Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Robin Bergmann

Visualisierung von Threat Intelligence Informationen
für Cyber Defence Centre

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Robin Bergmann

Visualisierung von Threat Intelligence Informationen für Cyber Defence Centre

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Angewandte Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Klaus-Peter Kossakowski
Zweitgutachter: Prof. Dr.-Ing. Martin Hübner

Abgegeben am 14.07.2015

Robin Bergmann

Thema der Bachelorarbeit

Visualisierung von Threat Intelligence Informationen für Cyber Defence Centre

Stichworte

Threat Intelligence, Visualisierung, Cyber Defence Centre, CERT, SOC, IDS, Honeypot, Botnet

Kurzzusammenfassung

Für den reibungslosen Ablauf in einem Cyber Defense Centre benötigen diese genaue Informationen über den aktuellen Zustand der zu schützenden Systeme. Diese Informationen müssen aus unterschiedlichen Quellen zusammengeführt und dann verarbeitet bzw. analysiert werden. Einerseits können die gesammelten Daten im Vorfeld zusammengefasst werden, um Zusammenhänge, wie z.B. zwischen Serverlast und Zugriffszahlen, herzustellen. Andererseits ist es notwendig, die Ergebnisse an den Menschen, als entscheidende Instanz, weiter zu geben. Es gilt einen Engpass und eine damit verbundene verzögerte Verarbeitungszeit, zu vermeiden. Dazu ist es bei der Informationsweitergabe zwischen Maschine und Mensch notwendig, die Informationen so aufzubereiten, dass der Mensch diese optimal verarbeiten kann.

Der Mensch hat eine beachtliche Fähigkeit, Zusammenhänge und große Datenmengen visuell zu verarbeiten. Diese Fähigkeit des Menschen gilt es zu nutzen, um einen möglichst reibungslosen Ablauf und die gewünschte optimale Verarbeitung zu gewährleisten.

In dieser Arbeit werden Möglichkeiten und Optimierungen zur Informationsdarstellung von bereits vorverarbeiteten Threat Intelligence Informationen untersucht.

Robin Bergmann

Title of the paper

Visualization of Threat Intelligence Information for Cyber Defence Centre

Keywords

Threat Intelligence, visualization, Cyber Defence Centre, CERT, SOC, IDS, Honeypot, Botnet

Abstract

For the correct running of a Cyber Defense Centre it need exact information about the current state of the systems to be protected by this Cyber Defense Centre. This information must be merged from different sources and then processed and analyzed. On the one hand, the collected data can be summarized in advance in order relationships such as between server load and drive traffic. On the other hand, it is necessary to give the results to the employee of the Cyber Defense Centre, as a final authority to react. It is the goal to avoid this bottleneck and a related deferred processing time. For the disclosure between machine and man it's necessary to reformat the information so that humans can process them optimally.

People have a remarkable ability to process and connect amounts of data visually. You can use this ability of people to ensure a smooth process and the desired optimum processing.

This paper study's options and optimizations for representing information from already preprocessed Threat Intelligence examines information.

Inhaltsverzeichnis

1 Einleitung

1.1 Ziel und Motivation

Das Ziel dieser Arbeit ist es, Wege aufzuzeigen, um den Informationsfluss in einem Cyber Defence Centre zu optimieren und damit eine verkürzte Reaktionszeit auf aktuelle Gefahren und neue Trends oder Entwicklungen bei bekannten Gefahren zu ermöglichen.

Um einen optimalen Ablauf in einem Cyber Defence Centre zu gewährleisten, benötigen die zuständigen Menschen genaue und aktuelle Daten über die zu schützenden Systeme und über die Gefahren, die diese betreffen. Diese Daten werden aus unterschiedlichen Quellen gesammelt, zusammengeführt und weiterverarbeitet. Auf dieser Grundlage können die gesammelten Daten zusammengefasst als Information an den Menschen weiter gegeben werden. An dieser Stelle kann ein Engpass entstehen und eine damit verbundene höhere Verarbeitungszeit. Um dies zu vermeiden, ist es bei der Informationsweitergabe zwischen Maschine und Mensch notwendig, die Informationen so aufzubereiten, dass der Mensch diese optimal verarbeiten kann.

Hier setzt die vorliegende Arbeit an. Ich versuche Möglichkeiten aufzuzeigen, mit deren Hilfe die benötigte Zeit zur Informationsweitergabe verkürzt werden kann. Das hat sowohl wirtschaftliche Aspekte als auch Vorteile für die Kunden der Cyber Defence Centre. Ein wirtschaftlicher Vorteil ist, dass weniger Manpower und damit verbunden weniger Kosten zur Analyse der Informationen gebraucht werden. Kunden profitieren von verkürzten und häufiger erkannten Vorfällen, die Ausfälle minimieren und die Wahrscheinlichkeit des Auftretens von Schäden verringern.

Es gilt also die Fähigkeit des Menschen, auch komplexe Zusammenhänge und große Datenmengen visuell in grafisch aufgearbeiteter Form schnell zu verarbeiten, zu nutzen. Dies geschieht mit Hilfe einer visuellen Darstellung wesentlich effizienter als bei gleicher Datenmenge, die nur textuell vorliegt.

1.2 Zielgruppe

Diese Arbeit wendet sich an zwei Zielgruppen: Einerseits sind es die bereits im Titel genannten Cyber Defence Centre, andererseits auch die Softwarefirmen, welche Threat Intelligence Tools entwickeln.

Cyber Defence Centre wird der Ansatz zur Optimierung der Arbeitsabläufe von Nutzen sein können. Hier wird vorwiegend auf die Optimierung der Erfassung von Informationen durch Menschen abgezielt.

Entwickler von Threat Intelligence Tools können durch die Weiterentwicklung der GUI ihrer Produkte höhere Marktakzeptanz und damit verbunden höhere Absatzzahlen erzielen.

Für die IT-Sicherheit im Allgemeinen wird diese Arbeit Wege zu verbesserten Reaktionszeiten und damit zu mehr Sicherheit aufzeigen. Durch verkürzte Reaktionszeiten und einen optimierten Informationsfluss können Gefahren schneller erkannt und abgewendet werden. Dies führt zu mehr Stabilität, Sicherheit und geringeren Beeinträchtigungen bei Angriffen.

1.3 Abgrenzung

Threat Intelligence Tools sammeln Daten aus verschiedenen Quellen und versuchen Rückschlüsse auf zukünftige Bedrohungen zu ziehen. In der vorliegenden Arbeit werden darüber hinaus Lösungen betrachtet, die momentan von Cyber Defence Centre genutzt werden. Es ist nicht Ziel dieser Arbeit, die Verarbeitungsschritte oder Vorgehensweisen dieser Tools zu optimieren.

In dieser Arbeit werden einige etablierte Visualisierungen vorgestellt, die sich für die Verarbeitung von Daten und Informationen durch Menschen insgesamt als nützlich erwiesen haben. Allerdings werden keine neuen Visualisierungstechniken entwickelt, vielmehr werden die vorgestellten Techniken als Werkzeuge genutzt.

Es werden in der vorliegenden Arbeit also Möglichkeiten und Optimierungen zur besseren Informationsdarstellung von bereits verarbeiteten Daten und dadurch vorliegenden Threat Intelligence Informationen untersucht und aufgezeigt.

1.4 Gliederung der weiteren Darstellung

In Kapitel 2 werden die für diese Arbeit notwendigen Visualisierungstechniken vorgestellt. Zuerst werden Grundlagen geschaffen, die allgemeine Anforderungen an Visualisierungstechniken beschreiben. Mit Hilfe der Visualisierung können dann, in Kapitel 4, die aus den Daten gewonnen Informationen anschaulich gemacht werden.

In Kapitel 3 wird die Vorgehensweise von Threat Intelligence erläutert. Es werden verschiedene Datenquellen vorgestellt und analysiert. Auf diese Analyse wird später in Kapitel 4 zurückgegriffen werden, in der die Datenkombination erfolgen soll. Da sich diese Arbeit mit der Verarbeitung von Threat Intelligence durch Cyber Defence Centre beschäftigt, wird der Begriff zunächst eingeengt und erklärt. Danach werden die einzelnen Bereiche des CDC und deren Anforderungen an Threat Intelligence abgeleitet.

Die Analyse und das Vorgehen der praktischen Untersuchung werden im 4ten Kapitel beschrieben. Zunächst werden die zuvor gewonnenen Erkenntnisse zusammengeführt und daraus ein Modell für Threat Intelligence für Cyber Defence Centre entwickelt um Schwerpunkte für die Visualisierung der Informationen zu verdeutlichen. Diese Visualisierungen werden anschließend mit den mit der Auswertung von Threat Intelligence befassten Personen in einem Sicherheitsunternehmen getestet.

In Kapitel 5, dem Fazit und Ausblick, werden die Ergebnisse dieser Arbeit zusammengefasst. Danach findet eine Bewertung der Ergebnisse statt und es werden Wege aufgezeigt, wie dieses Thema weiter untersucht oder bearbeitet werden kann.

1.5 Definitionen

1.5.1 Angriff

Ein Angriff stellt den Versuch, die Sicherheit eines Systems zu unterminieren dar. Genauer definiert, die Sicherheit eines Systems, die von einer intelligenten Bedrohung, d.h. einer bewussten Handlung, um Schutzmaßnahmen zu umgehen. Angriff kann aktiv oder passiv sein, durch Insider, Outsider oder über Vermittler.

In Organisationen wird auch eine bewusste Handlung zur Gefährdung der Netzwerksicherheit durch das Eindringen von Schadprogrammen als Angriff gewertet.

Darüber hinaus wird der Versuch der Überwindung von Verschlüsselungstechniken durch Kryptographie zu den Angriffen gezählt.

Zu den Zielen von Angriffen gehören: den eigenen Einflussbereich aktiv auszudehnen, der Diebstahl von Forschungsergebnissen oder Sabotage eines Systems zur Erschaffung eigener Vorteile.

1.5.2 Cyber Defence Centre (CDC)

Es gibt keine eindeutige oder gemeingültige Definition zu Cyber Defence Centre, da sich dieser Begriff in einem stetigen Wandel befindet. In dieser Arbeit wird er als Sammelbegriff für alle Instanzen zur Bekämpfung von Cyber Crime und zur Reaktion auf Vorfälle bzw. Angriffe genutzt. Darunter fallen sowohl CERTs (Computer/Cyber Emergency Response Teams) als auch SOCs (Security Operating Centre) und noch viele weitere wie Lagezentren oder ISACs (Information Sharing and Analysis Centre). Um den jeweiligen Nutzen für diese Untergruppen heraus zu stellen, ist es wichtig, die Arbeitsweise und Ziele der jeweiligen Instanz zu verstehen.

1.5.3 Computer Emergency Response Team (CERT)

CERTs sind in einer Art Baumstruktur organisiert. An deren Wurzel steht FIRST, der Dachverband aller CERTS weltweit. In zweiter Instanz folgt für Europa die TF-CSIRT, die den Dienst Trusted-Introducer zur Unterstützung von Sicherheitsteams und CERTs aufgebaut hat. Außerdem gibt es in vielen Ländern nationale Zusammenschlüsse wie z.B. den CERT-Verbund in Deutschland.

In einem CERT werden Vorfälle aufgenommen, analysiert und Lösungsstrategien entwickelt. Diese Arbeiten finden zum Teil unabhängig von einzelnen Angriffen statt, sondern beruht auf Daten über einer Vielzahl von Angriffen. Dies soll es ermöglichen, gemeingültige Lösungen zu entwickeln, welche dann an Betroffene weitergegeben werden können.

Ein anderer Teil der Arbeit eines CERTs, der in dieser Arbeit mehr zum Tragen kommt, ist die Reaktion auf Incidents. Auf diesen Aspekt wird in 3.7.1 näher eingegangen.

1.5.4 Security Operation Centre (SOC)

Die Aufgabe eines Security Operation Centre besteht darin, Angriffe und Vorfälle möglichst schnell zu erkennen und zu entdecken. Hier werden die vom CERT entwickelten Verteidigungsstrategien angewendet und auf den jeweiligen Fall angepasst. Außerdem werden alle Datenquellen zu Sicherheitsereignissen ausgewertet und untersucht, ob diese auf einen Angriff oder einen Vorfall hinweisen.

Ein SOC ist oft firmenintern oder wird als externer Dienstleister unter Vertrag genommen. Dies ist das erste Glied der Kette, wenn es um die Bekämpfung von Angriffen geht. Hier können Daten von realen Angriffen gesammelt und die Wirkung der Verteidigungsmaßnahmen unter Beweis gestellt werden, die im CERT entwickelt wurden.

1.5.5 Threat Intelligence (TI)

Unter Threat Intelligence wird im Allgemeinen die Informationsanalyse und Kombination zur Bekämpfung von Angriffen verstanden.

Zu den Zielen von TI zählt sowohl das Priorisieren von Alarmen und die Vorbeugung von Angriffen als auch die quantitative Reduzierung des Auftretens grundsätzlicher Probleme. Im Optimalfall soll TI Gefahren erkennen, bevor diese akut werden. Ist eine Gefahr erkannt worden, so wird diese an die zuständigen Menschen gemeldet.

Der Grundsatz von TI ist „Know your enemy“. Das soll heißen, dass TI weiter gehen soll als auf Alarme zu reagieren. Der Angreifer soll soweit nachvollzogen werden, dass eine Vorhersage des Verhaltens des Angreifers möglich wird.

1.5.6 Intrusion Detection System (IDS)

Ein Intrusion Detection System ist ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind. Das IDS kann ein Netzwerk als Firewall-Ergänzung schützen oder auch direkt auf dem zu überwachenden Computersystem laufen und so die Sicherheit von Netzwerken erhöhen. Neuere Systeme kombinieren die Stärken beider alten Komponenten.

In dieser Arbeit wird der Begriff „Intrusion Detection System“ nur als Abgrenzung zu TI erwähnt.

1.5.7 Honeypot

Ähnlich wie IDS-Systeme werden Honypots eingesetzt, um Daten über Angreifer zu erheben oder neue Angriffe zu erkennen.

Honypots sind jedoch Systeme, die bewusst mit Schwachstellen versehen werden, um Angreifern einen leichten Einbruch in das System zu ermöglichen. Diese Systeme sind nicht Teil der produktiven Umgebung und bieten damit die Möglichkeit, durch entsprechendes Monitoring einen Angriff zu registrieren und ggf. nachzuvollziehen, ohne die Produktion zu gefährden.

Es gibt zwei Kategorien von Honeypots: Low-Interaction Honeypots sind aufgrund ihrer primitiven Beschaffenheit nicht zur erfolgreichen Kompromittierung geschaffen. Sie sind einfach gehalten und vorrangig für die Intrusion Detection von Nutzen. Bei dieser Art der Honypots werden lediglich geringe Datenmengen erhoben. Der Angreifer merkt meist recht schnell, dass dieses System kein lohnenswertes Ziel für die Bemühungen des Angreifers ist. So kann meist nur ein Teil der Malware und die IP-Adresse des Angreifers erfasst werden.

High-Interaction Honeypots sind zur Vorgehensanalyse von Angreifern bestimmt. Allerdings scheitern daran auch gängige High-Interaction Honeypots, da der Angreifer die vermeintlich verwundbaren Services und Systeme schnell als Falle erkennt und den Angriff abbricht. Moderne High-Interaction Honeypots hingegen lassen den Angreifer in dem Glauben, erfolgreich eingebrochen zu sein. Ab diesem Zeitpunkt kann die verteidigende Organisation gefahrlos zusehen, wie sich der Angreifer in einer kontrollierten und isolierten Umgebung ausbreitet, oder auf welche Systeme oder Daten der Angreifer es tatsächlich abgesehen hat. Dadurch gewinnen sie einzigartige, für die Organisation relevante Daten zur Erweiterung der Threat Intelligence.

1.5.8 Botnetz

Ein Botnetz oder auch Botnet ist eine Menge von Rechnern, die durch automatisierte Computerprogramme, vernetzt sind. Die Bots (von englisch: robot „Roboter“) laufen auf vernetzten Rechnern, die sich ihre lokale Ressourcen und Daten gegenseitig zur Verfügung stellen. In Deutschland wurden 2010 über 470.000 solcher Bots identifiziert. Von ihnen waren im Durchschnitt etwa 2.000 pro Tag aktiv. Betreiber illegaler Botnetze installieren die Bots ohne das Wissen der Inhaber auf deren Computern und nutzen sie für ihre eigenen Zwecke. Die meisten Bots können von einem Botnetz-Operator (auch Bot-Master oder Bot-Herder genannt) über das Internet überwacht und befehligt werden. Dieser wird als Command-and-Control-Server(C&C) bezeichnet [1].

Botnetze werden meist von Angreifern eingesetzt, um Angriffe durchzuführen. Die wohl bekannteste Angriffsmethode ist der sogenannte Distributed Denial of Service (DDoS). Wenn Bots in zu schützenden Organisationen oder CDCs entdeckt werden, bietet sich eine gute Gelegenheit, um mehr Daten über den Bot-Master und damit über den Angreifer zu erheben, also die Threat Intelligence zu erweitern.

1.5.9 Incident

Ein Incident ist ein plötzlich auftretendes Ereignis. Incidents sind meist negativ, haben aber keine große Schadenswirkung. Ist die Schadenswirkung doch höher als zunächst angenommen, wird der Incident zu einem Security-Incident eskaliert.

Ein Incident kann ein Verfügbarkeitsproblem in einem Netzwerk, eine fehlerhafte Zonenübertragung oder ein einzelnes von Viren befallenes System sein. Für diese alltäglichen Incidents sind gewöhnlich Workflows etabliert. Die ausführenden Instanzen dieser Workflows sind ein Teil der Stammorganisation, d.h. Helpdesk oder SOCs. Sie werden geschult, um Zwischenfälle im Arbeitsalltag zu behandeln.

Da nur Incidents in den Aufgabenbereich von SOCs fallen, werden die Security-Incidents an ein CERT zur weiteren Bearbeitung weiter geleitet.

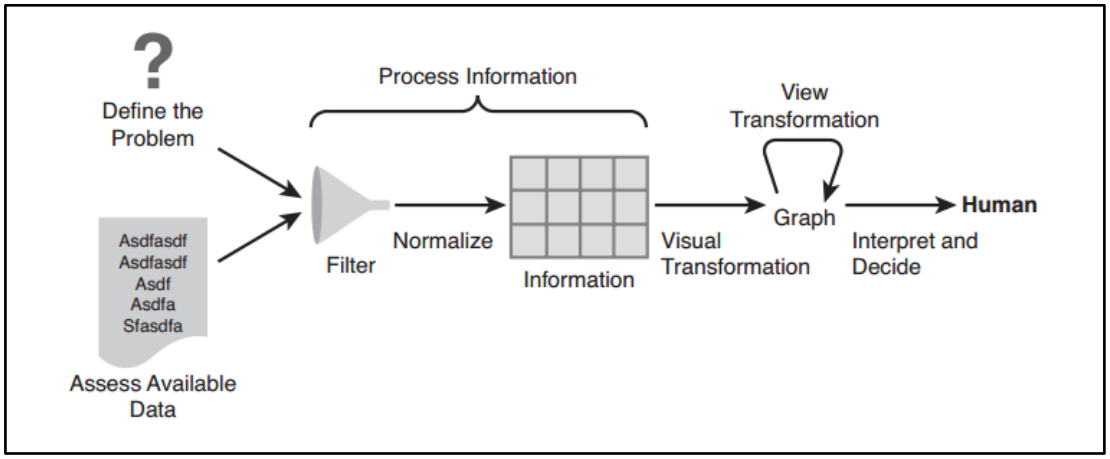
1.5.10 Daten & Informationen

In dieser Arbeit wird zwischen dem Begriff „Daten“ und dem Begriff „Informationen“ unterschieden. Daten sind Werte, die gesammelt bzw. erhoben werden und in keinerlei Zusammenhang stehen. Daten für die Threat Intelligence werden aus verschiedenen Quellen gesammelt, wie z.B. die weiter oben bereits aufgeführten Botnetze und Honypots. Informationen hingegen sind kombinierte Daten, aus denen sich Schlussfolgerungen ziehen lassen.

Um Informationen zu gewinnen, müssen Daten, die auch aus unterschiedlichen Quellen stammen können, in Zusammenhang gebracht werden. In Bezug auf die Threat Intelligence werden beispielsweise Daten über Schwachstellen, den Nutzen von Servern und die Daten über konkrete Angriffe ausgewertet und zu einer Information zusammengestellt.

2 Visualisierung

Im Kontext der Threat Intelligence sind die gesammelten, angereicherten und weiterverarbeiteten Informationen vorrangig zur Unterstützung der Analysten eines CDCs bestimmt. Wenn allerdings eine ausreichende Qualität der Meldungen gegeben ist, dann müssen die Informationen weiteren Nutzergruppen zur Verfügung gestellt werden, um so entsprechende Prozesse zu starten oder Entscheidungen zu ermöglichen. Dies sind zunächst die Mitarbeiter in Lagezentren oder CERTs, aber auch Techniker und Entscheidungsträger in Unternehmen und Behörden. Es müssen also Personengruppen berücksichtigt werden, die sich durch Funktion, Tätigkeit oder aufgrund der Tiefe des technischen Fachwissens voneinander unterscheiden. Damit ist die Notwendigkeit gegeben, Informationen allgemein verständlich aufzubereiten. Dazu müssen die Informationen in einer Form vorgehalten werden, so dass diese effizient durch Programme dargestellt werden können [2].



[Abbildung 1: Allgemeines Vorgehen zur Visualisierung [3]]

Statt sich auf einzelne Produkte zur Informationsvisualisierung zu konzentrieren, befasst sich diese Arbeit nur mit Visualisierungstechniken, wie sie in beliebige Systeme eingebaut werden könnten. Schwerpunkt sind Techniken, die eine Zusammenfassung der Daten, die durch das Threat Intelligence System visualisiert werden sollen, ermöglichen.

2.1 Funktionsweise von Visualisierung

Beim Versuch, die Fähigkeiten des menschlichen Gehirns zur visuellen Informationsverarbeitung zu nutzen, ist es erforderlich, vorher die grundlegenden Prinzipien der menschlichen Wahrnehmung zu verstehen.

Die Wahrnehmung kann uns nützliche Richtlinien für die Erstellung effektiver Visualisierungstechniken von Informationen liefern. Die folgenden Abschnitte geben eine Einführung in diese Grundsätze.

2.2 Grundlagen der Wahrnehmung

Als sogenannten „Ikonischen Speicher“ werden Mechanismen im Gehirn bezeichnet, die visuellen Input, ohne bewusste Anstrengung, für sehr kurze Zeiträume speichern. Dies gilt für einen Zeitraum zwischen 200 und 400 Millisekunden. Der ikonische Speicher ist auch als sensorischer Speicher bekannt. Er ist mit einem Prozess verbunden, der die erste Analyse des visuellen Inputs beschreibt, die das Gehirn vor der bewussten Verarbeitung vornimmt [4].

Es gibt Attribute, die während der visuellen Eingabe, ohne dass irgendeine bewusste Anstrengung erfolgt, als erste identifiziert werden. Zu den verarbeiteten Attributen zählen grundlegende Eigenschaften wie Farbe, Größe und Orientierung.

Die Nutzung der Kraft der ikonischen Speicher durch Visualisierungen erlaubt es, die kognitive Belastung für Menschen bei der Verarbeitung der Informationen erheblich zu reduzieren und zu helfen, effektiv zu kommunizieren. Es gilt Informationen in einer Weise darzustellen, so dass sie für den Betrachter „heraus springen“ und relevante Informationen schon bei kurzfristiger Betrachtung der Visualisierung wahrgenommen und verarbeitet werden können [5].

Die ersten drei Darstellungen in Abbildung 2 sind Beispiele für diese Darstellungsform. Sie zeigen, wie es möglich ist, das Auge des Betrachters einzufangen, ohne dass dieses sich bewusst anstrengen muss. Der gleiche Verlauf in der Abbildung 2 ist ein Gegenbeispiel für ein Attribut, welches nicht im ikonischen Speicher verarbeitet wird: die Parallelität der Linien.

2.3 Grundlagen der Gestaltung

Die Gestaltpsychologie beschreibt die psychologische Wahrnehmung von Einzelteilen, die aufgrund von Eigenschaften zu Strukturen und Ordnungen zusammengeschlossen werden.

Um diese Wahrnehmung nutzen zu können, verwendet diese Arbeit Konzepte der Gestalt-Theorie. Diese befasst sich mit dem Zusammenhang zwischen der Anordnung von Elementen und der psychologischen Wahrnehmung. Ziel ist es, die Wahrnehmung durch die Gestaltung der gelieferten Ergebnisse zu erleichtern.

Um diese Wahrnehmung zu erklären, wurde sie in verschiedene Ordnungssysteme aufgeteilt. Hieraus leiten sich einige Gesetzmäßigkeiten ab [6]:

a. Gesetz von Figur und Grund

Eine Ansammlung von Elementen teilt sich in eine klare Vordergrundfigur und einen diffusen Hintergrund auf. Beide Gruppen können zwar wahrgenommen werden, allerdings nicht gleichzeitig.

b. Gesetz der Gleichheit

Elemente der gleichen Farbe und Form werden zu Gruppen zusammengefasst und zusammen wahrgenommen.

c. Gesetz der Nähe

Elemente in räumlicher Nähe werden als Gruppe wahrgenommen.

d. Gesetz der Symmetrie

Elemente, die symmetrisch angeordnet sind, werden als Gruppe im Vordergrund wahrgenommen, während die nicht dazu passenden asymmetrischen Elemente in den Hintergrund rücken.

e. Gesetz der Geschlossenheit

Elemente, welche eine Linie bilden und dadurch eine Fläche begrenzen, werden als Gruppe wahrgenommen.

f. Gesetz des weiterführenden bzw. gleichen Verlaufs

Eine Linie, die durch Elemente gebildet wird, wird meist gedanklich in der gleichen Weise fortgeführt, wie sie begonnen hat. Es genügen oft schon Bruchstücke von Formen, welche dann gedanklich vervollständigt werden.

g. Gesetz der Erfahrung

Komplexe Anordnungen von Elementen werden meist mit Bekanntem assoziiert. Größere Elemente repräsentieren größere Zahlen als z.B. kleinere Elemente.

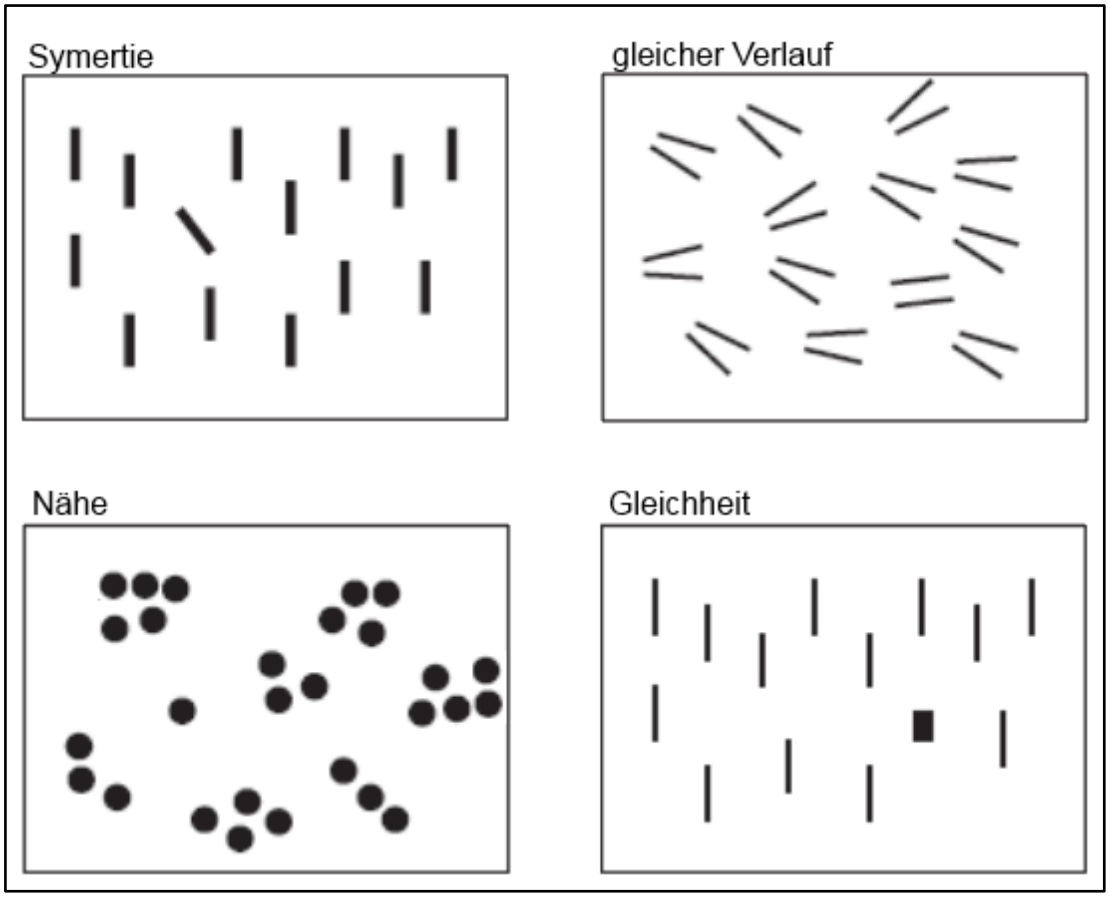
h. Gesetz der Kontinuität

Elemente, welche Formen oder Richtungen von vorangegangenen Elementen fortzusetzen scheinen, werden als Gruppe wahrgenommen.

i. Gesetz der gemeinsamen Bewegung

Elemente, die sich gleichzeitig in eine Richtung bewegen, werden als Gruppe wahrgenommen. Eine Bewegung in einem zeitlichen Verlauf von links unten nach rechts oben wird als positiv wahrgenommen [6].

Beispiel-Bilder:



[Abbildung 2: Beispiele zu Visualisierungstechniken [7]]

2.4 Grundlagen der Farbnutzung

Die Verwendung von Farbe ist für die Benutzerfreundlichkeit und Effektivität jeder Visualisierung extrem wichtig. Gute Visualisierungen können leicht zerstört werden, wenn Farbe eingesetzt wird, ohne die Prinzipien der menschlichen Wahrnehmung zu berücksichtigen. Farbe wird bei einer Visualisierung von Elementen mit Gruppen-Zusammengehörigkeit assoziiert.

Der Mensch besitzt drei Typen von Zapfen im Auge, die für die Farbwahrnehmung zuständig sind. Die Sensitivität der Zapfen ist sehr unterschiedlich, am deutlichsten nehmen Menschen Rot, dann Grün und am geringsten Blau war [7].

a. Eindeutige Farbtöne

Die Grundfarben werden leicht erkannt. Sie sind zu bevorzugen, wenn nur wenige Farben benötigt werden. Auch sollten, wenn möglich, nicht mehrere Farben aus dem gleichen Farbspektrum zur Darstellung verwendet werden.

b. Kontrast zum Hintergrund

Es muss beachtet werden, dass Farben abhängig vom Hintergrund unterschiedlich wirken und zur Geltung kommen. Wechselwirkungen können durch eine einheitliche Kontur (z.B. schwarz oder weiß) minimiert werden.

c. Unterscheidbarkeit

Die Farben sollen gut voneinander zu unterscheiden sein. Wenn es darum geht, ein Objekt einer bestimmten Farbe schnell zu finden, sollte die entsprechende Farbe eine hohe Farbspektrums-Differenz zum Rest der Visualisierung aufweisen.

d. Farbschwäche

Es gilt zu berücksichtigen, dass fast 10% der menschlichen Bevölkerung eine bestimmte Form von Farbschwäche aufweist, nämlich die Rot-Grün-Schwäche. Daher sollten Farbkodierung basierend auf rot-grün Kontrasten vermieden werden [7].

Empfohlene Farben für die Visualisierung:

Rot, Grün, Gelb, Blau, Schwarz, Weiß,

Pink, Cyan, Grau, Orange, Braun, Lila

[Abbildung 3: Farbbeispiele [7]]

Darüber hinaus gilt es noch folgende Punkte zu berücksichtigen:

Es sollten nur wenige Farben verwendet werden. Nur 5 bis 10 Farben können von Menschen schnell unterschieden werden.

Bei der Verwendung von Blau gilt, dass die beste Verwendung in großen Flächen stattfindet. Blau ist nicht für dünne Linien geeignet. Dies muss wegen schlechter menschlicher Wahrnehmung berücksichtigt werden.

Die Farben Rot und Grün ziehen den Fokus des betrachtenden Menschen auf sich.

Die Farben Schwarz, Weiß und Gelb treten optisch in den Hintergrund. Diese Farben werden nur in der Peripherie wahrgenommen.

Um den Kontrast zu erhöhen, sollten benachbarte Farben in Farbe und Helligkeit variieren.

Für große Flächen gilt es im Allgemeinen, keine satten Farben zu verwenden, bei Textmarkierungen sollten helle Farben gewählt werden.

Außerdem sollten keine benachbarten Farben verwendet werden, die sich nur im Blau-Anteil unterscheiden. Der Blauanteil ist von Menschen schwer wahrzunehmen.

Abschließend ist anzumerken, dass Assoziationen zu Farben von Menschen durch deren kulturelle Sozialisation variieren. In Deutschland gilt Rot z.B. als Gefahrensignal, in China steht Rot für das Leben. Also sollten diese Assoziationen in den Hintergrund gestellt, oder den jeweiligen kulturellen Gegebenheiten in den Ländern angepasst werden [7].

2.5 Resümee

“Why should we be interested in visualization? Because the human visual system is a pattern seeker of enormous power and subtlety. The eye and the visual cortex of the brain form a massively parallel processor that provides the highest-bandwidth channel into human cognitive centers.”

—Colin Ware, author of *Information Visualization: Perception for Design [8]*

Es ist wissenschaftlich erwiesen, dass es Darstellungsformen gibt, die es dem Menschen erleichtern, Informationen aufzunehmen und in Relation zueinander zu setzen.

Für die Visualisierung von Threat Intelligence Informationen eignen sich die hier vorgestellten Techniken besonders gut, da es der ikonische Speicher erlaubt, die aufbereiteten Informationen intuitiv aufzunehmen.

3 TI für CDCs

Herkömmliche Präventivmaßnahmen (bspw. Firewalls, Anti-Viren-Filter oder VPNs) reichen gerade im Kampf gegen gezielt gesteuerte Cyberattacken nicht mehr aus. Solche Cyberattacken erfolgen beispielsweise durch fremde Regierungen oder durch von der Konkurrenz beauftragte Hacker-Gruppen, deren deklariertes Ziel Wirtschafts- oder Industriespionage ist. Allgemein wird dann von sogenannten „Advanced Persistent Threats“ (APTs) gesprochen, wobei im Gegensatz zu „altmodischen“ Bedrohungen hierbei nicht gegen einen „automatisierten“ Code gekämpft wird, sondern gegen professionelle und hochmotivierte Hacker.

Es findet daher allmählich ein Paradigmenwechsel in der IT-Sicherheit statt. Antiviren-Programme, Intrusion Detection Systeme oder andere Präventivmaßnahmen stellen weiterhin einen unverzichtbaren Basisschutz gegenüber dem „Rauschen“ der allgemeinen und unspezifischen Angriffe im Internet dar. Diese Maßnahmen können aber nicht gegen APTs standhalten, die auf der Benutzerebene durch manipulierte PDFs oder Office-Dokumente in die Unternehmen gelangen. Daher ist es aus Verteidigersicht essenziell, die genauen Vorgehensweisen der Angreifer zu kennen und Zugriffe auf für solche Angriffe genutzte Systeme im Internet z.B. für Drive-by-Exploits oder Watering-Holes zu überwachen. Bisherige Maßnahmen müssen daher sowohl um ein intelligentes Monitoring als auch um erprobte Incident Response Prozesse sinnvoll erweitert werden.

Dank fortgeschrittener Risikoanalysen weiß man heute in der Regel sehr viel mehr über die Assets, die es in einer Organisation zu schützen gilt. Verhältnismäßig wenig weiß man hingegen weiterhin über die Angreifer. Für die nötige Threat Intelligence werden eine Menge an Daten benötigt, um diese zu kombinieren, im Kontext auszuwerten und so mehr über die potenziellen Angreifer zu erfahren. Um dieses Wissen über Angreifer zu erschließen, werden die dazu notwendigen Funktionen und Aufgaben heute in den CDCs aufgebaut und eingesetzt.

Neben den Analysten der CDCs gibt es weitere potentielle Nutzer für Threat Intelligence Informationen. Dazu gehören sowohl die Mitarbeiter in einem Lagezentrum oder CERT, die auf Grundlage dieser detaillierten Informationen allgemeine Warnungen und Handlungsempfehlungen herausgegeben. Aber auch Betreiber kritischer Infrastrukturen und die CERTs aus verschiedenen Geschäftsbereichen können einen direkten Nutzen aus solchen Informationen ziehen, die auf gezielte Angriffe hinweisen [2].

In dieser Arbeit werden Threat Intelligence Informationen von verschiedenen Anbietern und Services zur Betrachtung herangezogen. Dazu werden die Anforderungen der Cyber Defence Centre an Threat Intelligence hinzugenommen. Auf Grundlage eines erweiterten Modells von Threat Intelligence werden die weiteren Ausführungen vorgenommen. Unter zur Hilfenahme des Modells soll eine möglichst realitätsnahe und zugleich allgemeingültige Aussagen über Daten zur Informationsgewinnung für TI in einem CDC, getroffen werden.

3.1 Nutzen von Threat Intelligence

Die Informatik kann im Rahmen der IT-Sicherheit große Mengen an Daten gewinnen, z.B. durch Open Source Plattformen oder internes Monitoring. Daten zu betrachten, ohne diese in Beziehung zu setzen, bringt keinen Nutzen. Das Gewinnen der Daten ist also nicht das Problem. Ein Problem entsteht erst bei der Verarbeitung, Stichwort: Big Data. Um die Daten richtig auszuwerten und nutzen zu können, benötigt man TI. Bei der stetig anwachsenden Datenflut stellen sich Fragen, die zur Qualitätssicherung von TI beantwortet werden müssen:

- Welche Daten sind für die Auswertung relevant?
- Wie kann eine ausreichende Qualitätskontrolle der Daten durchgeführt werden?

Für die Identifizierung von relevanten Daten sind Analysten erforderlich. Damit die Anzahl der erforderlichen Analysten nicht proportional zu der Informationsmenge ansteigt, sind weitere technische Hilfsmittel für die Informationsverarbeitung erforderlich. Die Unterstützung der Analysten durch geeignete Hilfsmittel löst jedoch nicht die Problematik der Qualitätssicherung. Die Häufigkeit, wie oft eine Information in verschiedenen Datenquellen wiedergeben wird, kann ein Indiz für deren Relevanz sein. Dies ist aber keine verlässliche Aussage zu ihrem Wahrheitsgehalt. Wenn diese Informationen zur Entscheidungsfindung verwendet werden sollen, dann müssen sie durch traditionelle Mittel verifiziert werden [2].

3.2 Funktionsweise von Threat Intelligence

In der Literatur werden unterschiedliche Ansätze für die Datenbeschaffung angeführt. Zum einen gibt es öffentlich zugängliche Daten über Bedrohungen aus dem Internet (Open Source), zum anderen können Daten erhoben werden, die durch ein eigenes Sensornetz erhoben werden (Closed Source) und außerdem können Daten zwischen Organisationen, die sich gegenseitig vertrauen, auch untereinander ausgetauscht werden (Information Sharing).

Um bei Open Source Daten einen Qualitätsstandard aufzustellen, treten einige offenkundige Fragen auf, die vor der Verarbeitung beurteilt werden müssen:

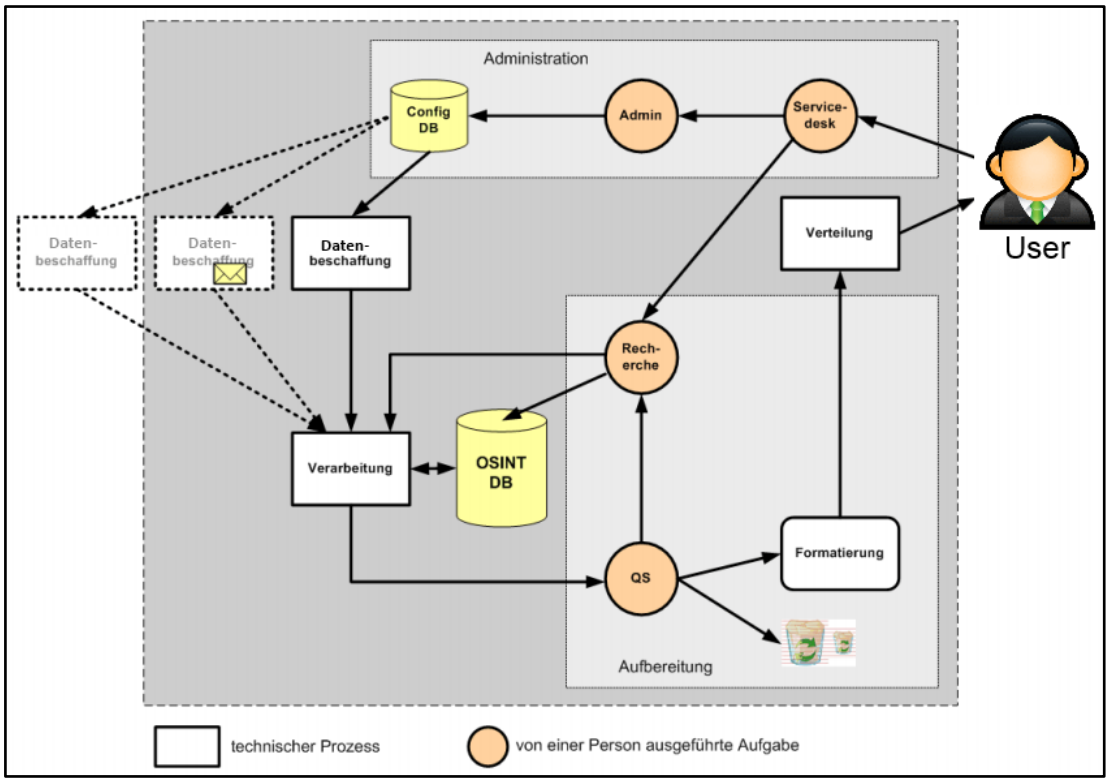
• Sind die Daten richtig?

• Sind die Daten komplett?

• In welcher Beziehung stehen die Daten zu mir?

Außerdem müssen bei der Qualitätskontrolle bestimmte Filter berücksichtigt werden, z.B. ob geografische Gegebenheiten eine Rolle spielen sollen oder ob ein Fokus auf ein Geschäftsfeld zu legen ist. Geografische Gegebenheiten könnten interessant sein, um Häufungen und damit erhöhte Eintrittswahrscheinlichkeiten zu erkennen. Bei Geschäftsfeldern können z.B. mit speziellen Angriffen nacheinander verschiedene Unternehmen attackiert werden [9].

Die grundsätzliche Arbeitsweise von Threat Intelligence Systemen könnte man als zyklisch beschreiben. Für die Erläuterung wird bei der Administration angesetzt, welche die technischen Voraussetzungen schafft und den Ablauf überwacht. Der zweite Schritt in diesen Systemen ist die Informationsbeschaffung. Als nächstes findet die Verarbeitung statt. Danach müssen die Daten visuell aufbereitet werden. Der letzte Schritt ist dann die Verteilung. (siehe Abbildung 4).



[Abbildung 4: Allgemeiner Ablaufplan von TI [2]]

Im Block „Administration“ werden die Datenquellen und die Systemvoraussetzungen zur Datenbeschaffung administriert.

Die in der Abbildung gekennzeichnete „Datenbeschaffung“ wird in Abschnitt 3.3 Datenquellen erklärt. In dieser Arbeit werden verschiedene Datenquellen betrachtet.

Der Schritt „Verarbeitung“ symbolisiert den Vorgang der Datenkombination, um Zusammenhänge zwischen einzelnen Daten herstellen zu können. Dies geschieht z.B. durch die Korrelation von Datumsangaben oder Zielobjekten.

Auf „ONIST“ wird im Abschnitt 3.3.1 eingegangen. Die Abkürzung „DB“ steht für Daten Bank.

Im Block „Aufbereitung“ findet die Informationsgewinnung statt. Die Daten werden miteinander kombiniert und visualisiert, um neue Informationen zu gewinnen und diese an den Menschen weiterzugeben.

„Verteilung“ beschreibt den Vorgang, die visualisierten Daten an die User auszuliefern.

3.3 Datenquellen

Bei der Beschaffung von Analysedaten gibt es zwei Ansätze. Einerseits können bereits zusammengestellte Daten bezogen werden, hier als Open Source aufgeführt, oder die Daten werden vom Unternehmen selbst gesammelt. Dies wird durch die in den folgenden Unterpunkten ausgeführten Ansätze beschrieben. Die intern generierten Daten nehmen eine Sonderposition ein, da diese immer notwendig sind, damit TI ebenfalls auf Incidents reagieren kann und diese bei der Informationsgewinnung berücksichtigt.

Auf käufliche, also Closed Source, Analysedaten wird hier nicht speziell eingegangen. Auch nicht auf Informationen von anderen Unternehmen oder Partnern. Es wird angenommen, dass diese in Bezug auf die weitere Verarbeitung wie Open Source Daten behandelt werden können.

3.3.1 Open Source

In dem Kontext von Threat Intelligence ist der Begriff „Open Source“ anders geprägt als im restlichen IT-Umfeld. Unter „Open Source Daten“ werden Daten verstanden, die allgemein zugänglich sind. Dabei ist zu berücksichtigen, dass der Zugriff auf die Quellen frei ist und diese einfach abzurufen sind. Diese Daten können z.B. aus den Medien, öffentlichen Stellen, Universitäten, Organisationen oder aus dem Privatsektor stammen. Ein besonderer Stellenwert kommt dabei dem Internet zu. Das Internet enthält die größte Informationsmenge, die der Mensch jemals geschaffen hat. Darüber hinaus stellt das Internet den Nutzern eine Reihe von neuen und innovativen Kommunikationsmethoden zur

Verfügung. Heutzutage ist nicht mehr die Verfügbarkeit von Informationen ein Problem, sondern eher die Fragestellung: Wie findet man die gewünschte Information? Ohne die Verwendung von Suchmaschinen wären Rechercheaufgaben im Internet in vielen Fällen von vornherein zum Scheitern verurteilt. Aber auch bei Verwendung der verbreiteten Werkzeuge ist das Resultat einer Anfrage in vielen Fällen nicht zufriedenstellend. Je nach Suchbegriff erhält man entweder zu viele Treffer oder es wird gar kein passendes Ergebnis geliefert.

Im Gegensatz zu den klassischen Informationsquellen, die unter den Begriff Closed Source fallen (u.a. Satelliten- und Fernmeldeaufklärung, sowie die Auswertung menschlicher Quellen), ist die Beschaffung von Open Source Informationen erheblich kostengünstiger. Darüber hinaus können die Informationen von mehreren potenzieller Analysten erfasst werden. Ebenso gestaltet sich die Verarbeitung und Weitergabe dieser Informationen erheblich leichter, da es sich dabei um nicht vertrauliche Informationen handelt. Die Hauptstärke der Open Source Intelligence (OSINT) liegt in der Vermittlung des Kontextes, der für die Einschätzung der aktuellen Sicherheitsfragen unabdingbar ist. Durch die anwachsende Komplexität der zu betreuenden Systeme ist es notwendig, sich abzeichnende Probleme und Trends frühzeitig zu identifizieren [2].

3.3.2 Botnetz-Analyse

Die Daten, die in der Botnetz-Analyse erhoben werden, sind wie Open Source Daten frei zugänglich, jedenfalls sofern die Daten rechtlich korrekt erhoben wurden. Im Unterschied zu Open Source Daten werden die Daten aus der Botnetz-Analyse jedoch von den IT-Betreibern oft selbst erhoben.

Die Beobachtung von Botnetzen kann riskant sein, da bei Aufdeckung der Beobachtung mit DDoS Angriffen zu rechnen sein kann. Mittelfristig kann auch angenommen werden, dass ein „Vergeltungsschlag“ erfolgen könnte.

Die Konsequenz ist, dass eine Beobachtung und Analyse von Botnetzen nicht aus dem Netzsegment erfolgen darf, in dem die zentralen IT-Systeme der Threat Intelligence oder der Produktivsysteme angesiedelt sind. Die Analysten müssen entweder unterschiedliche Anfragen durchführen oder die IP-Adressen müssen regelmäßig gewechselt werden [2].

Bleibt noch zu erwähnen, dass sich einige der Informationsbeschaffungsmaßnahmen in Deutschland als nicht eindeutig legal herausgestellt haben. Die Infiltrierung von Botnetzen für Informationsbeschaffung ist beispielsweise in Deutschland nicht legal. Hingegen ist die Registrierung der IP-Adressen, mit denen die Rechner Verbindung aufnehmen, keineswegs bedenklich. Es ist also möglich, C&C-Server zu identifizieren.

3.3.3 Intern generierte Daten

In Unternehmen, die IT einsetzen, fallen ebenfalls Daten an, die sich für die Auswertung eignen. Daten, die hier erhoben werden können, sind meist geordnete Daten, wie unter anderem:

- Zugriffshäufigkeiten auf IP-Adressen
- Systemlast
- IDS-Daten
- Uptime/Downtime Monitoring
- Bandbreitenüberwachung
- Applikations-Überwachung
- QoS Monitoring
- Sensoren(Raumtemperatur, Luftfeuchtigkeit, etc...)
- Event-Loggs

Die gesammelten Daten werden zu Administration der Systeme benötigt und an unterschiedlichen Stellen aufgezeichnet. Die „Bandbreitenüberwachung“ und die „Zugriffshäufigkeiten auf IP-Adressen“ werden von der Firewall registriert. Hingegen werden das „Uptime/Downtime Monitoring“ und die „Applikations-Überwachung“ von Monitoring-Tools übernommen. Im Betrieb einer Organisation werden diese Daten gesammelt, um Incidents zu registrieren und statistische Auswertungen fahren zu können.

3.3.4 Soziale Medien

Das Überwachen, Filtern und Analysieren von Daten aus sozialen Medien generiert ungeordnete Informationen. Diese Informationen können vorbeugend genutzt werden, um Angriffe zu erschweren und zu verhindern.

Der amerikanische Geheimdienst CIA nutzt zum überwachen von Sozialen Medien nach den Dokumenten von Edward Snowden z.B. das Programm „PRISM“ [10]. Diese Arbeit wird in Organisationen meist von Analysten übernommen.

Im Zuge dieser Art der Informationsbeschaffung werden z.B. Foren oder Chats überwacht, um Angriffsziele und Angriffsvektoren zu bestimmen, bevor diese akut werden. So kann die Schadenswirkung minimiert werden.

3.4 Berücksichtigte Anbieter

Da hier ein allgemeines Modell von Threat Intelligence erstellt werden soll, werden die Daten einiger am Markt vertretenen Anbietern betrachtet, um Gemeinsamkeiten und Unterschiede herauszustellen. Dazu soll das Angebot verschiedener Hersteller, die sich in IT-Securety spezialisiert haben, untersucht werden. Es wird erwartet, dass die Hersteller unterschiedliche Schwerpunkte gesetzt und Verfahren entwickelt haben. Um die Daten zu betrachten, gilt es daher, die größte Schnittmenge an Gemeinsamkeiten zu finden.

Als schwierig hat sich herausgestellt, Anbieter zu finden, welche eine gesamtheitliche Threat Intelligence Architektur anbieten. Es gibt einige Hersteller, die Teile einer solchen Architekturen oder Dienstleistungen, die dazu notwendig sind, anbieten. Der Fokus dieser Arbeit liegt auf der Optimierung der Threat Intelligence Informationsverarbeitung, durch die eine bessere Nutzung und Gewinnung von TI ermöglicht wird. Eine Analyse von fertigen Lösungen, welche typischerweise aus mehreren Teilen von unterschiedlichen Herstellern zusammengesetzt ist, würde an dieser Stelle zu weit führen und kann nicht geleistet werden.

3.4.1 AlienVault

AlienVault ist ein amerikanischer Entwickler und Anbieter von Computer-Sicherheits-Hardware. Die Hauptgeschäftsfelder von AlienVault sind die Bereitstellung kostenpflichtiger Netzwerksicherheit, für Organisationen und Unternehmen.

Die Quellen, die AleinVault heran zieht, um Daten für die Threat Intelligence zu schürfen, kommen aus dem Netzwerk von AlenVault selbst. Das Unternehmen hat ein breites Netzwerk aus Honypots aufgebaut und analysiert selbst Daten aus Hacker-Foren. Darüber hinaus beziehen sie Daten von Anbietern, welche mit ihnen zusammenarbeiten. Die so gewonnenen Daten werden als Open Source Daten auch anderen zur Verfügung gestellt. Als letzte Datenquelle dienen die Systeme der Nutzer. Hier wird die Last und das Verhalten überwacht, um daraus Rückschlüsse ziehen zu können [11].

- Schwachstellen and Exploits (software versionen)
- Bruteforce Attacken (IP-Adressen)
- Denial of Service Attacken (IP-Adressen)
- Malware Detection (Signaturen)
- Network-level Attacks
- SCADA Attacks (Signaturen)
- System Probing and Scanning
- Malicious Activity [12]

3.4.2 ENISA

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ist eine 2004 von der Europäischen Union gegründete Agentur. Sitz von ENISA ist Iraklio auf Kreta. Direktor der Behörde ist Udo Helmbrecht.

Die ENISA führte unter anderem eine Krisenmanagement-Übung ("Cyber Europe 2010") durch. Diese Übung sollte die Pläne, Richtlinien und Verfahren der EU-Mitgliedsstaaten bei der Bekämpfung von möglichen Krisen überprüfen. Darauf aufbauend wurde Ende 2012 die Krisenmanagement-Übung "Cyber Europe 2012" durchgeführt. ENISA soll dem European Cybercrime Centre zur Seite stehen [13].

- Drive-By Downloads (links)
- Malicious Code: Worms/Trojans (Signaturen)
- Code Injection (Signaturen)
- Exploit Kits (Signaturen)
- Botnets (IP-adresssen)
- Denial of Service Angriffe (IP-adresssen)
- Phishing (Links)
- Spam (Signaturen)
- Rogueware/Ransomware/Scareware (Signaturen) [14]

3.4.3 FireEye

FireEye ist ein Unternehmen mit Sitz in Milpitas, Kalifornien, USA. Das Unternehmen bietet Netzwerksicherheits-Software- und Dienstleistungen an. Bekannt wurde das Unternehmen unter anderem durch den Fund mehrerer Zero-Day-Lücken in Microsofts Internet Explorer und der Beteiligung an Untersuchungen von mehreren Botnetzen.

Das Unternehmen verfolgt einen neuen Sicherheitsansatz, der garantieren soll, dass zwischen Warnung und Abwehr nur wenige Minuten vergehen. Die Grundlage dafür ist die Datenverkehrsanalyse mittels Signaturen und heuristischen Methoden, um verdächtiges Verhalten auszumachen. Anschließend wird versucht, mittels Wiedereinspielung gegen eine Sandbox, eine Kompromittierung die Arbeitsweise nachzuvollziehen. Dies wird als revolutionäre Lösung gegen fortschrittliche Schadprogramme wie Advanced Persistent Threats und Zero-Day-Exploits vermarktet [22].

- Data flow analysis
- IP-Adressen (C&C Server, Phishing)
- Signaturen (IDS, Viren, Spam) [23]

3.4.4 MISP

Seit 2012 ist MISP als Open Source-Tool, unter GPLv3 Lizenz verfügbar. Zunächst vom belgischen Verteidigungsministerium entwickelt, wie das CyDefSig Projekt.

MISP ist eine Plattform für den Austausch, das Speichern und das Korrelieren der Indikatoren von gezielten Angriffen. Sie ermöglicht es Unternehmen, Informationen über Malware und ihre Indikatoren zu teilen. MISP-Nutzer sollen von dem Wissen über vorhandene Malware oder Bedrohungen profitieren. Das Ziel dieser Plattform ist die Verbesserung der Gegenmaßnahmen gegen gezielte Angriffe. Dazu wird die Einrichtung von Präventivmaßnahmen und Detektion von Angriffen ermöglicht [15].

- IP-Adressen
- Ganze Dateien (daraus gewonnen: IP-Adressen, Softlinks, Signaturen,…) [16]

3.4.5 ThreatSTOP

ThreatSTOP ist ein privat geführter Bedrohungsverlag. Informationen werden über ein zum Patent angemeldetes Verfahren verteilt. Dies geschieht über eine private, sichere Domain Name System. Das Unternehmen wurde von CTO Tom Byrnes gegründet.

Die Idee der Plattform beruht darauf, effizientere Methode für die Verwaltung und Sicherung von großen, heterogenen Gruppen von Firewalls zu finden. ThreatSTOP Service ist eine Cloud-basierte Lösung, die es bestehenden Firewalls und Routern ermöglicht, ein- und ausgehende Kommunikation zu Command und Control (C&C) Architektur zu blockieren. Der Service verhindert Datendiebstahl, reduziert Netzwerklast und Angriffsfläche [17].

- IP-Adressen [17]

3.4.6 Durch Anbieter gewonnene Daten

Wie sich herausgestellt hat, sind die Vorgehensweisen der Datenanbieter und damit auch die zur Verfügung gestellten Daten sehr unterschiedlich. In den Unterpunkten vom Abschnitt 3.4 Berücksichtigte AnbieterBerücksichtigte Anbieter werden die angebotenen Daten genau beschrieben. Um die Daten miteinander in Beziehung setzen zu können, müssen die Datenkategorien verallgemeinert werden, soweit das möglich ist. Einige der Datensätze passen in keine zu verallgemeinernde Kategorie oder würden eine eigene Kategorie bilden

Das von allen Anbietern zur Verfügung gestellte Minimum an Open Source Daten stellen IP-Adressen dar, die bereits bei anderen Vorfällen auffällig wurden. Signaturen von Malware wurden von vier der fünf betrachteten Anbietern zu Verfügung gestellt. Drei der betrachteten Anbieter stellen verdächtige Links zur Verfügung.

3.5 Daten zur Informationsgewinnung

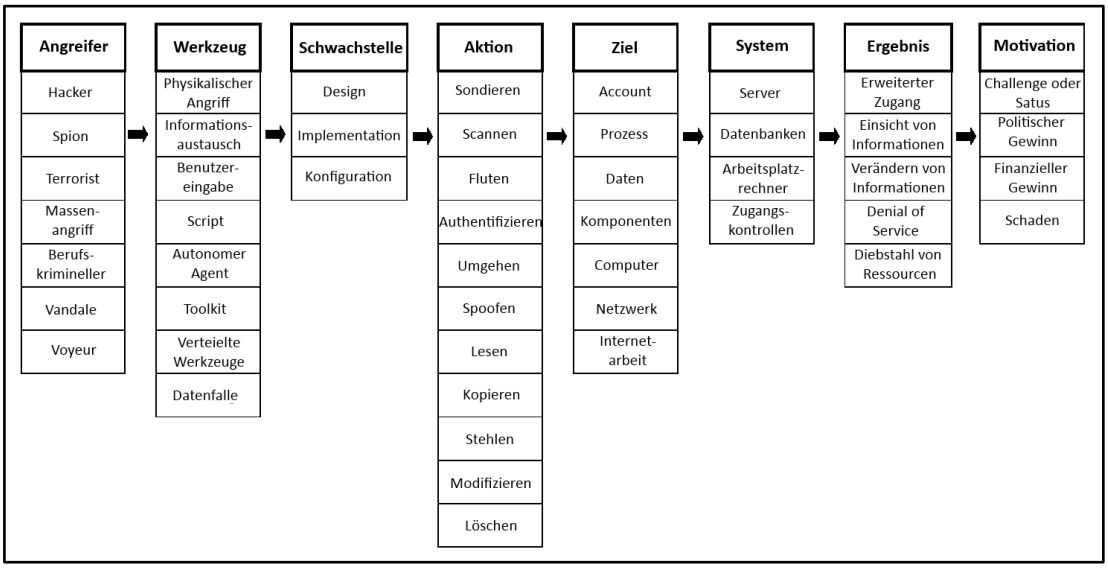
Wie bereits in Unterpunkt 3.4.6 ausgeführt, können nicht alle Daten in Datenkategorien zur besseren Vergleichbarkeit verallgemeinert werden.

Die verallgemeinerten Datensätze sind in die Kategorien IP-Adressen, Signaturen, Links, Applikationsdaten, Netzwerkdaten, Systemdaten und Event-Loggs zu unterteilen.

Zur Informationsgewinnung ist die Kombination dieser Daten erforderlich. Es wäre denkbar, eine Matrix zur Kombination aufzustellen und so jede denkbare Kombination aufzuführen und zu analysieren. Es geht bei der Informationsgewinnung jedoch nicht um die einfache Kombination zweier Datensätze, viel mehr muss der Kontext und das Ziel der Kombination berücksichtigt werden. Dabei erweist sich eine Kombination aus mehreren Datensätzen als nützlich (siehe Unterpunkt 4.5.3 ff.).

3.6 Modell von Threat Intelligence

Um ein allgemeines Modell zu Threat Intelligence zu erstellen, wird von einem Modell von John D. Howard und Thomas A. Longstaff ausgegangen. Das Modell wird für diesen Kontext um die zu schützenden Systeme erweitert.



[Abbildung 5: Angepasstes Modell von TI [18]]

Wie deutlich zu sehen ist, wird in diesem Modell jeder Aspekt vom Angreifer bis zum erfüllen seiner Motivation berücksichtigt. Es wird eine logische Verknüpfung zwischen dem Angreifer und dessen Ziel hergestellt.

Der Grundsatz „Know your enemy“ wird dadurch erfüllt. Es werden nicht nur die Assets oder Schwachstellen betrachtet, auch der Angreifer selbst wird berücksichtigt.

Durch die in dieser Arbeit erschlossenen Daten, die auf technischen Mitteln beruhen, können nur Zusammenhänge auf der technischen Ebene aufgezeigt werden. Zusammenhänge auf der Ebene von Geschäftsprozessen sind für eine Bewertung von Zielen der Angreifer wichtig, aber für diese Arbeit zu speziell und würden auch keine allgemeingültigen Aussagen zulassen.

3.7 Datenbezug zu CDCs

Wie bereits in der Definition von CDCs beschrieben, wird dieser Begriff in verschiedene Untergruppen unterteilt. Es soll nun geprüft werden, ob die Daten zur Informationsgewinnung, die für ein CDC sinnvoll sind, in einer der Untergruppen keine Anwendung findet. Dazu ist es notwendig, die Aufgaben und den Nutzen von TI in den Untergruppen herauszuarbeiten.

3.7.1 Verwendung in einem CERT

Ein CERT ist in erster Linie reaktiv tätig. Wenn es zu einem Vorfall kommt, kann ein CERT zum Einsatz kommen. Es werden drüber hinaus Schulungen gegeben und Unterstützung bei Entscheidungsprozessen geleistet.

„Das DFN-CERT bietet ein umfangreiches Spektrum an Dienstleistungen rund um das Thema IT-Sicherheit an. Dazu gehören unter anderem: Prävention, Reaktion, Beratung, Risikoanalysen, Schulungen, Forschung. In den Bereichen Netzwerksicherheit, Incident Response und Datenschutz sowie der Aufbau und Unterhalt skalierbarer und leistungsfähiger PKI-Infrastrukturen.“ [19]

In einem CERT soll auf Angriffe und Vorfälle reagiert werden. Dazu ist es notwendig, Daten zusammenzutragen und zu analysieren. Um einen optimalen Einsatz der Mittel zu gewährleisten, müssen die Ereignisse bewertet werden, dabei hilft Threat Intelligence. Weitere Anwendungsgebiete in einem CERT sind z.B. Prävention oder die Risikoanalyse. Dazu werden die Filter und die Qualitätskontrolle angepasst. Mit den Anpassungen wird die TI auf unterschiedliche Aufgaben ausgerichtet.

In Bezug auf das TI-Modell (siehe Abbildung 5) beschäftigt sich ein CERT vorwiegend mit den Kategorien „Aktion“, „System“ und „Ergebnis“. Hier wird nochmal die reaktive Arbeitsweise der CERTs deutlich.

3.7.2 Verwendung in einem SOC

Die Rolle eines SOC ist die aktive Erkennung von Sicherheitsvorfällen. Diese Instanz ist meist direkt in Firmen oder als Dienstleister angesiedelt. Es wird sowohl reaktiv als auch präventiv für Sicherheit gesorgt.

Zu den Aufgaben gehören:

• „Proactive Security Services“, die IT-Infrastrukturen Härten und Überwachen.

• „Incident Handling“, also die Behandlung von aufgetretenen Security Incidents.

• „Intelligence Services“, das Erkennen von Securitytrends und außergewöhnlichen Security-Anomalien [20].

In einem SOC muss der Normalbetrieb gewährleistet werden. Um ungewöhnliche Vorfälle zu untersuchen und diese in ein größeres Bild einordnen zu können, wird hier Threat Intelligence eingesetzt.

SOCs beschäftigen sich in Bezug auf das TI-Modell (siehe Abbildung 5) mit den Punkten „Ziel“, „System“ und „Schwachstelle“.

3.7.3 Verwendung in einer IT-Frühwarnzentrale

Diese Instanz ist dafür zuständig Informationen zu sammeln und zu filtern. Diese Tätigkeit findet im Hintergrund statt und arbeitet den CERTs und Unternehmen zu. Die hier gesammelten Informationen fließen aber auch in die TI ein, z.B. Erkenntnisse über neue Angriffsmethoden.

Von einer IT-Frühwarnzentrale wird Folgendes geleistet: „Integration von Sensornetzen (Daten) und anderen Quellen (Informationen) in einem übergreifenden Informationsmanagement; Unterstützung eines verteilten Analystenteams bei der täglichen Arbeit durch die integrierte Sicht; Bereitstellung nutzergruppenspezifischer Auswertungen und Analysen zur Verbesserung von deren Sicherheit.“ [21]

In einer IT-Frühwarnzentrale gilt es, möglichst schnell Gefahren zu erkennen. Jede Abweichung vom normalen Verhalten muss schnellstmöglich analysiert und bewertet werden. Dazu wird Threat Intelligence genutzt. TI gewinnt durch intelligente Datenkombination Informationen. Der Informationsgewinn findet ohne manuelle Analyse statt und weist auf mögliche Gefahren hin.

Eine IT-Frühwarnzentrale analysiert die Kategorien „Motivation“, „Ziel“, „Werkzeug“ und „Angreifer“ (siehe Abbildung 5). Es wird versucht den Angreifer und dessen Vorgehen so früh wie möglich zu identifizieren.

3.8 Ziel der Threat Intelligence

Ziele von TI sind sowohl das Priorisieren von Alarmen als auch die Vorbeugung von Angriffen und die quantitative Reduzierung des Auftretens grundsätzlicher Probleme. Wurde eine Gefahr erkannt, so wird diese an die zuständigen Menschen gemeldet. Allgemeiner formuliert ist das Ziel die Verbesserung der Gegenmaßnahmen gegen Angriffe. Im Optimalfall soll TI Gefahren erkennen, bevor diese akut werden.

3.9 Resümee

Die Anwendung von TI, insbesondere die Analyse von Angriffen, ist ein lohnenswertes Ziel. Um dies zu verwirklichen, sind entsprechende Maßnahmen zu treffen. Durch Techniken wie Botnetz-Analyse oder Honypots steigt das Bedrohungspotential weiter an. Diese Techniken setzen bewusst Schwachstellen ein, wodurch mehr Angreifer aufmerksam werden können. Auch ist bei der Erschließung von Open Source Datenquellen damit zu rechnen, dass eigene IP-Adressen blockiert werden, da Webserver und Dienste regelmäßig abgefragt werden. Auch Botnetz-Analysen können Informationen zu Tage fördern. Bei diesem Vorgehen muss man sicherstellen, dass eigene Systeme nicht in den Fokus der Angreifer geraten [2].

In allen Untergruppen des Cyber Defence Centre findet Threat Intelligence Anwendung. Von der Optimierung des Erkennens von Problemen und der Kommunikation zwischen Mensch und Maschine, kann jede Instanz profitieren.

Es wurde gezeigt, dass es nicht möglich ist, eine Untergruppe des CDC aus der Betrachtung heraus zu nehmen. Unter Abschnitt 3.7 Datenbezug zu CDCs wurde für jede Untergruppe des CDC ein oder mehrere Anwendungsfälle genannt. Da jede Untergruppe TI benötigt, gibt es keinen Datenbereich der nicht interessant wäre. TI wird bei dem vorbeugenden Schutz genauso genutzt wie bei der Bekämpfung eines aktiven Angriffs und der Analyse vergangener Angriffe. Es müssen also alle Daten, die zur Verfügung stehen, berücksichtigt und ausgewertet werden. In diesem Zusammenhang besteht wieder das Eingangs erwähnte Big-Data-Problem, so dass nur eine verbesserte Auswertung sowie eine optimale Visualisierung hier Mehrwert bringt.

4 Umsetzungsmöglichkeiten

4.1 Annahme

Das Ziel dieser Arbeit ist es, Wege aufzuzeigen, um den Informationsfluss in einem Cyber Defence Centre zu optimieren und damit eine verkürzte Reaktionszeit auf aktuelle Gefahren und neue Trends oder Entwicklungen bei bekannten Gefahren zu ermöglichen.

Die in dieser Arbeit aufgestellte Annahme ist es, dass dies durch eine Optimierung der Darstellung und Kombination der Informationen realisiert werden kann, wenn es gelingt, die Darstellungen so anzupassen, dass die zu übermittelnden Informationen intuitiv aufgenommen werden können. Darüber hinaus muss ein möglichst großer Teil der Aggregation und Korrelation der Informationen in den verwendeten Programmeablauf verlagert werden, wodurch eine zusätzliche Zeitersparnis zu erzielen ist, zumal Menschen von der Menge verfügbarer Informationen überlastet wären.

4.2 Methodik

Zunächst sollen Daten, welche zusammengefasst werden können, um einen Erkenntnisgewinn zu erzielen, betrachtet werden. Die daraus gewonnen Informationen sollen nun als optimale Visualisierung an den Menschen weiter gereicht werden, damit diese möglichst zeitnah reagieren können. Um die Eignung und Effizienz der Methoden zu überprüfen, wird ein User-Test durchgeführt.

4.2.1 Kombination der Informationen

Es gilt, relevante Daten zu kombinieren, wodurch neue Informationen ersichtlich werden. Dabei wird in diesem Schritt die Glaubwürdigkeit der Quellen der Daten nicht berücksichtigt. Im Zuge dieser Arbeit wird davon ausgegangen, dass die zugrunde liegenden Daten unzweifelhaft sind. Eine Kombination, die quellenübergreifend stattfindet, ist somit ohne weiteres möglich. In der Praxis muss, wie dies bereits im vorherigen Kapitel ausgeführt wurde, eine Qualitätssicherung erfolgen, bevor die Daten miteinander kombiniert werden dürfen.

Es werden anhand der verfügbaren Daten einige Kombinationen vorgestellt, die dem Autor als besonders sinnvoll erschienen. Jede Organisation hat einen eigenen Fokus, den es zu bei der praktischen Umsetzung in einem konkreten Kontext zu betrachten gilt. Die Bezugnahme auf ähnliche Anforderungen von CDCs ermöglicht es in dieser Arbeit, einen relativ großen Umfang von Daten zu nutzen.

4.2.2 Verwendete Visualisierungstechniken

Wie in Kapitel 2 Visualisierung bereits beschrieben, hängt die Art der Visualisierung von der Bewertung der zu übermittelnden Information ab.

Durch die Verwendung von unterschiedlichen Farbtönen können beispielsweise Bewertungen der von einem Objekt ausgehenden Gefahren klar ersichtlich gekennzeichnet und intuitiv unterschieden werden.

4.2.3 Testdesign

Den an dem Test teilnehmenden Personen wird ein Multiple-Choice-Bogen vorgelegt und eine Präsentation mit den erarbeiteten Visualisierungen gezeigt. Die jeweiligen Visualisierungen werden dabei nur kurze Zeit für die Personen sichtbar sein, auch für die Beantwortung des Bogens steht nur eine begrenzte Zeit zur Verfügung. Die Testpersonen sollen jeweils angeben, was sie von den Visualisierungen intuitiv erkannt bzw. wahrgenommen haben. Beispielsweise, welches System Ausgangspunkt eines aktuellen Angriffs ist gegenüber anderen, die nicht beteiligt oder betroffen sind.

Es werden Fragen zu einigen Eckpunkten der Visualisierung gestellt. Zur Kontrolle der Aussagen werden nicht ersichtliche Antwortmöglichkeiten in den Test aufgenommen.

4.3 Teilnehmer

Um einen Nutzen für CDCs aufzuzeigen, werden zwei Tests mit unterschiedlichen Testgruppen durchgeführt. Die eine Gruppe („CDC-Mitarbeiter“) besteht nur aus Menschen, die in einem CDC arbeiten. Es muss des Weiteren eine Gruppe berücksichtigt werden, die sich durch Funktion, Tätigkeit oder aufgrund der Tiefe des technischen Fachwissens von der Gruppe der CDC-Mitarbeiter unterscheidet. Dadurch ist die Notwendigkeit gegeben, Informationen allgemein verständlich aufzubereiten. Als Kontrolle dient daher eine Testgruppe von Menschen, die unterschiedliche Berufe ausüben und nicht im IT-Sicherheits-Umfeld arbeiten.

Visualisierungen, die bei beiden Gruppen ein einheitliches Ergebnis erzielen, können als allgemeinverständlich angesehen werden.

4.3.1 CDC-Mitarbeiter

Im Rahmen der Arbeit war es möglich eine freiwillige Umfrage unter den Mitarbeitern im „DFN-CERT“ durchzuführen. Die Mitarbeiter sind Teil einer Untergruppe eines CDCs und somit eine repräsentative Menge an Menschen für die Arbeitsweise eines CDCs.

4.3.2 Kontrollgruppe

Die für den Vergleich herangezogene Gruppe setzt sich aus Menschen mit unterschiedlichen Berufen und Alter zusammen. Die Ergebnisse des Tests in dieser Gruppe werden als allgemeine Assoziation angenommen.

4.4 Visualisierung

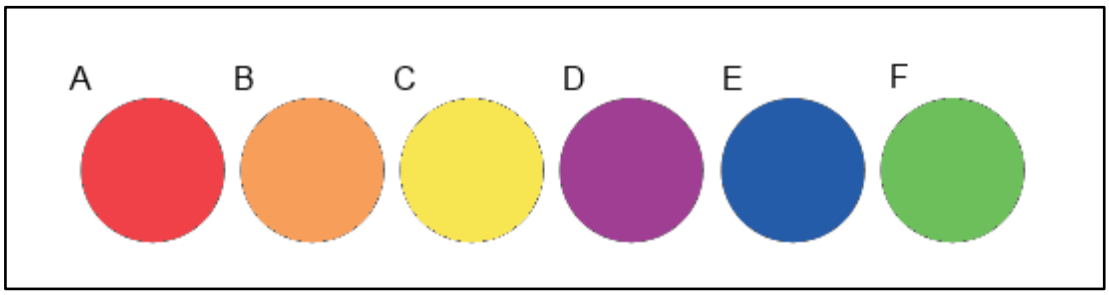
Es werden nun alle Beispiele zur Visualisierung und Datenkombination angeführt, die den Testpersonen vorgelegt wurden. Zunächst wird die Wahrnehmung der Farben und Symbole getestet. Hier geht es zunächst darum (4.4.1 und 4.4.2), eine intuitive Assoziation zu finden, die in keinem konkreten Zusammenhang steht. Danach (4.4.3 ff.) soll verdeutlicht werden, wie Visualisierung helfen kann, diese Informationen intuitiv verständlich aufzubereiten. Mit Hilfe dieser Visualisierungen wird dann gezeigt, welche Informationen durch die Testpersonen aus den Visualisierungen gewonnen werden können.

Bei den ersten beiden Beispielen (4.4.1 und 4.4.2) ist eine Mehrfachauswahl ausdrücklich erlaubt. Es soll keine direkte Verbindung von einer Darstellung zu einer Antwort hergestellt werden. Vielmehr sollen die Assoziationen der Testpersonen herausgestellt werden.

4.4.1 Farbwahrnehmung

In der ersten Visualisierung geht es um die Assoziationen, die von Menschen zu ausgewählten Farben hergestellt werden, ohne dies in einen Kontext zu setzen.

Um die Testpersonen nicht zu überfordern, konnte nur eine Auswahl an Farben in diesen Test aufgenommen werden. Einige der Quellen nannten die Farben „Rot“ und „Grün“ als die am stärksten assoziierten. Diese Behauptung sollte überprüft werden. Darüber hinaus wurden zufällige Farbwerte gewählt [7].

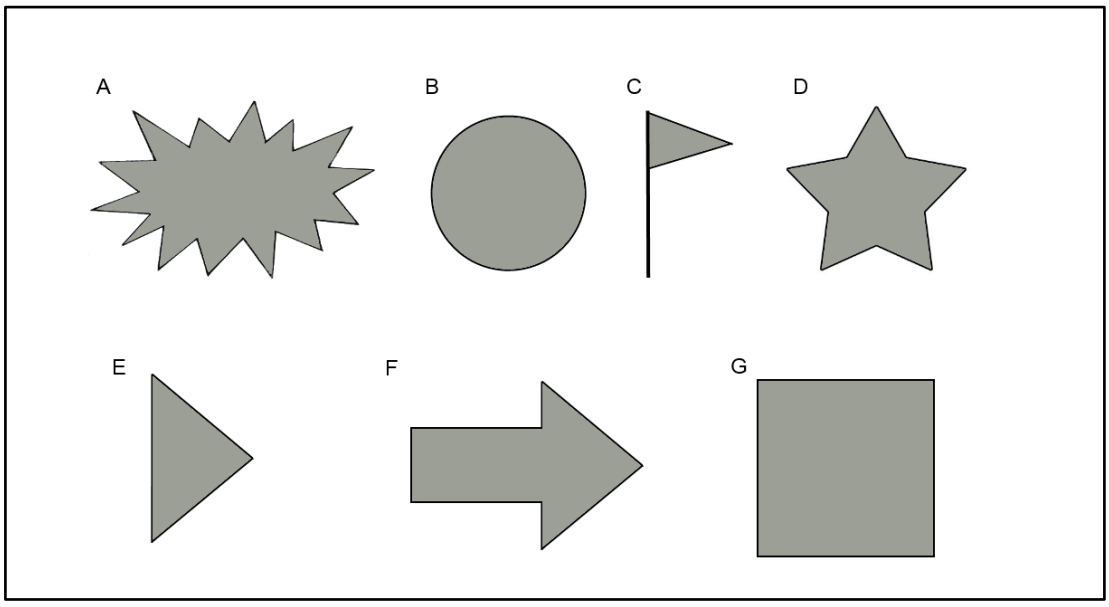


[Abbildung 6: Beispielvisualisierung zu Farben]

4.4.2 Symbole

Durch diese Visualisierung kann eine Assoziation und damit ein Wiedererkennen und eine Gruppierung erreicht werden. Wird bestimmten Symbolen intuitiv Bedeutung zugeordnet, können diese die Erfassung des Kontextes erheblich erleichtern.

In dieser Visualisierung wurde absichtlich keine Bezeichnungen für sie Symbole genannt, da Menschen mit diesen Bezeichnungen bereits Assoziationen verbinden könnten. Darüber hinaus können die Symbole unterschiedlich wahrgenommen werden. Das Symbol „D“ z.B. könnte als Vieleck oder als Stern erkannt werden.

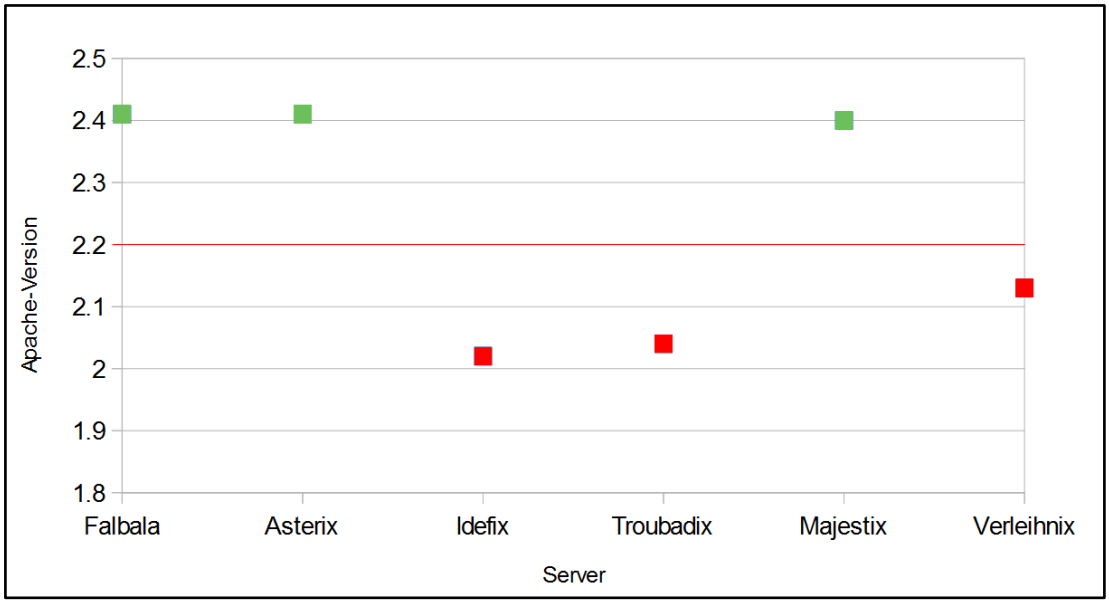


[Abbildung 7: Beispielvisualisierung zu Symbolen]

4.4.3 Informationsgewinnung: Patch-Level

Der Patch-Level von Systemen ist durch den Administrator meist durch wenig Aufwand zu ermitteln. Die Version einer eingesetzten Software auf mehreren Systemen und die Anzahl der Systeme, die diese Software verwenden, können visuell gut erfasst werden.

Ein neuer Angriff, der bestimmte Softwareversionen betrifft, wird durch die Überwachung von Herstellerinformationen und CERT-Meldungen zeitnah bekannt. Nun müssen die Administratoren möglichst schnell eine Übersicht gewinnen, welche der in der Organisation eingesetzten Systeme bereits gepatched wurden. Die noch nicht gepatcheten Systeme sollen durch die Visualisierung schnell gefunden werden können.



[Abbildung 8: Beispielvisualisierung zu Patch-Level]

Die als grün gekennzeichneten Systeme stellen in dem oben beschriebenen Kontext keine Gefährdung dar. Bei diesen Systemen wurden bereits neuere Versionen der Software installiert, die nicht angreifbar sind.

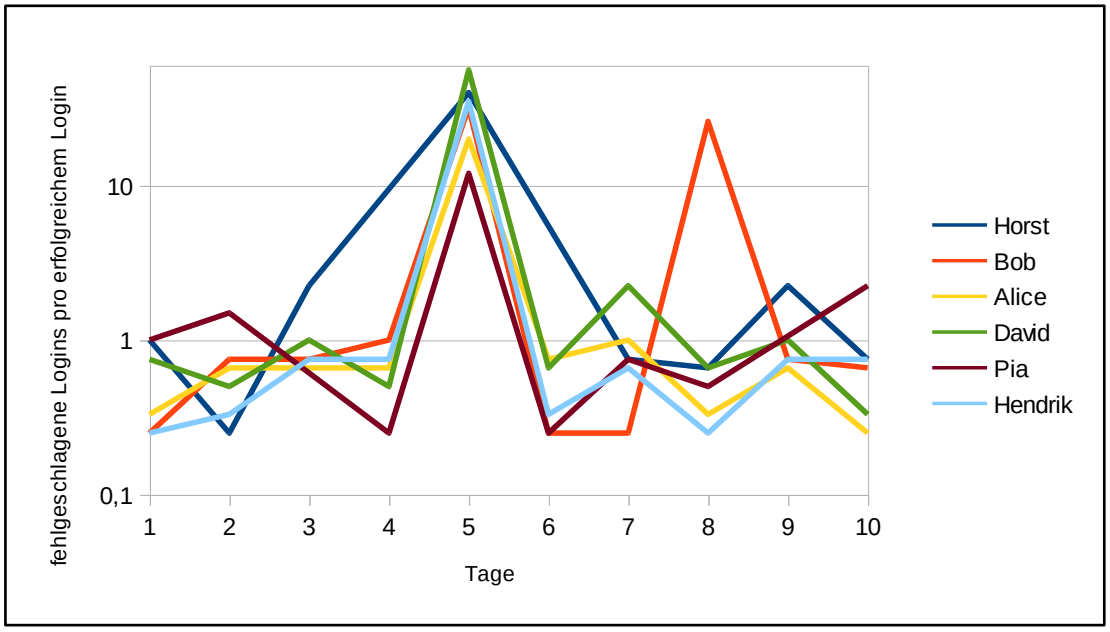
Rot werden in der Grafik Systeme gekennzeichnet, die in diesem Kontext gepatched werden sollten.

Die in der Grafik rot und dick dargestellte Linie stellt den Versionsstand der Software dar, ab der die auszunutzende Schwachstelle behoben wurde.

4.4.4 Informationsgewinnung: User-Login-Versuche

Login-Versuche von Mitarbeitern werden standardmäßig protokolliert. Diese Daten können die fehlgeschlagenen Logins so wie die erfolgreichen Logins in ein Verhältnis setzen. Hinzu kann ein zeitlicher Faktor genommen werden. Dadurch können diese Daten klar erfassbar visualisiert werden.

In diesem Beispiel sollen die von einem Angreifer potenziell kompromittierten Accounts schnell erkannt werden.



[Abbildung 9: Beispielvisualisierung zu User-Login-Versuche]

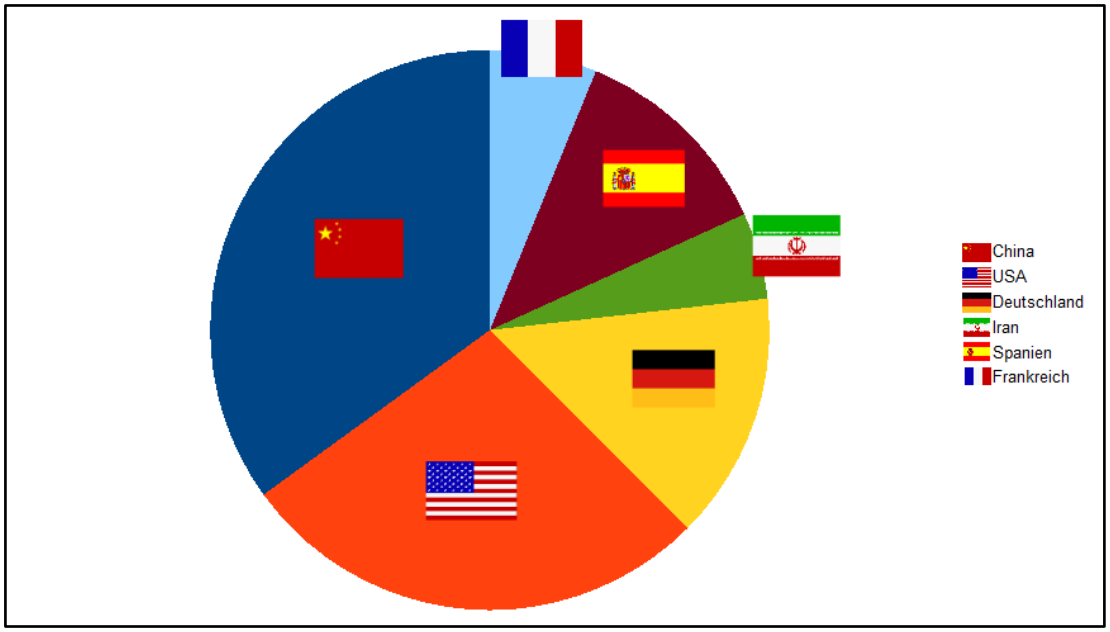
Die Skalierung der Y-Achse ist logarithmisch gewählt um die Diskrepanzen sinnvoll darzustellen.

Das Verhältnis von fehlerhaften zu gültigen Login-Versuchen liegt zunächst in einem zu erwartenden Bereichen. An Tag fünf wird ein deutlicher Zuwachs der Fehlversuche für alle User registriert. Der User Bob hat am achten Tag wieder eine deutlich erhöhte Menge an Fehlversuchen. Ein drastischer Anstieg der fehlgeschlagenen Login-Versuche deutet auf einen Brute-Force-Angriff hin.

4.4.5 Informationsgewinnung: Länderzugriffe

Verbindungen zwischen internen und externen Systemen können durch die Firewall geloggt werden. Die externen IP-Adressen können Ländern zugeordnet werden. Zugleich kann die insgesamt übertragene Datenmenge für das jeweilige Land ermittelt werden. Eine Grafik, die diese Informationen in ein Verhältnis setzt, kann den durchschnittlichen Datenverkehr in einzelne Länder darstellen.

Das in diesem Beispiel zu Grunde liegende Ziel könnte sein, einen besonders hohen Datenabfluss in ein Land zu erkennen, um dann durch weitere Maßnahmen diese genauer zu untersuchen.



[Abbildung 10: Beispielvisualisierung zu Länderzugriffe]

In dieser Grafik wird herausgestellt, in welche Länder Daten aus der Organisation übermittelt werden.

In diesem Beispiel nehmen USA und China eine Spitzenposition ein. Besteht nun mit den jeweiligen Ländern ein Abkommen oder eine Handelsbeziehung und entspricht dies dem üblichen Verhältnis, sind diese in diesem Kontext nicht weiter zu beachten. Hingegen kamen bisher kaum Datenübertragungen zum Iran vor, hier an Platz vier, dem nachgegangen werden muss.

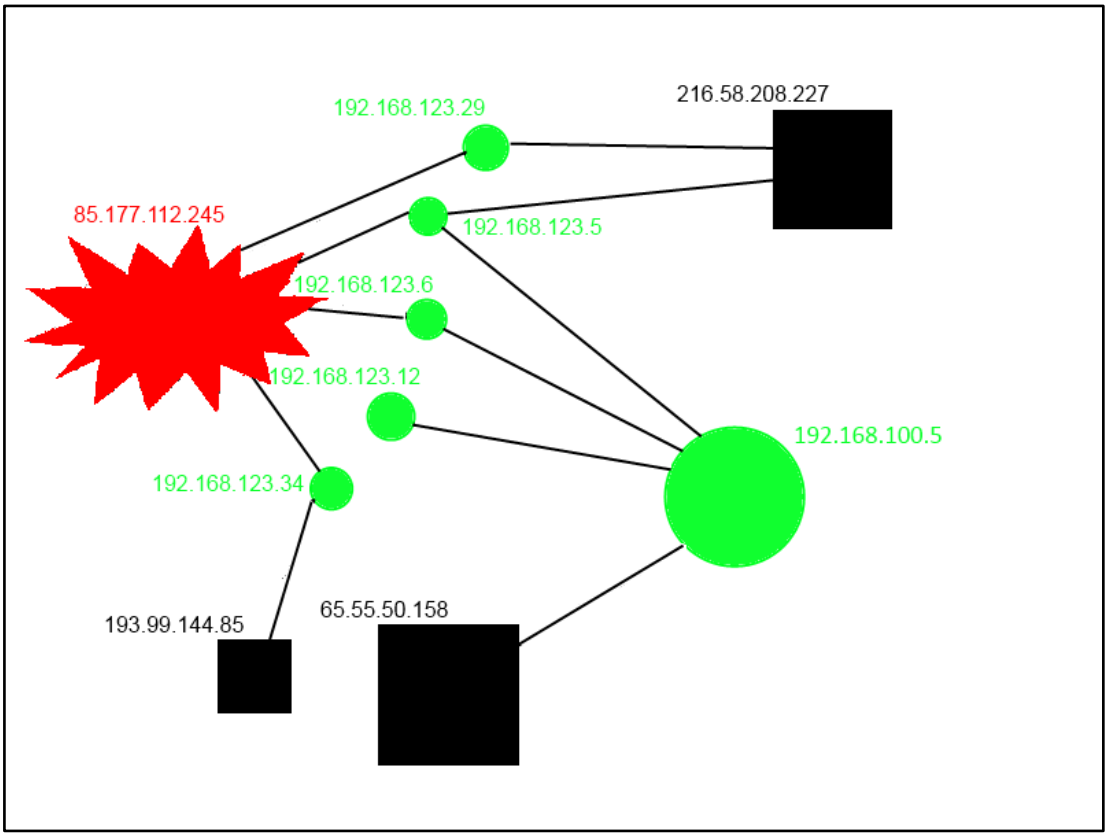
Die Legende ist mit Länderflaggen umgesetzt worden. Eine Zuordnung kann so bei bekannten Ländern auf den ersten Blick erfolgen, ohne die Legende zu studieren.

Es besteht ebenfalls die Möglichkeit, eine Zuordnung durch farbliche Abstimmung zu implizieren. Dazu würden beispielsweise die Länder mit dem höchsten Datenaustausch rot markiert werden, die folgenden mit gelben Farbschattierungen und die Länder mit dem geringsten Datenaufkommen in grün.

4.4.6 Informationsgewinnung: Zugriffe auf C&C-Server

Es können Zugriffszahlen auf IP-Adressen mit Quell- und Zieladressen, welche durch ein internes Monitoring erfasst sind, kombiniert werden. Wenn noch Informationen über aktive C&C-Server hinzukommen, die im Rahmen von CERT-Kooperationen ausgetauscht werden, kann innerhalb einer Grafik eine gebündelte Menge an Informationen übermittelt werden, die Beziehungen zu solchen C&C-Servern direkt aufzeigen.

Das Ziel der Datenkombination ist, Informationen über die Anzahl der potenziellen Bots im Netzwerk zu gewinnen.



[Abbildung 11: Beispielvisualisierung zu C&C-Server]

Die farbliche Markierung signalisiert, wie die IP-Adresse eingestuft wird. Rot bedeutet, die Adresse ist als kompromittiert zu betrachten. Verbindungen hierhin bedeuten daher Handlungsbedarf. Die grüne Farbe steht für Systeme, die im Netzwerk der Organisation stehen. Die schwarzen Symbole repräsentieren Systeme außerhalb der eigenen Organisation, über die keine weiteren Daten vorliegen und zunächst neutral bewertet werden.

Die Verbindungen lassen einen Zusammenhang zwischen den Adressen erkennen, um schnell eine mögliche Ausbreitung nachzuvollziehen. Hier kann die Anzahl der Zugriffe nicht abgeschätzt werden.

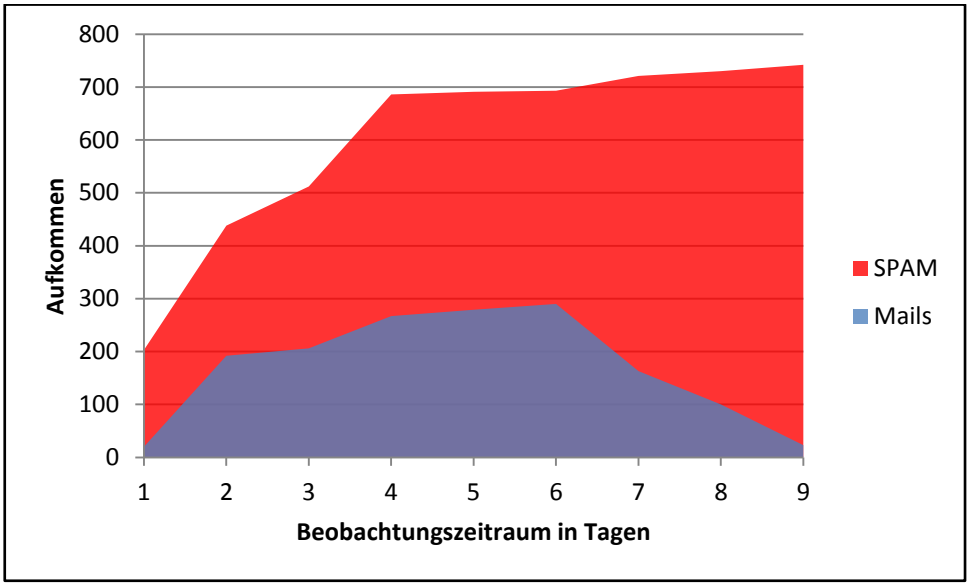
Die Symbole wurden zur weiteren Hervorhebung der jeweiligen Gruppen genutzt.

Die Größe des Symbols, zugehörig zur IP-Adresse, zeigt dessen Aktivität. Dies ist intuitiv einfacher wahrzunehmen, da dies die Bedeutung des Systems direkt verdeutlicht. Alternativ können die Verbindungen unterschiedlich stark dargestellt werden, dies ist jedoch verwirrender, weil es oft überlappende oder parallele Verbindungen schlecht darstellbar macht.

4.4.7 Informationsgewinnung: Spam Mails

Das Mail-Aufkommen für ein überwachtes Postfach über eine längere Zeitspanne kann mit dem Anteil der dort angefallenen Spammails/Phishing in Relation gesetzt werden.

Ein Ziel dieser Darstellung wäre z.B. einen Zusammenhang zwischen anlaufender Werbeaktion der Organisation (durch erhöhten Mailverkehr zu erkennen) und gesteigerten Phishing-/Malwareangriffen herzustellen.



[Abbildung 12: Beispielvisualisierung zu SPAM/Mails]

Ein sprunghafter Anstieg des unverdächtigen Mailverkehrs lässt auf einen Indikator z.B. eine Werbeaktion der Organisation schließen, bei der dieses Postfach angegeben wurde.

Die zusätzlichen rot eingefärbten Daten sind als Phishing/Spammails identifiziert. Ein ähnliches Verhalten wirft die Frage nach den Initiatoren einer solchen Angriffswelle auf.

4.5 Multiple-Choice-Bogen

Auf Grundlage der Visualisierungen wurden Multiple-Choice-Bögen entwickelt. Diese sind gut vergleichbar und geben eine Rückmeldung zu den gezeigten Visualisierungen. Um den Testpersonen keine manipulierenden Anhaltspunkte auf die Antworten zu geben, wurden zusätzliche, nicht stimmige Antwortmöglichkeiten in den Test aufgenommen.

In dieser Arbeit geht es um die intuitive Wahrnehmung der durch Threat Intelligence gewonnen und visuell aufbereiteten Daten. Dazu werden den Testpersonen die Visualisierungsbeispiele in Form einer Präsentation vorgestellt. Während der Präsentation sollen die Testpersonen die Multiple-Choice-Bögen ausfüllen.

Die ersten zwei Beispiele haben keinen Kontext, so dass die Testpersonen zunächst Sicherheit bei den zu beantwortenden Fragen bekommen können. Da bei den ersten beiden Beispielen nicht die schnelle Auffassung getestet wird, sondern die Testpersonen sich über die Assoziationen bewusst werden müssen, besteht kein Anlass, Testbedingungen zu setzen.

Es ist den Testpersonen möglich, mehrere Antworten anzukreuzen, da in diesem Test keine eins-zu-eins Beziehung zwischen den Darstellungen und den Antworten aufgezeigt werden soll. Es ist vielmehr das Ziel der Arbeit, die Assoziationen der Menschen zu einer Darstellung aufzuzeigen.

Die fünf weiteren Beispiele stehen in einem gemeinsamen Kontext und sollen es ermöglichen, eine gestellte Aufgabe optimal lösen zu können. Bei diesen Beispielen werden den Testpersonen, vor der Betrachtung, einige Testbedingungen und Informationen erläutert. Zudem ist es von Interesse, die Betrachtungszeit zu berücksichtigen, in der die Informationen erfasst werden. Um dies zu simulieren, wurden diese fünf Beispiele den Testpersonen nur für eine Zeitspanne von zehn Sekunden gezeigt.

In dem Test werden maximal sieben Antwortmöglichkeiten zu den Darstellungen gegeben, um die Aufmerksamkeitsspanne der Testpersonen nicht zu überbeanspruchen.

In den folgenden Unterpunkten werden die jeweiligen Tests und die den Testpersonen gegebenen Informationen aufgeführt.

4.5.1 Farbwahrnehmung

Wie bereits in 4.4 Visualisierung beschrieben, werden zu den ersten beiden Visualisierungsbeispielen (hier Abbildung 6) keine weiteren Informationen gegeben. Der Multiple-Choice-Test sah wie folgt aus:

1) Farbwahrnehmung

Welche Begriffe assoziierst du mit den folgenden Farben?

	Sicherheit	Gefahr	Achtung	Neuheit	HEX-Wert: 9F3E93	Nichts
A) Rot						
B) Orange						
C) Gelb						
D) Lila						
E) Blau						
F) Grün						
Ich habe eine Farbschwäche, ich lasse die Frage aus.						

[Tabelle 1: Farbwahrnehmung]

4.5.2 Symbole

Zum zweiten Visualisierungsbeispiel (hier Abbildung 7) sah der Multiple-Choice-Test wie folgt aus:

2) Symbole

Welche Begriffe assoziierst du mit den folgenden Symbolen?

	Orts-bindung	Neuheit	Abhängigkeit	Menge	Gefahr	Zeit	Nichts
A							
B							
C							
D							
E							
F							
G							

[Tabelle 2: Symbole]

4.5.3 Patch-Level

Wie bereits in 4.4 Visualisierung beschrieben, werden zu den folgenden Visualisierungsbeispielen (hier Abbildung 8) weitere Informationen gegeben:

- bevorstehender Angriff
- Schwachstelle in veralteter Version
- zu patchende Systeme

Der Multiple-Choice-Test sah wie folgt aus:

3) Patch-Level Welche Daten erkennst du in der Grafik?	
Falballa, Asterix und Idefix müssen gepatched werden.	
Idefix, Troubadix und Verleihnix müssen gepatched werden.	
Alle Server der Organisation.	
Der zu erreichende Patchstand ist mindestens 2.4.	
Der zu erreichende Patchstand ist mindestens 2.2.	
Die Grafik ist mir unverständlich.	

[Tabelle 3: Patch-Level]

4.5.4 User-Login-Versuche

Folgenden Informationen wurden zum Visualisierungsbeispiel (hier Abbildung 9) gegeben:

- Login versuche werden geloggt
- Verhältnis, fehlgeschlagene Login-Versuche pro erfolgreichen Logins

Der Multiple-Choice-Test sah wie folgt aus:

4) User-Login versuche Welche Daten erkennst du in der Grafik?	
Am 2. und 7. Tag wurde die Organisation angegriffen.	
Am 5. Tag wurde die Organisation angegriffen.	
David hat knapp 60 fehleingaben pro erfolgreichem Login.	
Der Angreifer war immer der selbe.	
Am 8. Tag wurde Bobs Account gebrutforced.	
Die Grafik ist mir unverständlich.	

[Tabelle 4: User-Login-Versuche]

4.5.5 Länderzugriffe

Folgende Informationen wurden zum Visualisierungsbeispiel (hier Abbildung 10) gegeben:

• Datenfluss in die jeweiligen Länder beobachtet

Der Multiple-Choice-Test sah wie folgt aus:

5) Länderzugriffe

Welche Daten erkennst du in der Grafik?

Mit USA und China werden die meisten Daten getauscht.	
Mit Frankreich und Spanien werden die meisten Daten getauscht.	
Die Flaggen kenne ich, machen eine Assoziation dadurch leichter.	
Die Flaggen kenne ich nicht, dadurch ist es schwer nach zu vollziehen.	
Es ist schwer die Flaggen zu erkennen.	
Die Grafik ist mir unverständlich.	

[Tabelle 5: Länderzugriffe]

4.5.6 Zugriffe auf C&C-Server

Folgende Informationen wurden zum Visualisierungsbeispiel (hier Abbildung 11) gegeben:

• Verbindung zwischen IP-Adressen

• Verbindungen zu C&C-Server(n) wurden wurde Protokoliert

Der Multiple-Choice-Test sah wie folgt aus:

6) Zugriffe auf C&C-Server

Welche Daten erkennst du in der Grafik?

Die IP-Adresse 85... scheint eine bösartig zu sein.	
Die IP-Adressen 192... sind private Adressen also die Systeme der Organisation.	
Die IP-Adressen in schwarz sind zu vernachlässigen.	
Die IP-Adressen in schwarz sind öffentliche Adressen.	
Ich weiß nicht ob die Größe der Symbole eine Bedeutung hat.	
Die Grafik ist mir unverständlich.	

[Tabelle 6: C&C-Server]

4.5.7 Spam Mails

Folgende Informationen wurden zum Visualisierungsbeispiel (hier Abbildung 12) gegeben:

• Verhältnis von Nutzmails zu Spam-/Phishingmails

Der Multiple-Choice-Test sah wie folgt aus:

7) SPAM Mails

Welche Daten erkennst du in der Grafik?

Es gibt immer mehr Spam als eigentliche Mails.	
Der Anteil der eigentlichen Mails lässt nach einer knappen Woche nach.	
Das Postfach existiert wahrscheinlich schon länger.	
Das Postfach scheint neu zu sein.	
Der Anteil der Spammails wächst kontinuierlich.	
Die Grafik ist mir unverständlich.	

[Tabelle 7: SPAM/Mails]

4.6 Auswertung

Dieses Kapitel ist, wie die vorhergehenden Kapitel (4.4 Visualisierung und 4.5 Multiple-Choice-Bogen), entsprechend der Reihenfolge der Beispielvisualisierungen unterteilt. Durch diese Unterteilung ist es möglich, für jedes Beispiel einen direkten Vergleich zwischen den CDC-Mitarbeitern und der Kontrollgruppe zu ziehen.

Zunächst werden die Antworten der CDC-Mitarbeiter analysiert. Hierbei werden die gewonnen Erkenntnisse textuell formuliert. Die Erkenntnisse werden mit Prozentangabe untermauert.

Danach wird die Kontrollgruppe analysiert. Bei der Beschreibung wird wie bei den CDC-Mitarbeitern vorgegangen.

Als Abschluss des jeweiligen Unterpunkts werden die Unterschiede zwischen den beiden Gruppen herausgestellt und interpretiert.

4.6.1 Farbwahrnehmung

CDC-Mitarbeiter:

Assoziationen ohne Kontext haben interessante Ergebnisse gebracht. Knapp 52% der Assoziationen brachte Rot mit „Gefahr“ in Verbindung, weitere 30% assoziierten mit der Farbe „Achtung“. Orange wurde zu gleichen Teilen mit „Gefahr“ und „Achtung“ assoziiert. Die Farbe Lila hat bei den meisten Testpersonen keine Assoziation hervorgerufen. Die eindeutigste Assoziation wurde bei Grün mit „Sicherheit“ gefunden, auf diese Verbindung fielen immerhin über 70% der Antworten.

Kontrollgruppe:

Teile der Ergebnisse stimmen mit der Gruppe der CDC-Mitarbeiter überein. Jeweils 45% der Assoziation der Farbe Rot entfällt auf „Gefahr“ und „Achtung“. 50% der Assoziationen mit Orange fielen auf „Achtung“. Bei Gelb ist die Assoziation mit „Achtung“ (58%) stärker ausgeprägt. Auch in dieser Gruppe fiel es den Testpersonen schwer, eine Assoziation mit Lila herzustellen. Grün wurde in dieser Gruppe noch zu 55% mit „Sicherheit“ in Verbindung gebracht.

Vergleich der Gruppen:

Bei den CDC-Mitarbeitern gab es bei der Farbe Rot eine deutlichere Assoziation mit „Gefahr“. Gelb hingegen wurde bei der „Kontrollgruppe“ stark mit „Achtung“ assoziiert. Bei Grün stimmen die Testpersonen beider Gruppen überein, diese Farbe mit „Sicherheit“ zu assoziieren.

Allgemein können starke Assoziationen mit Rot und Grün festgestellt werden. Diese Farben eigenen sich gut zur Darstellung von Gefahren bzw. Sicherheit. Bei Orange ist eine merkliche Assoziation mit „Achtung“ aufgetreten.

Bei der Auswertung muss berücksichtigt werden, dass ein Großteil der Testpersonen aus dem gleichen Kulturkreis stammt. Bei einem Internationalen Test würden die Ergebnisse mit hoher Wahrscheinlichkeit anders ausfallen.

4.6.2 Symbole

CDC-Mitarbeiter:

Die Mitarbeiter eines CDC haben unerwartete Assoziationen aufgezeigt. Das Symbol A wurde fast ausschließlich mit „Gefahr“ und „Neuheit“ in Verbindung gebracht, dies aber zu nahezu gleichen Teilen. 62% der Angaben fielen bei dem Symbol C auf „Ortsbindung“. D wurde zu gleichen Teilen mit „Neuheit“ und „Nichts“ in Verbindung gebracht. Die eindeutigste Assoziation wurde bei dem Symbol F mit „Abhängigkeit“ gefunden. Mit dem Symbol G haben die Testpersonen am wenigsten Assoziationen verbinden können.

Kontrollgruppe:

Bei den Symbolen wurde „Neuheit“ und „Ortsbindung“ verstärkt erkannt. Das Symbol A wurde zu zweidritteln mit „Neuheit“ und zu einem Drittel mit „Gefahr“ assoziiert. 50% der Angaben entfielen auf den Zusammenhang von Symbol B zu „Menge“

Vergleich der Gruppen:

Die Auswertung der beiden Gruppen hat einen Zusammenhang zwischen Symbol A und sowohl „Neuheit“ als auch „Gefahr“ belegt. Das Symbol B wurde von beiden Gruppen mit „Menge“ assoziiert. Bei dem Symbol C stimmten die Testpersonen ebenfalls überein, eine „Ortsbindung“ zu sehen. Die Symbole D, E und F wurden von den Gruppen unterschiedlich bewertet. CDC-Mitglieder haben dem Symbol F eine klare „Abhängigkeit“ zugeschrieben. G wurde in beiden Gruppen keine Assoziation zugeordnet.

Zusammenfassend eignet sich Das Symbol A zur Darstellung von neuen Gefahren und das Symbol C als örtliche Markierung. Mengen und damit auch Mengenverhältnisse lassen sich am besten durch das Symbol B darstellen. Im Kontext eines CDCs lassen sich Abhängigkeiten gut durch das Symbol F visualisieren.

4.6.3 Patch-Level

CDC-Mitarbeiter:

Die dargestellten Informationen wurden schnell erfasst. Ca. 87% der Testpersonen haben die noch zu patchenden Systeme richtig identifiziert und die 2. Antwort gewählt. Mehr als 66% konnten aus der Visualisierung den zu erreichenden Patchstand richtig erkennen.

Kontrollgruppe:

Bei der Kontrollgruppe zeigte sich ein überraschend hoher Erkennungsgrad. 70% der Testpersonen haben die zu patchenden Systeme richtig erkannt. Gut 40% der Befragten haben den zu erreichenden Patchstand der Visualisierung entnehmen können.

Vergleich der Gruppen:

Die primär wahrgenommene Information war die zu patchenden Server. Diese wurden von den meisten Testpersonen beider Gruppen identifiziert. Die CDC-Mitarbeiter konnten darüber hinaus den zu erreichenden Patchstand erkennen.

Das Hervorheben der bedrohten Systeme und des notwendigen Patchstandes durch eine rote Markierung hat die Informationsaufnahme optimiert.

4.6.4 User-Login versuche

CDC-Mitarbeiter:

Bei der Darstellung dieser Visualisierung gab es bei der Präsentation technische Schwierigkeiten. Trotz einer farblichen Verzerrung durch den Beamer konnten fast alle Testpersonen (mehr als 85%) dem Beispiel den Angriff auf die gesamte Organisation entnehmen. Mehr als die Hälfte hat den Angriff auf Bobs Account ermitteln können.

Kontrollgruppe:

Den Angriff auf die Organisation wurde von 80% der Testpersonen erkannt. Eine Testperson konnte die logarithmische Unterteilung der Y-Achse nachvollziehen.

Vergleich der Gruppen:

Der Angriff auf die Organisation wurde durchweg gut erkannt. Die CDC-Mitarbeiter erkannten darüber hinaus den Angriff auf Bobs Account. Nahezu keine Testperson konnte die Werte des Verhältnisses zwischen fehlgeschlagenen Logins und erfolgreichen einschätzen.

Die Wahl eine logarithmische Achse darzustellen hat zu Verwirrung geführt. Es fällt dem Menschen schwer, ein solches System zu durchdringen. Daher ist diese zur Optimierung der Visualisierung von Verhältnissen ungeeignet. Bei dem Test mit den CDC-Mitarbeitern kam es zu einer Farbverzerrung der Darstellung durch den Beamer. Dies kann dazu geführt haben, dass Bob als Angriffsziel nicht erkannt wurde, sondern der Angriff jemanden anders zugeordnet wurde. Ein Problem bei farblicher Darstellung ist also die Ausgabe der Visualisierungen. An dieser Stelle kann es zu Fehlinformationen kommen.

4.6.5 Länderzugriffe

CDC-Mitarbeiter:

In diesem Test zeichnet sich ein klares Bild ab. Mit über 85% wurden am deutlichsten die Länder mit dem höchsten Datenaustausch identifiziert. Zweidrittel der Testpersonen fanden die Flaggen hilfreich, nur 7% haben sich daran gestört.

Kontrollgruppe:

Für die Kontrollgruppe stellte sich diese Grafik als leicht verständlich heraus. Die Länder mit dem höchsten Datenaustausch wurden von 80% der Befragten richtig identifiziert. Die Flaggen haben 60% der Testpersonen weitergeholfen.

Vergleich der Gruppen:

Die deutlichste Informationsgewinnung war bei diesem Beispiel zu sehen. Die Länder, welche am aktivsten Daten mit der Organisation ausgetauscht haben, wurden zuverlässig erkannt. Auch die Flaggen waren den meisten Testpersonen beider Gruppen eine Hilfe.

Die Ergebnisse zeigen, dass sich zum Visualisieren von in Verhältnisse aufgeteilte Mengen ein Kreis-Diagramm anbietet.

4.6.6 Zugriffe auf C&C-Server

CDC-Mitarbeiter:

Es konnten nur wenige Informationen von den Mitarbeitern erfasst werden. Dieses Beispiel wurde als das unverständlichste identifiziert. 20% der Teilnehmer konnten hier keine Informationen entnehmen. Nur 40% der Mitarbeiter haben einen Sinn in der Größe der Symbole vermutet. 60% der Testpersonen haben den C&C-Server identifiziert.

Kontrollgruppe:

Der Angreifer wurde von den meisten Testpersonen erkannt. 90% der Testpersonen konnten den C&C-Server identifizieren. Ungefähr 60% der Befragten haben die schwarzen Symbole als unwichtig eingestuft.

Vergleich der Gruppen:

Der C&C-Server wurde zuverlässig erkannt. Die Kombination des Symbols mit der roten Farbe haben den Fokus auf den C&C-Server gelenkt. Durch die Verwendung unterschiedlicher Symbole wurde deren Aussagekraft durch die Größenverhältnisse in den Hintergrund gerückt.

Es dürfen nur ausgewählte Symbole verwendet werden, um die Testpersonen nicht mit Informationen zu überfordern. Die farbliche Markierung und Gruppierung wird am schnellsten wahrgenommen. Um eine Zusammengehörigkeit zu symbolisieren und gleichzeitig Unterscheide aufzuzeigen, darf maximal jeweils eine Methode eingesetzt werden. Weitere Assoziationen in einer Symbolgruppe verwirren die Testpersonen.

4.6.7 Spam Mails

CDC-Mitarbeiter:

Hier bestehen wenige Unklarheiten. Fast 95% der Befragten hat die Visualisierung soweit verstanden, dass erkannt wurde, dass zu jedem Zeitpunkt mehr SPAM als Mails im Postfach identifiziert werden. 53% der Testpersonen haben dem Postfach zugeschrieben, dass es neu sei.

Kontrollgruppe:

100% der Testpersonen haben erkannt, dass mehr SPAM als nützliche Mails im Postfach eingegangen sind. Den stetigen Zuwachs an SPAM haben 90% nachvollzogen. Das Zurückgehen der Mails haben 70% der Testpersonen erkannt.

Vergleich der Gruppen:

Der Anteil der SPAM-Mails wurde von beiden Gruppen klar erkannt. Die meisten Testpersonen haben auch den kontinuierlichen Anstieg des SPAM-Aufkommens registriert.

Das Postfach wurde von rund der Hälfte der Testpersonen für neu gehalten. Um den Umstand einer angelaufenen Aktion oder eines neuen Postfachs zu verdeutlichen, sollte ein längerer Zeitraum betrachtet werden.

4.7 Resümee

In Vorbereitung des Tests wurden Daten so zusammengeführt, dass neue Informationen gewonnen wurden. Diese Informationen wurden im Anschluss daran den zuständigen Personen veranschaulicht, indem geeignete Visualisierungsformen gefunden wurden. Die praktische Überprüfung der intuitiven Wahrnehmung hat gezeigt, dass viele der in dieser Arbeit vorgestellten Techniken für einen optimalen Informationsfluss zwischen Maschine und Mensch sorgen können und bestätigen somit die dieser Arbeit zugrunde liegende Annahme.

5 Fazit und Ausblick

5.1 Fazit

Die Arbeit hat das Ziel erreicht. Nicht nur wurde gezeigt, dass es möglich ist, Daten grafisch zu bündeln, sondern auch diese Informationen leicht verständlich für den Menschen dazustellen.

In der Arbeit wurden zunächst die Begrifflichkeiten definiert und erklärt. Hierbei ist wichtig zu beachten, dass einige der Begriffe in der Fachliteratur noch nicht allgemeingültig und exakt definiert wurden. In dieser Arbeit musste also ein eigenes Verständnis von diesen Begriffen erarbeitet werden. Einige der Definitionen stimmen vielleicht nicht vollständig mit dem Verständnis der jeweiligen Leser dieser Arbeit überein, sind aber im Rahmen dieser Arbeit ausreichend. Es wurde versucht, die Begriffe soweit wie möglich und so spezifisch wie nötig zu fassen.

Anschließend wurde beispielhaft gezeigt, wie Daten kombiniert werden können. Durch die grafische Aufbereitung werden die durch die Kombination neu gewonnen Informationen leicht für den Menschen verständlich.

Abschließend wurde festgestellt, dass bei einer Darstellung, wie sie hier erarbeitet wurde, der Fokus auf die zu übermittelnden Informationen zu legen ist. Das bedeutet, dass im Vorfeld geplant werden muss, welche Daten erhoben werden können, wie diese im Zusammenhang stehen und welche Erkenntnisgewinne durch ihre Kombination zu erreichen sind. Bei der Darstellung gilt es, den Fokus auf die Informationen zu legen, welche an den Menschen weitergegeben werden sollen. Es muss also viel Arbeit im Vorfeld geleistet werden, um eine Zeitersparnis im täglichen Betrieb zu erreichen.

5.2 Ausblick

Weiterführende Arbeiten in diesem Bereich könnten sich damit befassen, die hier gewonnenen Erkenntnisse in Programmcode umzusetzen. Also eine GUI zu bauen, die sich aus verschieden Datenquellen bedient und die Informationen darstellt. Dazu müssten eine Reihe von APIs geschaffen werden, damit die Software auf verschiedene Systeme zugreifen kann.

Des Weiteren könnte diese Arbeit auf einen bestimmten Fall angewendet werden, um ein bestimmtes, bereits vorhandenes System, zu erweitern bzw. zu optimieren. Das würde sich firmenintern anbieten, wenn dort bereits Systeme für z.B. Monitoring vorhanden sind.

Die Arbeit kann auch als Grundlage genutzt werden, um die GUI einer neuer Threat Intelligence Software anzufertigen. In diesem Fall würden die Daten von der Software selbst generiert und weitere, in dieser Arbeit nicht genannte, Daten können hinzugefügt werden.

Literaturverzeichnis

[1] URL: http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20110405_01, 01.07.2015

[2] “Frühwarnung vor IT-Angriffen zum Schutz von Informationsinfrastrukturen” / Bundesamt für Sicherheit in der Informationstechnik – 2008. Bundesamt für Sicherheit in der Informationstechnik 2008

[3] “Applied Security Visualization“ / Raffael Marty – 2008. Pearson Education, Inc. 2009

[4] URL: https://de.wikipedia.org/wiki/Ikonisches_Gedächtnis, 22.06.2015

[5] “Network Security Visualisation Techniques in Early Warning Systems” / Marcus Weseloh 2009. Universität Hamburg 2009

[6] URL: https://www.uni-weimar.de/medien/wiki/images/Gestalttheorie.pdf, 25.06.2015

[7] URL: http://www.informatik.uni-leipzig.de/bsv/homepage/sites/default/files/Infovis-2-Wahrnehmung_1.pdf, 17.05.2015

[8] “Information Visualization: Perception for Design” / Colin Ware- 2013. Elsevier Inc. 2012

[9] “What is Cyber Threat Intelligence and Why Do You Need It?“ iSHIGHT Partners 2014. iSHIGHT Partners 2014

[10] In: *The Guardian* am 31. Juli 2013 *NSA Prism program taps in to user data of Apple, Google and others* / Glenn Greenwald; Ewen MacAskill

[11] URL: https://www.alienvault.com/de 03.02.2015

[12] URL: https://www.alienvault.com/docs/data-sheets/AlienVault-Labs.pdf 05.02.2015

[13] URL: http://www.enisa.europa.eu 28.02.2015

[14] URL: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport 04.03.2015

[15] URL: https://www.fireeye.com/ 10.03.2015

[16] URL: http://www.vanimpe.eu/2015/03/15/getting-started-misp-malware-information-sharing-platform-threat-sharing-part-2/ 10.03.2015

[17] URL: http://threatstop.com/ 12.03.2015

[18] “A Common Language for Computer Security Incidents” / John D. Howard; Thomas A. Longstaff – 1998. Sandia National Laboratories 1998

[19] URL: https://www.dfn-cert.de/leistungen.html 04.04.2015

[20] URL: http://www.vega-deutschland.de 04.04.2015

[21] URL: http://www.carmentis.org/ 12.04.2015

[22] URL: https://www.fireeye.com/ 11.05.2015

[23] URL: https://www.google.com/patents/US20030084318 11.05.2015

Anhang

Versicherung über Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, den _____ _____