugriff [16]
  - Unsichere Standard-Einstellungen auf VPN-Komponenten [16]
- WLAN [16], [94], [110]
  - Abhören der WLAN-Kommunikation [16], [110]
  - Angriffe auf WLAN-Komponenten [16]
  - Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation [16]
  - Fehlerhafte Konfiguration der WLAN-Infrastruktur [16]
  - Unvollständige Authentifizierung [110]
  - Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen [16]
  - Vollständige Schlüsselsuche [110]

Phase 3: Ausweitung der Rechte

- Nutzung von internen Netzverbindungen für laterale (seitliche) Bewegungen [43]

Phase 4: Zielerreichung

- Integritätsverlust/Tampering der Netze [16], [133]
- Vertraulichkeitsverlust der Netze [16], [133]

A.4. Anwendungen

Phase 1: Informationsgewinnung

- Ausspähen von Informationen/Spionage (Excavation) [16], [5], [108], [153]
  - Fingerprinting [5], [108], [153]
    - passives Fingerprinting [108]
    - fuzzy-os-fingerprinting [108]
  - Footprinting [5]
- „Geschwätzige Dienste“ (zu viele Informationen werden preisgegeben durch login-Meldungen, Versionsnummern, Fehlermeldungen und vieles mehr) [56]
- Reverse Engineering [16], [5], [108]

Phase 2: Angriff auf das Ziel (Allgemeine Bedrohungen)

- Authentisierungsangriffe (z. B. Authentication Abuse, Authentication Bypass) [16], [13], [5], [43], [112], [81], [83], [65], [108], [110], [120], [153]
  - Biometrieangriffe [35], [83], [110]
    - Finger- und Handabdruck [83], [110], [120]
    - Gesichtserkennung [83], [110], [120]
    - Handschrifterkennung [83], [110]
    - Iris-Scan [83], [110], [120]
    - Retina-Scan [83], [110], [120]
    - Stimmerkennung [83], [110]
    - Venen-Scan [83], [110]
  - CAPTCHAS [112]
  - Manipulation kontaktbehafter und berührungsloser Systeme [83], [108], [110], [120]
    - Kontaktkarten [83]
    - Magnetstreifenkarten [83]
    - PKI/Digitale Signaturen [112], [108]
    - Proximity Card [83]
    - RFID [83]
    - Skimming [110]
    - Smart-Cards [83], [108], [120]
  - Passwörtangriffe (z. B. Systematisches Ausprobieren) [16], [112], [65], [153]
    - Brute Force [5], [112], [81], [110], [153]

    - Credential Harvesting (ernten) [43]
    - Nutzung von gebrochenen Passwörtern [110]
    - Passwort erraten [83], [110]
    - Pass-the-Hash [43]
    - Pass-the-Ticket [43]
    - Wörterbuchangriff [81], [110], [120]
- Einspielen/Wiedereinspielen von Nachrichten [16], [70], [83], [110]
- Hijkacking (z. B. Browser Hijacker) [43], [70], [112], [83], [81], [110], [120]
- Kryptographieangriffe [16], [43], [70], [112], [83]
  - Adaptive Chosen-Plaintext Attack [112]
  - Brechen von Schlüsseln [43], [83]
  - Chosen-Plaintext Attack [70], [112]
  - Cyphertext-only Attack [112]
  - Diebstahl von Schlüsseln [43]
  - Fehler in verschlüsselten Daten durch Manipulation [16]
  - Known-Plaintext Attack [70], [112]
  - Kompromittierung kryptographischer Schlüssel [16]
  - Rubber Horse Attack [112]
- Manipulation von Software [16], [5], [153]
  - Code/File Inclusion [5], [153]
  - Manipulation von Daten und Werkzeugen beim Patch- und Änderungsmanagement [16]
  - Software Integrity Attack [5]
  - Unberechtigter Zugriff auf Daten durch Einbringen von Code (z. B. in ein SAP System) [16], [5]
- Repudiation [133]
- Schadsoftware/-programme [1], [16], [11], [13], [35], [43], [56], [112], [81], [83], [94], [66], [65], [110], [120]
  - Bot-Netze [16], [110]
  - Backdoor [1], [43], [112], [83], [110]
  - Bacteria [11]
  - Deworming [1]
  - Dropper [110]
  - Hostile Mobile Code Agent [110]

- Infestation [43]
- Logic Bomb [1], [11], [83], [110]
- Rabbit [1], [11], [110]
- Rootkit [13], [83], [81], [110]
- Script Attack (z. B. Java Script) [110]
- Spyware [1], [83], [65]
- Time Bomb [110]
- Trojanische Pferde (z. B. Remote Access) [1], [16], [11], [13], [56], [112], [81], [83], [65], [110], [120]
- Viren [1], [16], [11], [13], [56], [112], [81], [83], [65], [120]
  - Amored [83]
  - Anti-Anti-Viruses Techniques [1]
  - Betriebssystem [120]
  - Boot [56], [112], [83], [65], [120]
  - Cavity [83]
  - Companion [83], [120]
  - Encryption [1], [112]
  - File [56], [112], [65]
  - Makro [16], [56], [112], [83], [65], [120]
  - Metamorph [1], [112], [83]
  - Multipartite [112], [65], [120]
  - Oligomorphism [1]
  - Polymorph [1], [112], [83]
  - Sector [112]
  - Sparse Infecting [112]
  - Speicherresistent [120]
  - Stealth [1], [112], [83]
- Whack-a-Mole [43]
- Würmer [1], [11], [13], [56], [112], [65], [110], [120]
  - Contagion [120]
  - Flash Worms [120]
  - Hit-List Scanning [120]
  - Permutation Scanning [120]

    - Topological Scanning [120]
  - Zombie [1], [110]
- Spoofing/Identitätsdiebstahl [16], [5], [35], [43], [70], [112], [81], [65], [133], [120], [153]
  - Anmelde-/Sitzungsvorhersage (Imitierung von Nutzern) [153]
  - Content Spoofing [5]
  - Gefälschte Zertifikate [16]
  - Homograph Attack [81]
  - Man-in-the-Middle-Angriff [16], [70], [112], [83]
  - Maskerade [16]
  - Resource Location Spoofing [5]
  - Session Fixation [112], [153]
- Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen [16]
- Software-Schwachstellen oder –Fehler [16], [5], [37], [56], [70], [112], [83], [110], [153]
  - Ausführung von eingeschränkten Dateioperationen (Path Equivalence) [37]
  - Datenverarbeitungsfehler [37]
  - Dateizugriff außerhalb eines eingeschränkten Verzeichnisses (Path Traversal) [37]
  - Directory Traversal [83]
  - Einspielen (Flashen) von manipulierten Software-Updates/-Upgrades (z. B. bei eingebetteten Systemen) [16]
  - Fehlende Input Validation/Input Data Manipulation [5], [112], [83]
  - Falsche Durchsetzung von Daten- und/oder Nachrichtenstrukturen [37]
  - Falsche Einhaltung von/Schlechte Programmierstandards [37]
  - Falsch geschriebene Ausdrücke innerhalb des Codes [37]
  - Falsche Handhabung von Zeigern [37]
  - Falscher Umgang mit Kommunikationskanälen und Zugriffspfaden [37]
  - Falsche Verwendung von Argumenten oder Parametern innerhalb von Funktionsaufrufen [37]
  - Falsche/Unsachgemäße Prüfung und/oder Behandlung von außergewöhnlichen Bedingungen [37]
  - Falscher Vergleich von Entitäten [37]
  - Falscher Zugriff auf indizierbare Ressourcen (‚Range Error‘) [37]

- Fehlerhafte Berechnungen [37]
- Fehlerbedingungen, Rückgabewerte, Statuscodes [37]
- Format String Attacks [153]
- Illegaler Zustandswechsel (z. B. Buffer Overflow - Erzeugung von unverschlüsselten Zuständen) [5], [56], [70], [112], [83], [108], [110]
- Initialisierungs- und Bereinigungsfehler [37]
- Integer Overflow [110], [153]
- Logikfehler [37]
- Missbrauch von Funktionalitäten [5]
- Numerische Fehler [37]
- Off-by-One Fehler [110]
- Parametermanipulation Länge, Typ und Anzahl (z. B. Cookie, HTTP, URL) [5], [112], [83], [110]
- Race Condition (kritischer Wettlauf - Angriff auf geteilte Ressourcen) [56], [83], [110]
- Schutzmechanismusfehler [37]
- Sicherheitsprobleme der Benutzeroberfläche [37]
- Sicherheitsfunktionen (Authentifizierung, Zugriffskontrolle, Vertraulichkeit, Kryptographie und Rechteverwaltung) [37]
- Software-Konzeptionsfehler [16], [37], [56], [112]
  - Audit [37]
  - Authentifizierung (Authenticate Actors) [37]
  - Begrenzung der Zugriffspunkte (entry points) (Limit Exposure) [37]
  - Berechtigung (Authorize Actors) [37]
  - Datenverschlüsselung (Encrypt Data) [37]
  - Identifizierung (Identify Actors) [37]
  - Sperrmechanismen (Lock Computer) [37]
  - Übergreifende Aspekte (Cross Cutting) [37]
  - Überprüfung der Nachrichtenintegrität (Verify Message Integrity) [37]
  - Validierung von Eingaben (Validate Inputs) [37]
  - Verwaltung von Nutzer Sessions (Manage User Sessions) [37]
  - Verstoß gegen Sichere Design-Prinzipien [37]
  - Zugriffsbeschränkung (Limit Access) [37]

  - Time-of-Check to Time-of-Use [110]
  - Unbeendeter Null-Terminated String [110]
  - Undokumentierter Zugangspunkt [110]
  - Unerwartetes Codeverhalten [37]
  - Unsachgemäße Interaktion zwischen mehreren korrekt arbeitenden Entitäten [37]
  - Unsachgemäße Kontrolle einer Ressource während des Life-Cycles [37]
  - Unsachgemäße Verwaltung von Systemressourcen [37]
  - Unsicheres Dienstprogramm [110]
  - Unvollständige Mediation [110]
  - Unzureichendes Kontrollflussmanagement [37]
  - Verwendung von nicht genügend zufälligen Werten [37]
  - Zeit und Zustand [37]

Phase 2: Angriff auf das Ziel (Spezielle Bedrohungen)

- Betriebssysteme [16], [94], [153]
  - Windows [16], [94]
    * Angriffe mit Authentifizierung [94]
    * Angriffe ohne Authentifizierung [94]
    * Fehlerhafte Konfiguration von Windows-/basierten IT-Systemen [16]
    * Kompromittierung von RDP-Benutzersitzungen ab Windows Server 2003 [16]
    * Missbrauch von Administratorrechten bei Windows-Betriebssystemen [16]
    * Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen [16]
    * Vertraulichkeitsverletzung trotz BitLocker-Laufwerksverschlüsselung ab Windows Vista [16]
  - UNIX [16], [94]
    * Angriffe über Remote [94]
    * Angriffe mit lokalem Zugriff [94]
    * Gefälschte Antworten auf XDMCP-Broadcasts bei Terminalservern [16]
    * Methoden nach Kontrolle von Root [94]
    * Missbräuchliche Nutzung eines Unix-Systems mit Hilfe von UUCP [16]

    - Umleiten von X-Window-Sitzungen [16]
  - z/OS [16]
    - Benutzung fremder Kennungen unter z/OS-Systemen [16]
    - Fehlerhafte Konfiguration der Unix System Services unter z/OS [16]
    - Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF [16]
    - Manipulation der z/OS-Systemsteuerung [16]
    - Missbrauch von RACF-Attributen unter z/OS [16]
    - Unbefugtes Erlangen höherer Rechte im RACF [16]
    - Unzureichender Dateischutz des z/OS-Systems [16]
    - Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems [16]
    - Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers [16]
    - Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen [16]
    - Verschleiern von Manipulationen unter z/OS [16]
  - OS Commanding [153]
- Anwendungssoftware/Dienst [16], [5], [37], [43], [56], [112], [81], [83], [94], [136], [108], [110], [153]
  - E-mail [16], [43], [112], [81], [83], [94], [110]
    - E-mail-Spoofing [81]
    - Mitlesen von E-mails [16]
    - Manipulation E-mail-Nachrichten [110]
    - Manipulation des E-mail-Headers [110]
    - Missbrauch aktiver Inhalte in E-Mails [16]
    - Missbrauch von Webmail [16]
    - Vortäuschen eines falschen Absenders [16]
  - Datenbanken [16], [110]
    - Manipulation an Daten oder Software bei Datenbanksystemen [16]
    - Unterlaufen von Zugriffskontrollen über ODBC [16]
    - SQL-Injection Datenbank [16]
    - Verlust der Datenbankintegrität/-konsistenz [16]
  - Groupware [16]
    - Missbräuchliche Groupware-Nutzung (Anwendung und System) [16]

- Web (Anwendung/Service) [16], [5], [37], [43], [56], [112], [81], [83], [94], [136], [108], [110], [153]
  - Angriffe auf das Identitäts- und Zugriffsmanagement bei Web-Services [16]
  - Ausnutzen von Schwachstellen in Backend-Anwendungen [16]
  - Browser Angriffe [43], [110], [153]
    - Man-in-the-Browser [110]
    - Keystroke Logger [43], [81], [110]
    - Page-in-the-Middle [110]
    - Program Download Substitution [110]
    - User-in-the-Middle [110]
    - URL Redirector Abuse - für Social Engineering Angriffe [153]
  - Clickjacking [16], [110]
  - Content Spoofing [153]
  - Cross-Site Request Forgery (CSRF, XSRF, Session Riding) [16], [153]
  - Cross-Site Scripting (XSS) [16], [43], [112], [83], [94], [136], [110], [153]
  - Drive-by-Download [43], [110]
  - Einbindung von fremden Daten und Schadcode bei Webanwendungen und Web-Services [16]
  - Fehlerhafte Anwendung von Standards [16]
  - Fehler in der Logik von Webanwendungen und Web-Services [16]
  - HTTP [153]
    - HTTP Request Splitting [153]
    - HTTP Response Splitting [153]
    - HTTP Request Smuggling [153]
    - HTTP Response Smuggling [153]
  - Injection-Angriffe [16], [5], [43], [83], [94], [136], [108], [110], [153]
    - Command Injection [5], [83]
    - LDAP Injection [83], [153]
    - Mail Command Injection [153]
    - Null Byte Injection [153]
    - SSI Injection [94], [153]
    - SQL Injection [43], [83], [94], [108], [110], [153]
    - XML Injection [83], [153]

  - XPath Injection [153]
  - XQuery Injection [153]
* Informationsgewinnung über Web-Services [16]
* Missbrauch aktiver Inhalte (Browser) [16]
* Missbrauch einer Webanwendung durch automatisierte Nutzung (Änderung von Formulareingaben) [16]
* Missbrauch einer Webanwendung durch automatisierte Nutzung (Ausspähen von Passwörtern) [16]
* Missbrauch von Funktionalitäten [153]
* Missbrauch von Kurz-URLs oder QR-Codes [16], [112]
* Offenlegung vertraulicher Informationen bei Webanwendungen [16], [153]
  - Path Traversal [153]
  - Predictable Resource Location [153]
  - Routing Detour (Man-in-the-middle-attack) [153]
* Umgehung clientseitig umgesetzter Sicherheitsfunktionen von Webanwendungen und Web-Services [16]
* Umgehung der Autorisierung bei Webanwendungen und Web-Services [16]
* Unautorisierte Benutzung web-basierter Administrationswerkzeuge [16]
* Unbefugter Zugriff auf Daten eines anderen Mandanten bei Webanwendungen und Web-Services [16]
* Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen und Web-Services [16]
* Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen [16]
* Unzureichendes Session-Management von Webanwendungen und Web-Services [16]
* Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services [16]
* Watering-Hole [43]
* Web-Bugs (eingebettete Bilder) [16], [110]
* Web-Spoofing (Information Steeling, Link Changing, Image Manipulation) [16], [56], [81], [83]
* XML [16], [136], [108]

      - XML Attribute Blowup [153]
      - XML External Entities (XXE) [153]
      - XML Entity Expansion [153]
      - XML Injection [153]
- Richtlinien [16]
  - Manipulation von Richtlinien in einer SOA [16]
- Cloud [16], [43], [110]
  - Manipulation der Abrechnungsinformationen [16]
  - Missbrauch von Administratorrechten im Cloud-Management [16]
  - Missbrauch von Services [16]
  - Unberechtigter Zugriff auf Daten innerhalb einer Cloud-Storage-Lösung [16]
  - Ungeeignete Konfiguration von Cloud-Diensten und Cloud-Verwaltungssystemen [16]
  - Ungewollte Preisgabe von Informationen durch Cloud Cartography [16]
  - Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Dienstleister [16]
- Samba [16]
  - Fehlkonfiguration der Samba-Kommunikationsprotokolle [16]
  - Fehlerhafte Konfiguration eines Samba-Servers [16]
- Lotus Notes/Outlook [16]
  - Fehlerhafte Konfiguration eines Lotus Domino Servers [16]
  - Fehlerhafte Konfiguration eines Lotus Notes Clients oder eines Fremdclients mit Zugriff auf Lotus Domino [16]
  - Hacking Lotus Notes/Domino [16]
  - Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes/Domino [16]
  - Missbrauch von Programmierschnittstellen unter Outlook [16]
- Verzeichnisdienst [16]
  - Angriffe auf Registries (Diensteverzeichnisse) und Repositories (Metadaten-Speicher) [16]
  - Fehlerhafte Konfiguration des Active Directory [16]
  - Fehlerhafte Konfiguration des LDAP-Zugriffs auf Verzeichnisdienste [16]
  - Fehlerhafte Konfiguration von Verzeichnisdiensten [16]

        * Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff [16]
        * Novell eDirectory [16]
            · Fehlerhafte Konfiguration des LDAP-Zugriffs auf Novell eDirectory [16]
            · Fehlerhafte Konfiguration des Intranet-Clientzugriffs auf Novell eDirectory [16]
            · Fehlerhafte Konfiguration von Novell eDirectory [16]
        * OpenLDAP [16]
            · Fehlerhafte Konfiguration von OpenLDAP [16]
            · Unzureichende Trennung von Offline- und Online-Zugriffen auf OpenLDAP [16]

Phase 3: Ausweitung der Rechte

- Missbrauch von Berechtigungen/Elevation of Privileges [16], [43], [83], [133], [65], [136], [108]
  - Missbrauch von Administratorrechten [16], [43]
  - Missbrauch von Benutzerrechten [16], [65], [136]
    * Passwörter [16], [136]
    * Schlüssel [16], [136]
    * Session Keys [16], [136]
    * Unberechtigtes Überschreiben (z. B. von Archivmedien) [16]
  - Unbefugtes Erlangen höherer Rechte [16], [108]
- Remote [16], [35], [94], [66], [136], [108]
  - Missbrauch von Fernwartungszugängen (z. B. für Managementfunktionen von Routern/durch Missbrauch von SAML-Token in SOA-Umgebungen) [16], [108]
  - Insecure Deseralization [136]

Phase 4: Zielerreichung

- Integritätsverlust/Tampering der Anwendungen [16], [133]
- Vertraulichkeitsverlust der Anwendungen [16], [43], [133], [136]
  - Vertraulichkeitsverlust schützenswerter Informationen (z. B. Steal data at rest or in-transit while it is unencrypted through the application itself or at other vulnerable points in time) [16], [43]
  - Vertraulichkeitsverlust durch Auslagerungsdateien [16]
  - Information Disclosure/Sensitive Data Exposure [133], [136]

A.5. Menschen

Phase 1: Informationsgewinnung

- Ausspähen von Informationen (z. B. durch Malicious Hacker/Espionage) [16], [112], [66]
  - Beeinträchtigung durch Großveranstaltungen [16]
  - Beeinträchtigung durch wechselnde Einsatzumgebung [16]
  - Gefährdung durch Reinigungs- oder Fremdpersonal [16]
  - Großereignisse im Umfeld [16]
  - Missbrauch sozialer Netzwerke [16]
  - Unberechtigte Nutzung oder Administration von Geräten und Systemen [16]
  - Weitergabe von Daten an Dritte (z. B. durch den Outsourcing-Dienstleister) [16]
- Social Engineering [16], [5], [99], [108]
  - Informationserhebung [5], [108]
  - Sorglosigkeit im Umgang mit Informationen [16]
  - Weitergabe falscher oder interner Informationen [16]

Phase 2: Angriff auf das Ziel

- Social Engineering [16], [13], [5], [35], [56], [112], [81], [83], [99], [65], [108], [110]
  - Baiting [112]
  - Drive-by-Pharming [83]
  - Fehlende Identifizierung zwischen Gesprächsteilnehmern [16]
  - Informationserhebung [5], [108]
  - Manipulation durch Familienangehörige und Besucher [16]
  - Manipulation menschlichen Verhaltens [13], [5]
  - Nötigung, Erpressung oder Korruption [16], [13], [112], [65]
  - Pharming [16], [13], [35], [81], [83]
  - Phishing [16], [13], [35], [43], [112], [81], [83], [110]
    - Content-Injection Phishing [81]
    - Deceptive Phishing [81]
    - Malware-Based Phishing (Keyloggers, Screenloggers, Session Hijackers, Web Trojans, Host File Poisoning, System Reconfiguration Attacks, Data Theft) [81]
    - Man-in-the-Middle Phishing [81]

    - Search Engine Phishing [81]
  - Reverse Social Engineering [13]
  - Spear Phishing [43], [112], [81], [83]
  - SPIT und Vishing [16], [13], [112], [83]
  - Sorglosigkeit im Umgang mit Informationen [16]
  - Tailgaitng [112]
  - Unzureichende Identifikationsprüfung von Kommunikationspartnern [16]
  - Vortäuschen falscher Anrufer-Telefonnummern oder SMS-Absender [16]
  - Weitergabe falscher oder interner Informationen [16]
- Fehler und Unterlassung (Error and Omissions) in der Administration [16], [37], [43], [56], [112], [94], [136], [66]
  - Administration [16], [43], [112], [136]
    - Administrationsfehler bei Web-Services [16]
    - Falsche Vergabe von Zugriffsrechten (z.B im Novell eDirectory) [16]
    - Fehlende oder ungeeignete Segmentierung [16]
    - Fehlerhafte Administration eines DBMS [16]
    - Fehlerhafte Administration von Routern und Switches [16]
    - Fehlerhafte Administration von Zugangs- und Zugriffsrechten (z. B. nicht gepflegte oder gelöschte Accounts) [16], [43], [94]
    - Fehlerhafte Einbindung eines Internet Information Server (z. B. Microsoft IIS) in die Systemumgebung [16]
    - Fehlerhafte Netzanbindungen eines Virtualisierungsservers [16]
    - Nutzung von Komponenten mit bekannten Schwachstelle [136]
    - Schwache Passwörter [112]
    - Unzureichende Protokollierung und/oder Monitoring [43], [136]
  - Konfiguration [16], [37], [56], [112], [94]
    - Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client [16]
    - Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client [16]
    - Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen [16]
    - Fehlerhafte Konfiguration von Exchange [16]
    - Fehlerhafte Konfiguration von Mac OS X [16]
    - Fehlerhafte Konfiguration von Outlook [16]

    - Fehlerhafte Konfiguration von Routern und Switches [16], [94]
    - Fehlende und ungenügende Implementierungen bzw. Konfigurationen in einer SOA [16]
    - Fehlerhafte Zuordnung von Ressourcen des SAN [16]
    - Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen [16]
    - Konfigurationsfehler [16]
    - Konfigurationsfehler bei Web-Services [16], [94]
    - Probleme bei der IPSec-Konfiguration [16]
    - Ungeeignete Konfiguration der aktiven Netzkomponenten [16]
    - Ungeeignete Konfiguration des Managementsystems [16]
  - Mangelnde Erfahrung/Unwissenheit [16], [112]
    - Fehleinschätzung der Relevanz von Patches und Änderungen [16], [94]
    - Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung [16], [43]
    - Fehlende Policies (z. B. Incident Response Plan) [43], [112], [94]
    - Fehlerhafte Administration bei der Protokollierung [16]
    - Fehlerhafte Auswahl von relevanten Protokolldaten [16]
    - Fehlinterpretation von Ereignissen [16]
    - Fehlplanung oder fehlende Anpassung [16]
    - Unsichere kryptographische Algorithmen [16], [94]
    - Veralten von Kryptoverfahren [16]
    - Verstoß gegen Gesetze oder Regelungen (z. B. beim Einsatz kryptographischer Verfahren) [16]
- Fehler und Unterlassung (Error and Omissions) in der Nutzung [16], [112], [66]
  - Fahrlässigkeit [16], [112]
    - Bedienungsfehler [16], [112]
    - Falscher Umgang mit defekten Datenträgern [16]
    - Fehlbedienung von Kryptomodulen [16]
    - Fehlerhafte Nutzung eines Cloud Services [16]
    - Kein ordnungsgemäßer PC-Benutzerwechsel [16]
    - Informationen/Produkte aus unzuverlässiger Quelle [16]
    - Nichtbeachtung von Sicherheitsmaßnahmen [16]
    - Server im laufenden Betrieb ausschalten [16]

    - Schlechte oder fehlende Authentikationsverfahren und -mechanismen [16]
    - Unbeabsichtigte Datenmanipulation [16]
    - Undokumentierte Funktionen [16]
    - Ungeeigneter Umgang mit Passwörtern oder anderen Authentifikationsmechanismen [16]
    - Ungeeignetes Verhalten bei der Internet-Nutzung (z. B. Softwaredownload) [16], [112]
    - Ungenehmigte Nutzung von externen Dienstleistungen [16]
    - Ungeregelte und sorglose Nutzung von Druckern, Kopierern und Multifunktionsgeräten [16]
    - Unerlaubte private Nutzung des dienstlichen Mobiltelefons, Smartphones, Tablets oder PDAs [16]
    - Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners [16]
    - Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme [16]
    - Unstrukturierte Datenhaltung [16]
    - Verlust von BitLocker-verschlüsselten Daten [16]
    - Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten [16]
  - Vorsatz (Employee Sabotage) [16], [112], [66]
    - Abstreiten von Handlungen [16]
    - Einschleusen von Programmen [65]
    - Falsche Dateneingabe [65]
    - Mangelhafte Akzeptanz von Informationssicherheit [16]
    - Missbrauch personenbezogener Daten [16]
    - Missbrauch von Werten oder Informationen [112]
    - Modifizierung von Daten [65]

Phase 3: Ausweitung der Rechte

- über Anwendungen, IT-Systeme, Netze

Phase 4: Zielerreichung

- Zugang/Zutritt/Zugriff zu Infrastruktur, Anwendungen, IT-Systemen, Netzen

A.6. Informationsräume

Phase 1: Informationsgewinnung

- Identifizierung von Geheimhaltungsgraden
- Identifizierung von wichtigen operationellen Knoten

Phase 2: Angriff auf das Ziel

- Abgreifen von Informationen, wenn sie unverschlüsselt sind [43]
- Einschleusen falscher Inhalte in eingestufte Dokumente
- Einschleusen falscher eingestufter Dokumente
- Fehlende Kennzeichnung der Geheimhaltungsgrade [84]
- Fehlerhafte, Falsche Auswahl des Geheimhaltungsgrades [112]
- Fehlende Kontrolle der Geheimhaltungsgrade
- Fehlerhafte Verwaltung von Datenträgern [84]
- Informationsfluss von oben (z. B. GEHEIM) nach unten (z. B. Öffentlich) [6]
- Überwindung der physikalischen Grenzen zwischen Informationsräumen
- Unbefugtes Eindringen in Informationsräume
- Verändern von Daten während der Übertragung [84]
- Verlust, Verfälschung gespeicherter Daten [16]
- Verstöße gegen den Grundsatz „Kenntnis nur wenn nötig“

Phase 3: Ausweitung der Rechte

- Änderung der Höhe der Sicherheitsüberprüfung des Personals
- Manipulation der Geheimhaltungsgrade

Phase 4: Zielerreichung

- Integritätsverlust/Tampering der Informationsräume
- Vertraulichkeitsverlust (z. B. Informationsabfluss aus höheren Geheimhaltungsgraden)