**Technische Universität Ilmenau**

**Fakultät Wirtschaftswissenschaften und Medien**

**Fachgebiet Informations- und Wissensmanagement**

**Univ.-Prof. Dr. Dirk Stelzer**

**Hauptseminar Informationsmanagement**

**im WS 2016/2017**

Thema Nr. 8

# Monitoring von Cyber-Attacken – Vergleich von Verfahren zur Anomalieerkennung

vorgelegt von:

Arning, Ann-Katrin

Karl-Liebknecht-Straße 1, 98693 Ilmenau

0172 8804748

ann-katrin.arning@tu-ilmenau.de

55406

Wirtschaftsinformatik

**Zusammenfassung**

Die zunehmende Kommunikation über Netzwerke und das Internet führt dazu, dass diese Infrastrukturen ein immer interessanteres Angriffsziel darstellen. Die Zahl der Cyber-Angriffe steigt, ebenso wie deren Professionalität. In den letzten Jahren wurde daher nach effektiven wie auch effizienten Verfahren gesucht, Anomalien auf Rechnern und in Netzwerken aufzuspüren um erkennen zu können, ob eine Attacke auf ein Gerät bzw. das Netzwerk erfolgreich durchgeführt wurde und dadurch die Sicherheit der eigenen Daten bedroht ist. Verfahren aus den letzten fünf Jahren sollen in dieser Arbeit vorgestellt und verglichen werden. Ziel ist es festzustellen, für welche Systeme sie sich eignen und wie effektiv diese sind.

**Abstract**

**Monitoring of Cyber Attacks – a Comparison of Anomaly Detection Techniques**

Increasing communication over networks and the Internet means that these infrastructures are an increasingly interesting target. The number of cyber-attacks is growing, as is their professionalism. In recent years, effective as well as efficient methods have been identified to detect anomalies on computers and in networks in order to detect an attack on a device or the network and find out whether the security of one's data is threatened. In this work methods developed in the past five years are introduced and compared to each other in order to determine which systems they are suitable for and how effective they are.

**Inhaltsverzeichnis**

# Abkürzungsverzeichnis

| | |
|---|---|
| ACCEPT | Anomaliemanagement in Computersystemen durch Complex Event Processing Technologie |
| ANSII | Anomalieerkennung und eingebettete Sicherheit in industriellen Informationssystemen |
| APT | Advanced Persistent Threat |
| AS | Autonomes System |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CAD | Content Anomaly Detection |
| CEP | Complex Event Processing |
| DoS | Denial-of-Service |
| FPR | False Positive Rate |
| GVK | Gemeinsamer Verbundkatalog |
| HIVE | Hypervisor-basierte innovative Verfahren zur Anomalieerkennung mit Hardwareunterstützung |
| iAID | innovative Anomaly- and Intrusion-Detection |
| ISP | Internet Service Provider |
| SDN | Software Defined Networking |
| TPM | Trusted Platform Module |
| TPR | True Positive Rate |
| VM | virtuelle Maschine |
| VMI | Virtual Machine Introspection |

# Tabellenverzeichnis

# 1 Einleitung

## 1.1 Problemstellung

In den vergangenen Jahren ist die Zahl der Cyberangriffe weltweit gestiegen. Wurden Netzwerke von Firmen im Jahr 2009 noch 3,4 Millionen mal angegriffen, so waren es 2014 bereits 42,8 Millionen gemeldete Attacken.[1]

Der Bericht zur Lage der IT-Sicherheit in Deutschland 2016, herausgegeben durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), stellt klar, dass man aufgrund „der dynamischen Bedrohungslage und der zunehmenden Professionalisierung der Angreifer […] heute davon ausgehen [muss], dass die Netzgrenzen der IT-Systeme überwunden werden können.“[2] Ein frühes Erkennen einer Infiltration ist daher wichtig, um „die negativen Effekte des Angriffs [zu] minimieren“[3].

Für die Erkennung von Angriffen gibt es zwei grundsätzlich verschiedene Ansätze, welche in Werkzeuge zum Monitoring von Cyber-Attacken implementiert werden: Zum einen die Mustererkennung, welche eine Infiltration anhand bereits vorhandener Muster vorangegangener Attacken im Datenverkehr aufdeckt.[4] Zum anderen die Anomalieerkennung, welche Abweichungen von normalem Verhalten aufspürt und als Bedrohung erkennen kann.[5] Die Anomalieerkennung ist im Hinblick auf das Erkennen von neuartigen Attacken der Mustererkennung überlegen, da bei einem solchen Angriff noch keine Informationen über das Verhalten der Attacke bekannt ist, dieses Verhalten aber mit großer Sicherheit von einem normalen Datenverkehr abweichen wird.[6]

In den letzten Jahren gab es einige Forschungen und Entwicklungen im Bereich der Anomalieerkennung, gefördert von Firmen, Universitäten, Ministerien und Ländern, um für eine höhere Sicherheit in Netzwerken zu sorgen.[7]

---

[1] Vgl. PwC /Anzahl Cyberangriffe/
[2] BSI /Lagebericht 2016/
[3] ebenda
[4] Vgl. Milliken /Intrusion Detection/ 345
[5] Vgl. ebenda
[6] Vgl. ebenda
[7] Vgl. z. B. Treinen, Thurimella /Rule Mining/; Gao, Reiter, Song /Distance Measurement/; Mehdi, Khalid, Khayam /Software Defined Networking/; Fiedler et al. /Anomalieerkennung CAIS/ und Gad /Schlussbericht iAID Frankfurt/

## 1.2 Zielsetzung

Ziel dieser Arbeit ist es, Verfahren der Anomalieerkennung zu beschreiben und zu vergleichen. Insbesondere sollen folgende Forschungsfragen beantwortet werden:

- Welche Verfahren eignen sich für welche IT-Systeme?
- Wie zuverlässig sind die Verfahren?
- Wo liegen die Grenzen der Anomalieerkennung?

## 1.3 Methodik

Um verschiedene Verfahren der Anomalieerkennung zu untersuchen, wird eine Literaturrecherche durchgeführt. Hierzu wird der gemeinsame Verbundkatalog (GVK) herangezogen. Da der Fokus dieser Arbeit auf den neuesten Erkenntnissen in Bezug auf Anomalieerkennung liegen soll, wird in der Datenbank nur solche Literatur betrachtet, welche zwischen 2011 und 2016 publiziert wurde.

Es wurden zwei Suchstrings definiert, mit welchen die Datenbank durchsucht werden soll. Der Suchstring soll deutlich machen, dass nach Verfahren der Anomalieerkennung im Bereich der Angriffserkennung gesucht wird. Zum einen für die englische Suche: ‚anomaly detection intrusion detection network', zum anderen für deutsche Literatur: ‚anomalieerkennung'. Der Zusatz *network* in der englischen Suchformel soll sicherstellen, dass sich die Verfahren auch auf Netzwerke beziehen. Auf die Begriffe *intrusion detection* und *network* bzw. deren Übersetzung wird bei der deutschen Suche verzichtet, da sie die Ergebnisse zu sehr einschränken.

Bei der Sichtung der Ergebnisse wird darauf geachtet, dass sich die in den Veröffentlichungen beschriebenen Verfahren der Anomalieerkennung auf das Monitoring von Cyber Angriffen übertragen lassen. Die einzelnen Verfahren werden zusammenfassend beschrieben, sodass nicht die Ergebnisse verschiedener Forschungsprojekte im Vordergrund stehen, sondern die übergeordneten Herangehensweisen an die Anomalieerkennung. Eingeordnet werden die Ergebnisse anhand der von García-Teodoro et al. entwickelten Kategorien[8].

[8] *Statistical-based*, *knowledge-based* und *machine learning-based*. Vgl. García-Teodoro et al. /Anomaly-based intrusion detection/ 20

### 1.4 Aufbau

Das zweite Kapitel dieser Arbeit widmet sich den Grundlagen von Cyber-Attacken und deren Überwachung und ordnet die Anomalieerkennung in den Kontext des Monitorings ein.

Im dritten Kapitel werden verschiedene Verfahren der Anomalieerkennung vorgestellt, welche in einem vierten Kapitel verglichen werden. Aufbauend auf dem Vergleich sollen die im Abschnitt ‚Zielsetzung' genannten Forschungsfragen beantwortet werden.

Im Anschluss daran folgen Zusammenfassung, Ausblick und Fazit der Arbeit.

## 2 Grundlagen der Cyber Security

### 2.1 Cyber-Attacken

Cyber-Attacken sind Angriffe aus dem Internet. Darunter wird ein „nicht autorisierte[r] Zugriff bzw. [ein] nicht autorisierte[r] Zugriffsversuch auf das System"[9] verstanden. Angriffe gefährden unter anderem Vertraulichkeit, Datenintegrität oder Verfügbarkeit.[10]

Bei Angriffen wird zwischen den Arten der Bedrohung entschieden. Dazu gehört das *Abhören* einer Kommunikation, das *Verändern, Löschen oder Einfügen von Daten* oder das gezielte *Verzögern und Wiedereinspielen von Daten*. Gibt sich der Angreifer als eine vertrauenswürdige Instanz aus, um Zugang auf ein ansonsten unzugängliches System zu erhalten, wird von *Maskierung* gesprochen. Bei einer *Autorisierungsverletzung* stehen dem Angreifer erweiterte Rechte (z. B. Administratorrechte) zur Verfügung, welche er nicht haben sollte. Eine weitere Art der Bedrohung stellt das *Abstreiten von Ereignissen* dar, wobei eine Instanz vorgibt, an einem bestimmten Ereignis (z. B. Bestellvorgang) nicht beteiligt gewesen zu sein. Eine letzte Bedrohungsart bildet die *Sabotage*. Dazu zählen so genannte Denial-of-Service (DoS) Attacken, welche die Verfügbarkeit von Diensten oder Systemen gefährden.[11]

Immer häufiger werden die oben genannten Bedrohungsarten kombiniert, um möglichst wirkungsvolle und komplexe Angriffe durchzuführen. Bezeichnet werden diese als Advanced Persistent Threats (APTs). Durch die Verteilung wirken einzelne Angriffe

[9] Eckert /IT-Sicherheit/ 19
[10] Vgl. ebenda
[11] Vgl. zum Absatz Bless et al. /Sichere Netzwerkkommunikation/ 14 ff.

weniger bedrohlich und der eigentliche Angriff kann zum einen schwerer vorhergesagt, zum anderen im Nachhinein auch schlechter rekonstruiert werden.[12]

## 2.2 Monitoring von Cyber-Attacken

Das Erkennen von Angriffen auf ein System ist schwierig, vor allem angesichts der immer komplexer werdenden Attacken. Es muss davon ausgegangen werden, dass nicht mehr alle Angriffe abgewehrt werden können. Immer wichtiger wird es daher, bereits erfolgreich durchgeführte Angriffe zu erkennen und Gegenmaßnahmen zu ergreifen.[13] Nur ein „intensives Beobachten […] der gefährdeten Ressourcen“[14] gibt Hinweise auf nicht erwünschten Datenverkehr innerhalb des Systems. Dieses Vorgehen wird als *Monitoring* bezeichnet. Zu den Aufgaben des Monitoring zählen beispielsweise das Sammeln von Informationen, die Analyse des Datenverkehrs oder die Problemdiagnose.[15] Die Ergebnisse des Monitorings werden anschließend grafisch aufgearbeitet und in entsprechenden Tools sichtbar gemacht.

## 2.3 Methoden zur Erkennung von Angriffen

### 2.3.1 Mustererkennung

Die Mustererkennung dient dazu, in Abläufen oder Datenströmen innerhalb des Systems ein Muster zu entdecken, welches bereits durch frühere Angriffe bekannt ist und auf Basis dessen einen Angriff zu erkennen.

Ein wichtiger Aspekt dabei ist, dass bei dieser Monitoringmethode tatsächlich nur in bekannten Mustern eine Bedrohung entdeckt werden kann. Dies bedeutet, dass das System mit aktuellen Mustern bekannter Bedrohungen auf den neusten Stand gebracht werden muss, sodass diese Bedrohungen auch erkannt werden können. Dem System unbekannte Angriffe werden durch diese Methode nicht aufgedeckt.[16] Diesem

[12] Vgl. zum Absatz Leopold et al. /Einleitung CAIS/ 6
[13] Vgl. BSI /Lagebericht 2016/
[14] Eckert /IT-Sicherheit/ 20
[15] Vgl. de Godoy Stênico, Ling /Network Traffic Monitoring/
[16] Vgl. zum Absatz Milliken /Intrusion Detection/ 345

wesentlichen Nachteil steht der Vorteil gegenüber, dass das Konzept sehr gute Ergebnisse bei der Erkennung bereits bekannter Angriffe liefert.[17]

Bekannte Antivirenprogramme wie beispielsweise *AntiVir* von *Avira* arbeiten unter anderem mit einer erkennungsmusterbasierten Virenerkennung.[18]

### 2.3.1 Anomalieerkennung

Im Gegensatz zur Mustererkennung benötigt die Anomalieerkennung keine Informationen über bereits bekannte Angriffe in Form von Signaturen oder Mustern. Bei diesem Ansatz ist das normale Verhalten des Systems bekannt. Was von diesem bekannten Verhalten abweicht, wird als Anomalie erkannt und deutet auf einen Angriff hin. Hier löst ein anomales Verhalten einen Alarm aus, nicht wie bei der Mustererkennung ein bekanntes auffälliges Verhalten.[19]

Der wesentliche Vorteil bei der Anomalieerkennung ist, dass auch bisher unbekannte Angriffe entdeckt werden können.[20] Die Wahrscheinlichkeit, dass ein Angriff erkannt wird, ist bei bekannten sowie unbekannten Bedrohungen gleich hoch. Im Hinblick darauf, dass durchschnittlich täglich 160.000 neue Bedrohungsmuster[21] bekannt werden, verspricht die Anomalieerkennung einen besseren Schutz als die Mustererkennung.

## 3 Verfahren zur Anomalieerkennung

Bereits im Jahr 2008 gab es eine Untersuchung von Pedro García-Teodoro et al. zu verschiedenen Verfahren der Anomalieerkennung. Die Autoren erarbeiteten drei Hauptkategorien, in welche sich die Ansätze einteilen lassen. Es handelt sich dabei um die Kategorien *statistical-based*, *knowledge-based* und *machine learning-based*.[22] Diese sollen im Folgenden übernommen werden und der Einteilung der neusten Entwicklungen im Bereich der Anomalieerkennung dienen.

[17] Vgl. García-Teodoro et al. /Anomaly-based intrusion detection/ 19
[18] Vgl. Avira /Maximale Sicherheit/
[19] Vgl. zum Absatz García-Teodoro et al. /Anomaly-based intrusion detection/ 19
[20] Vgl. ebenda
[21] Vgl. Gold /Malware Samples/
[22] Vgl. García-Teodoro et al. /Anomaly-based intrusion detection/ 20

## 3.1 Statistical-based

### 3.1.1 Analyse von NetFlow-Daten innerhalb von ISPs

Ein Verbundprojekt der Universität Darmstadt entwickelte ein Verfahren zur Anomalieerkennung bei Internet Service Providern (ISPs). Dabei werden NetFlow-Daten innerhalb des Netzes eines ISPs über ein Zeitfenster gesammelt und ein Wert für deren Entropie gebildet. Der Wert kann über die Quell-IP, den Quell-Port, Ziel-IP oder Ziel-Port gebildet werden. Möglich wäre auch, die Metriken zu kombinieren. Falls die Entropie die durchschnittliche Entropie der letzten $n$ Zeitfenster, abzüglich eines Schwellwertes, unterschreitet, wird eine Anomalie erkannt. [23]

Die an der Anomalie beteiligten Hosts werden anderen ISPs mitgeteilt. Um zu gewährleisten, dass die Daten von diesen ISPs ausgewertet werden können, werden lediglich ausgehende NetFlows mit Ziel-IP und Ziel-Port untersucht. So hat jeder ISP die Möglichkeit, an einem Angriff beteiligte Hosts zu blockieren. Die Kommunikation zwischen den ISPs trägt außerdem dazu bei, dass die Rate der falsch erkannten Anomalien sinkt.[24]

Das beschriebene Verfahren setzt außerdem Fuzzy Logic ein, um die Art des Angriffs zu bestimmen.[25] Doch da das eigentliche Verfahren der Anomalieerkennung nicht auf maschinellem Lernen beruht, wurde es den statistischen Verfahren zugeordnet.

### 3.1.2 Trusted Computing

Bei diesem als statistisch eingestuften Ansatz geht es darum, die Integrität von Geräten innerhalb eines Netzwerkes zu gewährleisten. Als Anomalie wird hier „eine Veränderung der Gerätefirmware die nicht durch ein Firmware-Update des Herstellers verursacht wurde ebenso [verstanden], wie das nachträgliche und unplanmäßige Ausführen von nicht autorisierten Programmen auf einem Gerät“[26] [27].

Auf jedem System (hier: Gerät) befindet sich ein Trusted Platform Module (TPM), welches vor dem eigentlichen Systemstart aktiviert wird und jeden Schritt des Boot-Vorgangs kryptographisch misst. Aus der Messung wird ein Hash-Wert generiert, sodass sich zum Ende des Boot-Vorgangs eine Hash-Kette bilden lässt. Anhand dieser Hash-

[23] Vgl. zum Abschnitt Baier, Abt /Anomalieerkennung INSAIN/ 55-58
[24] Vgl. zum Abschnitt ebenda 50
[25] Vgl. Baier, Abt /Anomalieerkennung INSAIN/ 57
[26] Dreher, Kehrer /Schlussbericht ANSII Neckartenzlingen/ 8
[27] Kommafehler aus Dokument übernommen

Kette kann abgeglichen werden, ob der Bootvorgang dem erwarteten Prozess entspricht. Auch nach dem Bootvorgang überwacht das TPM das Starten von Programmen und Prozessen. Konzipiert wurde das vorgestellte Verfahren für Geräte im industriellen Bereich, welche meist nach einem Regelwerk oder einer Definition aufgesetzt werden und sich stark gleichen und somit gut überwachen lassen.[28]

Die Idee, TPM zur Anomalieerkennung einzusetzen, wurde ebenfalls vom Projekt ‚Hypervisor-basierte innovative Verfahren zur Anomalieerkennung mit Hardwareunterstützung' (HIVE) aufgegriffen. Bei diesem Ansatz sollten Systemkomponenten virtualisiert werden, was die Komplexität der Systemzusammenhänge verringert. Im Gegensatz zum oben beschriebenen Ansatz sollte das System allerdings in der Lage sein, normales Verhalten durch maschinelles Lernen selbst zu erlernen.[29] [30]

### 3.1.3 Inter-AS Routing Anomalien

Um Anomalien nicht nur in einem abgeschlossenen System wie dem eigenen Netzwerk zu identifizieren, sondern globale Anomalien zu erkennen, wurde 2014 das sogenannte MonIKA-Framework entwickelt, welches Betreibern von Rechensystemen[31] erlaubt, Monitoring-Daten auszutauschen. Wichtig hierbei war es, die verschiedenen Interessen der Teilnehmer zu berücksichtigen und diese Daten so weit wie möglich zu anonymisieren.[32]

Die Erkennung von Anomalien wie beispielsweise Spoothing oder Hijacking basiert dabei auf bereits publizierten Forschungen[33] und wird auf den Monitoring-Daten der beteiligten Betreiber von Rechensystemen ausgeführt. Die Anomalieerkennung wird, zusätzlich zu den bekannten Verfahren, durch das Sammeln und Auswerten zusätzlicher Daten erweitert. Dazu gehören Routing-Beziehungen aus vertrauenswürdigen Quellen um abzuleiten, ob einer Subnetzmaske vertraut werden kann. Dies hilft dabei, auftretende Anomalien weiter als legitim oder illegitim zu klassifizieren.[34]

---

[28] Vgl. zum Absatz Dreher, Kehrer /Schlussbericht ANSII Neckartenzlingen/ 9
[29] Vgl. zum Absatz Wagner, Wessel /Schlussbericht HIVE Garching/ 3-4
[30] Leider war der Schlussbericht zu Arbeitspaket 3, den innovativen Sicherheitsmechanismen zur Anomalieerkennung, nicht verfügbar, sodass keine genaue Beschreibung ausformuliert werden konnte.
[31] Autonome Systeme (AS)
[32] Vgl. zum Absatz Meier /Schlussbericht MonIKA Wachtberg/ 3
[33] Vgl. Lad et al. /PHAS/; Qiu et al. /Bogus Route Information/ und Zhao et al. /Invalid Routing Announcement/
[34] Vgl. zum Absatz Wübbeling, Meiser, Elsner /Routing Anomalies/ 229-234

### 3.1.4 Analyse von Dateizugriffen

Zu Cyber-Angriffen gehört auch die Spionage vertraulicher (Firmen-)Daten. Eine Möglichkeit, einen solchen Vorfall zu erkennen, wurde von Gates et al. entwickelt. Sie stufen den Informationsgehalt eines Dokumentes anhand seiner Position innerhalb des Systems (Ordnerstruktur) und den Zugriffen anderer Nutzer darauf ein. Anhand des üblichen Verhaltens eines Nutzers kann dann festgestellt werden, ob der aktuelle Zugriff auf ein bestimmtes Dokument seinem vergangenen Verhalten entspricht. Wurde das entsprechende Dokument, auf welches der Nutzer zugreift, als wesentlich wichtiger eingestuft als die bisherigen Dokumente, so kann dies auf einen Fall von Spionage hindeuten.[35]

Die Arbeiten von Gates et al. konzentrierten sich auf das Aufdecken von Spionage durch Mitarbeiter. Es sollte allerdings ohne weiteres möglich sein, durch den oben beschriebenen Ansatz auch Zugriffe durch eingeschleuste Malware zu erkennen.

Auch Salem und Stolfo entwickelten einen ähnlichen Ansatz, bei welchem ein Zugriffsprofil des Nutzers erstellt wird. Salem und Stolfo gehen davon aus, dass das Suchverhalten eines maskierten Angreifers durch eine größere Anzahl an Zugriffen und einem weniger zielgerichteten Suchverhalten aufgedeckt werden kann.[36]

## 3.2 Knowledge-based

Wissensbasierte Systeme, hier auch als Expertensysteme bezeichnet, implementieren oft eine der anderen beiden Ansätze der Anomalieerkennung, weshalb diesem Abschnitt kein eigenes Verfahren zugeteilt wurde. [37]

## 3.3 Machine learning-based

### 3.3.1 Analyse von Log-Dateien

Eine Möglichkeit, Anomalien in einem System zu erkennen, stellt die Analyse von Log-Dateien dar. Alle relevanten Log-Dateien werden gesammelt und ausgewertet. Dazu gehören beispielsweise Logs von Firewalls, Anwendungsservern, Tools zur

[35] Vgl. zum Absatz Gates et al. /File Access/ 384
[36] Vgl. zum Absatz Salem, Stolfo /Search Behavior/ 181
[37] Vgl. García-Teodoro et al. /Anomaly-based intrusion detection/ 21

Leistungsmessung oder Intrusion Detection Systemen.[38] Innerhalb der Logs werden sogenannte Atome (einzelne Zeichen oder Zeichenketten) gesammelt, über welche wiederum zusammenhängende Regionen erkannt werden können. Hierzu orientiert sich der Algorithmus an der Mustererkennung aus der Bioinformatik. Tritt bei einem nächsten Aufruf ein Ereignis auf, zu welchem weitere Atome innerhalb einer Region fehlen (entsprechende Einträge in der Firewall oder bestimmte Ressourcen innerhalb des Requests), so kann dies als Anomalie und somit als Angriff gewertet werden.[39]

Das beschriebene System durchläuft zwei Phasen, welche nach einer bestimmten Zeit parallel ablaufen. Zum einen die Lernphase, in welcher das System den normalen Zustand erlernt. Hier treten häufiger Alarme auf, welche von autorisiertem Personal als normal oder verdächtig eingestuft werden müssen. Aus den Erkenntnissen lernt das System bis es in die Betriebsphase übergeht. Doch auch während dieser Phase ist der Einsatz einer Person notwendig, welche neue Vorkommnisse mithilfe entsprechenden Knowhows einstufen kann. Aus der Einstufung leitet das System ab, welche Ereignisse zum normalen Verhalten zählen und was als Anomalie eingestuft werden muss.[40]

Andere Ansätze schränken sich bei der Verwendung von Log-Dateien ein. 2014 stellten Manadhata et al. einen Ansatz vor, bei welchem sie die Daten aus den HTTP Proxy Logs eines Unternehmens in einen Graphen übertrugen, in welchem jeder Knoten für einen Host und jede Kante für eine Verbindung stand. Durch eine aus Unternehmensinformationen gewonnene *ground truth*, welche Hosts als schädlich gelten und welche nicht, und der Anwendung eines *belief propagation* Algorithmus[41] konnte mit hoher Wahrscheinlichkeit kalkuliert werden, welche der weiteren Hosts infiltriert waren.[42]

### 3.3.2 Complex Event Processing (CEP)

Ein weiterer Ansatz, Anomalien mithilfe maschinellen Lernens zu erkennen, ist die Erweiterung und Analyse von NetFlow-Daten. Im Projekt ‚innovative Anomaly- and Intrusion-Detection' (iAID) des Bundesministeriums für Bildung und Forschung wurde ein neues Datenformat entwickelt, die so genannten IAS-Flow-Daten, welche auf

[38] Vgl. Fiedler et al. /Anomalieerkennung CAIS/ 92
[39] Vgl. zum Absatz Fiedler et al. /Anomalieerkennung CAIS/ 93
[40] Vgl. zum Absatz ebenda 94
[41] Vgl. Yedidia, Freeman, Weiss /Belief Propagation/
[42] Vgl. zum Absatz Manadhata et al. /Graph Inference/ 3-6

NetFlow basieren.[43] Zusätzlich zu den Informationen, welche NetFlow-Sensoren innerhalb des Netzwerks liefern, werden unter anderem Zähler erfasst, welche zuvor definiert werden können (z. B. Anzahl der Paket Header).[44] Eine Complex Event Processing (CEP) Engine bereitet die Daten weiter auf und erstellt zusätzliche Ereignisse durch die Korrelation über Zeit und Reihenfolge der IAS-Flow-Daten.[45]

Die so gesammelten und erzeugten Daten werden an die Anomalieerkennung weitergeleitet, welche aus zwei Phasen besteht: In einem ersten Schritt werden die Ereignisse anhand „von einfachen statischen Regeln bis hin zu intelligenten Automatismen (z.B. K-Means etc.)“[46] in drei Cluster eingeteilt, den White-, Black- und Grey-Listen. Ereignisse der erstgenannten Liste sollen im Anschluss nicht weiter untersucht werden, sie gehören zum harmlosen Datenverkehr. Ereignisse aus der zweitgenannten Liste werden dem Administrator mitgeteilt. Inhalte der Grey-Liste werden durch „gängige Verfahren wie Probabilistische Neuronale Netze“[47] untersucht (zweite Phase der Anomalieerkennung) und in die White- bzw. Black-Liste eingetragen.[48] Da K-Means und Neuronale Netze zu selbstlernenden Verfahren zählen, wurde diese Art der Anomalieerkennung dem maschinellen Lernen zugeordnet.

Einen alternativen Ansatz, Complex Event Processing einzusetzen, untersuchte das Projekt ‚Anomalieerkennung in Computersystemen durch Complex Event Processing Technologie‘ (ACCEPT). Als Ergebnis entwickelten die beteiligten Stellen eine vertrauenswürdige virtuelle Maschine (VM), welche CEP Verfahren einsetzt, um sowohl historische Daten als auch in Echtzeit gesammelte Daten effizient und effektiv zu analysieren. Im Gegensatz zum Projekt iAID werden hier allerdings keine NetFlow-Daten untersucht, sondern Betriebsdaten von Anwendungen in virtuellen Maschinen.[49] Mit letztgenannter Technologie, der Virtual Machine Introspection (VMI), beschäftigte sich auch die Technische Universität München als Beitrag zum Projekt ANSII. Leider konnte kein Prototyp fertiggestellt werden.[50]

---

[43] Vgl. Pohlmann /Schlussbericht iAID Gelsenkirchen/ 3
[44] Vgl. Gad /Schlussbericht iAID Frankfurt/ 20
[45] Vgl. ebenda 23
[46] Pohlmann /Schlussbericht iAID Gelsenkirchen/ 11
[47] Ebenda 12
[48] Vgl zum Absatz Pohlmann /Schlussbericht iAID Gelsenkirchen/ 11-12
[49] Vgl. zum Absatz Mezini /Schlussbericht ACCEPT Darmstadt/ 4-5
[50] Vgl. zu den letzten beiden Sätzen Kinkelin et al. /Schlussbericht ANSII Garching/ 4-5

### 3.3.3 Content Anomaly Detection (CAD) über mehrere Server

Boggs et al. sammeln Daten von mehreren Servern, um den Blick von einer einzelnen Domäne auf mehrere Seiten zu erweitern. Zu diesem Zweck werden durch Content Anomaly Detection (CED) Sensoren die Daten der eingehenden GET Requests auf jedem Server gesammelt. Diese Daten werden normalisiert und decodiert, um einen einheitlichen Vergleich anstellen und die Daten auswerten zu können. Zur Auswertung werden sogenannte Bloom Filter[51] genutzt, welche die eingehenden Daten in $n$-Gramme teilen und analysieren. Werden auf Basis der vorher verarbeiteten Trainingsdaten Anomalien erkannt, werden diese Informationen über das Alarmaustauschsystem *Worminator*[52] an die anderen beteiligten Server verteilt, was eine schnellere und zuverlässigere Erkennung neuartiger Attacken auf globaler Ebene ermöglicht.[53]

### 3.3.4 Software Defined Networking (SDN)

Ein Ansatz, welcher vor allem für Heimnetzwerke oder kleinere Firmen gedacht ist, macht sich das Software Defined Networking (SDN) zunutze. SDN „ist ein Konzept zum Netzwerk-Aufbau. Dabei wird die Kontrolle von der Hardware entkoppelt und an […] den Controller […] übergeben.“[54] Dies ermöglicht es, Algorithmen zur Anomalieerkennung in den Controller zu implementieren, sodass die Verbindungsdaten durch diesen ausgewertet und entsprechend verarbeitet (geblockt oder weitergeleitet) werden können. In einem ersten Prototypen von Mehdi et al. wurden vier bereits bekannte Algorithmen[55] implementiert, wovon zwei selbstlernend agieren. Es wäre jedoch durch die Möglichkeit, den Controller softwareseitig zu steuern denkbar, jeden beliebigen Algorithmus zu implementieren.[56]

## 4 Vergleich der Verfahren zur Anomalieerkennung

Die Verfahren zur Erkennung von Anomalien sollen im Folgenden mithilfe einer Tabelle (Tab. 4-1) verglichen werden. Dabei werden die vorgestellten Ansätze weiter unterteilt in

---

[51] Vgl. Bloom /Hash Coding/
[52] Vgl. Locasto et al. /Collaborative Security/
[53] Vgl. zum Absatz Boggs et al. /Collaborative Anomaly Detection/
[54] Rouse /SDN/
[55] Vgl. Gu, McCallum, Towsley /Anomalies in Network Traffic/; Mahoney /Packet Bytes/; Schechter, Jung, Berger /Worm Infections/ und Williamson /Throttling Viruses/
[56] Vgl. zum Absatz Mehdi, Khalid, Khayam /Software Defined Networking/ 165

die dazu veröffentlichten Forschungen, sodass die Konzepte der Autoren im Vergleich berücksichtigt werden können.

Die **Systeme, auf welchen die beschriebenen Verfahren eingesetzt werden können**, lassen sich in drei Kategorien einteilen: einzelne Rechner und Geräte, ein lokales Netzwerk oder ein globales Netzwerk. Einige Ansätze führen die Anomalieerkennung innerhalb des lokalen Netzwerks durch, tauschen die Ergebnisse allerdings global aus, weshalb sie beiden Systemen zugeordnet werden.

**Erkennbare Cyber-Attacken** sind in der Tabelle folgendermaßen vertreten: *Malware* steht für jegliche Schadsoftware, welche auf einem Rechner oder Server installiert sein kann. Durch eine solche Schadsoftware lassen sich beispielsweise Daten abhören oder verändern. *Botnetze* sind Verbunde von Bot-Instanzen und lassen zu, dass das System durch fremden Einfluss gesteuert und für schädliche Zwecke verwendet werden kann. *DoS-Attacken* und *Maskierung* wurden bereits in Kapitel zwei beschrieben. Der Begriff *Spionage* steht hier für Entwendung von Daten durch einen Mitarbeiter. Es wäre allerdings denkbar, dass ein solcher Angriff auch durch Malware durchgeführt werden kann. In der folgenden Tabelle sind die Schwerpunkte der jeweiligen Verfahren gekennzeichnet.

Die unten stehende Tabelle soll außerdem die in der Einleitung genannte Frage nach der **Zuverlässigkeit der Anomalieerkennung** beantworten. Nicht alle Forschungen haben konkrete Forschungsergebnisse hierzu veröffentlicht, die bekannten Zahlen befinden sich jedoch in der Tabelle. TPR steht dabei für die *True Positive Rate*, also die korrekt erkannten Angriffe. FPR bedeutet *False Positive Rate* und gibt an, wie viele Anomalien fälschlicherweise gemeldet wurden, obwohl es sich dabei nicht um einen Angriff handelte.

| ANSATZ DER ANOMALIEERKENNUNG | PROJEKT/KONZEPT | SYSTEM | SCHWERPUNKTE | ZUVERLÄSSIGKEIT |
|---|---|---|---|---|
| **NETFLOW DATEN INNERHALB ISPS** | INSAIN/ISPs | globales Netzwerk | Botnetz, DoS | FPR: < 1,5%[57] |
| **TRUSTED COMPUTING** | ANSII/Bootvorgang | Rechner | Malware | keine Angaben |
| | HIVE/Virtualisierung | Rechner | Malware | keine Angaben |
| **INTER-AS ROUTING** | MonIKA/Inter-AS Routing | lokales/globales Netzwerk | Botnetz | 74% mehr gesicherte Informationen als in Datenbanken über Hosts[58] |
| **DATEIZUGRIFFE** | File Access | Rechner | Spionage | TPR: 80%<br>FPR: 2,5%[59] |
| | Search Behavior | Rechner | Spionage, Maskierung | TPR: 26,8% - 75.8%<br>FPR: 1,3% - 7,7%[60] |
| **ANALYSE VON LOG-DATEIEN** | CAIS/Logs | lokales Netzwerk | Malware, Botnetz, DoS | keine Angaben |
| | Graph Inference | lokales Netzwerk | Malware, Botnetz | TPR: 95,2%<br>FPR: 0,68%[61] |
| **COMPLEX EVENT PROCESSING** | iAID/IAS-Flow-Daten | lokales Netzwerk | Malware, Botnetz, DoS | keine Angaben |
| | ACCEPT/Virtualisierung | Rechner | Malware | keine Angaben |
| **CONTENT ANOMALY DETECTION** | Collaborative | lokales/globales Netzwerk | Malware, Botnetz, DoS | FPR: 0,03%[62] |
| **SOFTWARE DEFINED NETWORKING** | Software Defined Networking | lokales Netzwerk | Malware, Botnetz | TPR: 90%<br>FPR: 0% - 4%[63] |

Tab. 4-1: Vergleich der Verfahren

Grenzen von Intrusion Detection Systemen wurden bereits 2002 von Kemmerer und Vigna beschrieben und betreffen vor allem die Punkte Effektivität, Leistung und die Begrenzung auf die lokale Sicht.[64]

Ähnlich sieht es auch bei den **Grenzen der Anomalieerkennung** aus, wie García-Teodoro beschreibt.[65] Wie Tabelle 4-1 zu entnehmen, gibt es noch immer eine zum Teil hohe Rate an fälschlicherweise gemeldeten Angriffen (FPR), was zu einer unnötigen Belastung der verantwortlichen Personen führt, welche die Vorfälle untersuchen müssen. Dennoch stellen die Verfahren der Anomalieerkennung einen vielversprechenderen Ansatz gegenüber der Mustererkennung dar. Einige der oben beschriebenen Ansätze

[57] Vgl. Baier, Abt /Anomalieerkennung INSAIN/ 61
[58] Vgl. Wübbeling, Elsner, Meier /Routing Anomalies/ 234
[59] Vgl. beide Werte Gates et al. /File Access/ 398
[60] Vgl. beide Werte Salem, Stolfo /Search Behavior/ 185
[61] Vgl. beide Werte Manadhata et al. /Graph Inference/ 11
[62] Vgl. Boggs et al. /Collaborative Anomaly Detection/ 158
[63] Vgl. beide Werte Mehdi, Khalid, Khayam /Software Defined Networking/ 173
[64] Vgl. Kemmerer, Vigna /Intrusion Detection History/ 28-29
[65] Vgl García-Teodoro /Anomaly-based intrusion detection/ 26

kombinieren lokale und globale Analyse, sodass sich die Grenzen der untersuchten Systeme erweitern und ein großflächigeres Bild erfasst werden kann. Die Art der Implementierung spielt bei der Frage nach den Grenzen daher eine zentrale Rolle und richtet sich nach dem Zweck der Überwachung. Einige vorgestellte Verfahren wurden mit einem speziellen Ziel entwickelt, beispielsweise die Überwachung der Endgeräte im Projekt ANSII. Andere Ansätze, wie zum Beispiel die Logdatei-Analyse im Projekt CAIS, sind modularer gestaltet und erlauben eine Einbeziehung vielfältiger Ressourcen, sodass die Möglichkeiten der Überwachung nahezu unbegrenzt sind, solange entsprechende Log-Dateien vorliegen. Grundsätzlich lässt sich jedoch sagen, dass die Überwachung von Endgeräten eher dafür geeignet ist, Malware und Spionage aufzudecken. Die Analyse über ein lokales Netzwerk hingegen eignet sich bevorzugt zum Erkennen von Botnetzen und DoS-Attacken. Eine Erweiterung auf das globale Netz erhöht die Chance, Anomalien aufzudecken.

# 5 Schlussbemerkungen

**Zusammenfassung:** In den vorangegangenen Kapiteln wurden aktuelle Verfahren aus dem Bereich der Anomalieerkennung vorgestellt. Diese wurden für verschiedene Anwendungsgebiete entwickelt, von der Überwachung eines im Netzwerk betriebenen Endgerätes bis hin zur Analyse von Verbindungsdaten über ein globales Netzwerk hinweg. Die Verfahren bedienen sich bei der Aufdeckung von Anomalien oft bereits bekannter Algorithmen und implementieren diese auf eine neue Art und Weise. Die untersuchten Daten reichen dabei von Verbindungsdaten direkt am Router (SDN) über vorliegende Dateien (File Access, Logdateien) bis hin zu globalen Verbindungsdaten. Durch die Wahl dieser Daten und der Implementierung der Anomalieerkennung unterscheiden sich die Ansätze hinsichtlich ihrer Abdeckung und der Möglichkeit, verschiedene Arten der Anomalien zu erkennen. Die Forschungsergebnisse der vorgestellten Untersuchungen zeigen weiterhin, dass zum Teil sehr gute Ergebnisse hinsichtlich der Anomalieerkennung damit erzielt werden konnten, und dass an anderen Stellen weitere Forschungen nötig sind, um eine akzeptable Erkennungsrate und eine möglichst geringe False Positive Rate zu erreichen.

**Kritische Würdigung:** Aufgrund des begrenzten Rahmens konnte nur eine beschränkte Auswahl an Anomalieerkennungsverfahren vorgestellt werden. Auch der Umfang und

die Ausführlichkeit, mit welcher die Verfahren beschrieben werden konnten, waren durch den vorgegebenen Rahmen der Arbeit beschränkt. Daraus folgt, dass die Beschreibungen sehr abstrakt gehalten werden mussten. Eine detailliertere Zusammenfassung der Hintergründe der Forschungen und der Vorgehensweise hätten zum Verständnis und einer besseren Einordnung beigetragen. Der Abstraktionsgrad, welcher bei der Beschreibung nötig war, erschwerte außerdem den Vergleich der Verfahren im Laufe der Arbeit. Einige der Ansätze sind sehr granular gestaltet, sodass sie universeller eingesetzt werden können als Verfahren, welche für ein spezielles Einsatzgebiet entwickelt wurden. Auch die Literaturrecherche selbst war durch den vorgegebenen zeitlichen Rahmen nur oberflächlich möglich. Eine längere Einarbeitung in die verwendeten Algorithmen konnte nur bedingt erfolgen und führte dazu, dass in der Literatur bereits bekannte Verfahren lediglich indirekt zitiert bzw. auf deren Quellen hingewiesen werden konnte.

Bei der Einarbeitung ist weiterhin aufgefallen, dass viele Projekte zum Thema Anomalieerkennung durch das Ministerium für Bildung und Forschung finanziert wurden und die Trennung in diese einzelnen Projekte, durch die Vorgabe eines Schwerpunktes, durchaus berechtigt war. Dennoch konnte der Eindruck gewonnen werden, dass durch eine nähere Zusammenarbeit der beteiligten Partner unterschiedlicher Projekte durch den Austausch von Erfahrungen und Ergebnissen ein größerer Nutzen hätte entstehen können. Die Projekte, in welchen einige der vorgestellten Verfahren entwickelt wurden, wurden recht zeitgleich durchgeführt, was eine Zusammenarbeit erleichtert hätte.

**Ausblick:** Da die Gefahr von Cyber-Attacken durch die Verlagerung der Kommunikation ins Internet oder in Netzwerke immer größer wird und die Professionalisierung der Angreifer immer weiter steigt, ist ein funktionierendes System zur Erkennung einer Attacke wichtiger denn je und seine Bedeutung im Kampf um Datensicherheit und Schutz vor feindlicher Übernahme wird weiterhin zunehmen. Daraus folgt, dass das Interesse an effektiveren Algorithmen zur Anomalieerkennung und flächendeckenden Implementierungen unverändert hoch sein wird. Neue Erkenntnisse im Bereich künstlicher Intelligenz und maschinellen Lernens können den Entwicklungen auf dem Gebiet der Anomalieerkennung neuen Anstoß geben und dazu beitragen, Rechner und Netzwerke effektiver zu schützen. Das Hauptziel dabei wird sein, die Erkennungsrate auf möglichst vielen Gebieten zu steigern und die False Positive Rate auf ein Minimum zu reduzieren.

# 6 Literaturverzeichnis

Fiedler et al. /Anomalieerkennung CAIS/

Roman Fiedler, Florian Skopik, Thomas Mandl, Kurt Einzinger: Erkennen von Anomalien und Angriffsmustern. In: Cyber Attack Information System. Springer-Verlag, Berlin, Heidelberg 2015, S. 89-118.

Baier, Abt /Anomalieerkennung INSAIN/

Harald Baier, Sebastian Abt: Abschlussbericht zum FHprofUnt Verbundprojekt Institutional Network and Service Provider Anomaly Inspection (INSAIN): Ergebnisse des Verbundpartners Hochschule Darmstadt. Darmstadt 2015.

Gu, McCallum, Towsley /Anomalies in Network Traffic/

Yu Gu, Andrew McCallum, Don Towsley: Detecting anomalies in network traffic using maximum entropy estimation. In: Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement. Berkley 2005, S. 32.

García-Teodoro /Anomaly-based intrusion detection/

Pedro García-Teodoro et al.: Anomaly-based network intrusion detection: Techniques, systems and challanges. In: Computers & Science. Nr. 28, 2009, S. 18-28.

PwC /Anzahl Cyberangriffe/

PwC, Anzahl der jährlichen Cyberangriffe weltweit in den Jahren 2009 bis 2014 (in Millionen). https://de.statista.com/statistik/daten/studie/348766/umfrage/jaehrliche-anzahl-von-internetangriffen-weltweit/ o.O. o.J., Abruf: 2016-11-16.

Yedidia, Freeman, Weiss /Belief Propagation/

Jonathan S. Yedidia, William T. Freeman, Yair Weiss: Understanding Belief Propagation and its Generalizations. In: Gerhard Lakemeyer, Bernhard Nebel: Exploring Artificial Intelligence in the New Millennium. Morgan Kaufmann Publishers Inc., San Francisco 2003, S. 239-269.

Qiu et al. /Bogus Route Information/

Jian Qiu et al.: Detecting bogus BGP route information: Going beyond prefix hijacking. In: Third International Conference on Security and Privacy in Communication Networks and the Workshops. 2007, S. 281-390.

Boggs et al. /Collaborative Anomaly Detection/

Nathaniel Boggs et al.: Cross-Domain Collaborative Anomaly Detection: So Far Yet So Close. In: Robin Sommer, Davide Balzarotti, Gregor Maier (Hrsg.): Recent Advances in Intrusion Detection. Springer-Verlag, Berlin, Heidelberg 2011, S. 142-160.

Locasto et al. /Collaborative Security/

Michael E. Locasto et al.: Towards Collaborative Security and P2P Intrusion Detection. In: Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop. 2005, S. 333-339.

Gao, Reiter, Song /Distance Measurement/

Debin Gao, Michael K. Reiter, Dawn Sing: Behavioral Distance Measurement Using Hidden Markov Models. In: Diego Zamboni, Christopher Kruegel (Hrsg.): Recent Advances in Intrusion Detection. Springer-Verlag, Berlin, Heidelberg 2006, S. 19-40.

Leopold et al. /Einleitung CAIS/

Helmut Leopold et al.: Einleitung zum Cyber Attack Information System. In: Cyber Attack Information System. Springer-Verlag, Berlin, Heidelberg 2015, S. 1 - 12.

Gates et al. /File Access/

Christopher Gates et al.: Detecting Insider Information Theft Using Features from File Access Logs. In: Miroslaw Kutylowski, Jaideep Vaidya (Hrsg.): Computer Security – ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part I. Springer-Verlag, Cham, Heidelberg, New York, Dordrecht, London 2014, S. 383-400.

Manadhata et al. /Graph Inference/

Pratyusa K. Manadhata et al.: Detecting Malicious Domains via Graph Inference. In: Miroslaw Kutylowski, Jaideep Vaidya (Hrsg.): Computer Security – ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part I. Springer-Verlag, Cham, Heidelberg, New York, Dordrecht, London 2014, S. 1-18.

Bloom /Hash Coding/

Burton H. Bloom: Space/Time Trade-offs in Hash Coding with Allowable Errors. In: Communications of the ACM. Nr. 13(7). ACM, New York 1970, S. 422-426.

Milliken /Intrusion Detection/

Jonny Milliken: Introduction to Wireless Intrusion Detection Systems. In: Al-Sakib K. Pathan: The State of the Art in Intrusion Prevention and Detection. Taylor & Francis Group. Boca Raton 2014, S. 335-360.

Kemmerer, Vigna /Intrusion Detection History/

Jonny Milliken: Introduction Detection: A Brief History and Overview. In Computer. Nr. 25. 2002, S. 27-30.

Zhao et al. /Invalid Routing Announcement/

Xiaoliang Zhao et al.: Detection of Invalid Routing Announcement in the Internet. In: Proceedings of the 2002 International Conference on Dependable Systems and Networks. 2002, S. 59-68.

Eckert /IT-Sicherheit/

Claudia Eckert: IT-Sicherheit, Konzepte – Verfahren – Protokolle. 8. Auflage, Oldenburg Verlag, München 2013.

BSI /Lagebericht 2016/

Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT Sicherheit in Deutschland 2016. Frankfurt am Main 2016.

Gold /Malware Samples/

Steve Gold: 160,000 new malware samples arriving every day. http://www.scmagazineuk.com/160000-new-malware-samples-arriving-every-day/article/349235/ o.O. 2014, Abruf: 2016-12-03

Avira /Maximale Sicherheit/

Avira: Maximale Sicherheit: Avira AntiVir Version 10. http://www.avira.com/de/press-details/nid/456/news/maximized+security+avira+av+10 o.O. 2010, Abruf: 2016-12-02

de Godoy Stênico, Ling /Network Traffic Monitoring/

Jeferson W. de Godoy Stênico, Lee L. Ling: Network Traffic Monitoring and Analysis. In: Al-Sakib K. Pathan: The State of the Art in Intrusion Prevention and Detection. Taylor & Francis Group. Boca Raton 2014, S. 23-46.

Mahoney /Packet Bytes/

Matthew V. Mahoney: Network Traffic Anomaly Detection Based on Packet Bytes. In: Proceedings of the 2003 AMC Symposium on Applied Computing. Springer-Verlag. New York 2003, S. 346-350.

Lad et al. /PHAS/

Mohid Lad et al.: PHAS: a prefix hijack alert system. In: Proceedings of the 15th conference on USENIX Security Symposium. Nr. 15, 2006, S. 18-28.

Wübbeling, Elsner, Meier /Routing Anomalies/

Matthias Wübbeling, Till Elsner, Michael Meier: Inter-AS Routing Anomalies: Improved Detection and Classification. In: Pascal Brangetto, Markus Maybaum, Jan Stinissen: Proceedings of 6th International Conference on Cyber Conflict. Tallinn 2014, S. 223-238.

Treinen, Thurimella /Rule Mining/

James J. Treinen, Ramakrishna Thurimella: A Framework for the Application of Association Rule Mining in Large Intrusion Detection Infrastructures. In: Diego Zamboni, Christopher Kruegel (Hrsg.): Recent Advances in Intrusion Detection. Springer-Verlag, Berlin, Heidelberg 2006, S. 1-18.

Mezini /Schlussbericht ACCEPT Darmstadt/

Mira Mezini: ACCEPT Anomaliemanagement in Computersystemen durch Complex Event Processing Technologie (Anomaly Management in computer systems through complex event processing technology). Darmstadt 2015.

Kinkelin et al. /Schlussbericht ANSII Garching/

Holger Kinkelin et al.: Schlussbericht zum ANSII-Teilvorhaben „Hybride Mechanismen zur Erkennung und Verhinderung von Angriffen auf vernetzte Systeme durch Netzwerk-Monitoring und Integritätsüberwachung“. Garching bei München 2014.

Dreher, Kehrer /Schlussbericht ANSII Neckartenzlingen/

Andreas Dreher, Stephan Kehrer: Schlussbericht zum Teilvorhaben „Spezifizierung und Implementierung eines Anomaliedetektors für industrielle Netzwerkgeräte auf Geräteebene und in der Netzwerktopologie“. Neckartenzlingen 2014.

Wagner, Wessel /Schlussbericht HIVE Garching/

Steffen Wagner, Sascha Wessel: Schlussbericht Fraunhofer-Institut AISEC, Projekt HIVE „Hypervisor-basierte innovative Verfahren zur Anomalieerkennung mit Hardwareunterstützung“. Garching bei München 2014.

Gad /Schlussbericht iAID Frankfurt/

Rüdiger Gad: Schlussbericht ‚innovative Anomaly- and Intrusion-Detection (iAID)‘ Teilvorhaben: ‚Anomaly Detection and Response System (AdaRS)‘. Frankfurt am Main 2015.

Pohlmann /Schlussbericht iAID Gelsenkirchen/

Norbert Pohlmann: Schlussbericht ‚innovative Anomaly- and Intrusion-Detection (iAID)‘ Teilvorhaben: ‚Flowdatenanomalieerkennung und benutzerunterstützte, intelligente Alarm-Filterung‘. Gelsenkirchen 2015.

Rouse /SDN/

Margaret Rouse: Software-defined Networking (SDN), Definition. http://www.searchnetworking.de/definition/Software-defined-Networking-SDN o.O. o.J., Abruf: 2016-12-07

Meier /Schlussbericht MonIKA Wachtberg/

Michael Meier: Abschlussbericht für das Teilvorhaben „Erkennung von Anomalien“ (EvA) im Verbundprojekt „Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung“ (MonIKA). Wachtberg 2014.

Bless et al. /Sichere Netzwerkkommunikation/

Roland Bless et al.: Sichere Netzwerkkommunikation. Springer-Verlag, Berlin, Heidelberg 2005.

Mehdi, Khalid, Khayam /Software Defined Networking/

Syed A. Mehdi, Junaid Khalid, Syed A. Khayam: Revisiting Traffic Anomaly Detection Using Software Defined Networking. In: Robin Sommer, Davide Balzarotti, Gregor Maier (Hrsg.): Recent Advances in Intrusion Detection. Springer-Verlag, Berlin, Heidelberg 2011, S. 161-180.

Salem, Stolfo /Search Behavior/

Malek B. Salem, Slavatore J. Stolfo: Modeling User Search Behavior for Masquerade Detection. In: Robin Sommer, Davide Balzarotti, Gregor Maier (Hrsg.): Recent Advances in Intrusion Detection. Springer-Verlag, Berlin, Heidelberg 2011, S. 181-200.

Williamson /Throttling Viruses/

M M. Williamson: Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code. In: 18th Annual Computer Security Applications Conference, 2002, Proceedings. o.O. 2002, S. 61-68.

Schechter, Jung, Berger /Worm Infections/

Stuart E. Schechter, Jaeyeon Jung, Arthur W. Berger: Fast Detection of Scanning Worm Infections. In: Erland Jonsson, Alfonso Valdes, Magnus Almgren: Recent Advances in Intrusion Detection. Springer-Verlag, Heidelberg 2004, S. 59-81.