HAW HAMBURG

Bachelorarbeit

Kai Uwe Sternke

Client Honeypots: Einsatzmöglichkeiten in Unternehmen und Analyse des Nutzens

Hochschule für Angewandte Wissenschaften Hamburg
Fakultät Technik und Informatik
Department Informatik

Hamburg University of Applied Sciences
Faculty of Computer Science and Engineering
Department Computer Science

Kai Uwe Sternke

Client Honeypots: Einsatzmöglichkeiten in Unternehmen und Analyse des Nutzens

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang Bachelor of Science Wirtschaftsinformatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter: Prof. Dr. Bettina Buth

Eingereicht am: 30. Januar 2021

Kai Uwe Sternke

Thema der Arbeit

Client Honeypots: Einsatzmöglichkeiten in Unternehmen und Analyse des Nutzens

Stichworte

Client Honeypot, Honeyclient, Cybersicherheit, Honeypots im Unternehmen

Kurzzusammenfassung

Während die Nutzung des Internets für Unternehmen unabdingbar geworden ist, birgt dieses eine konstante Bedrohung für deren IT-Systeme. Ein signifikanter Anteil der Bedrohungen geht von Webseiten aus, die gezielt das Verhalten von Anwendern ausnutzen. Client Honeypots haben sich als ein wirksames Werkzeug erwiesen, um solche Webseiten ausfindig zu machen. Sie täuschen vor, ein Nutzer zu sein und können automatisiert Informationen über diese Bedrohungen sammeln. In dieser Arbeit wird analysiert, ob, nach dem derzeitigen Stand der Forschung, die Verwendung von Client Honeypots ein aktives Mittel zur Verteidigung gegen Angreifer darstellen kann. Diese Untersuchung wird anhand eines fiktiven Unternehmens durchgeführt.

Kai Uwe Sternke

Title of Thesis

Client Honeypots: Corporate usages and an analysis of their benefits

Keywords

Client Honeypot, Honeyclient, Cyber Security, Honeypots in businesses

Abstract

While the use of the Internet has become indispensable for businesses, it poses a constant threat to their IT systems. A significant proportion of threats come from websites that target user behavior.

Client honeypots have proven to be an effective tool to detect such websites. They impersonate a user and can collect information about these threats. This thesis analyzes whether, according to the current state of research, the use of client honeypots can be an active mean of defense against attackers. The analysis is based on a fictional company

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Dieser Teil erläutert den allgemeinen Aufbau dieser Arbeit. Zunächst wird die Motivation hinter der Bearbeitung des Themas benannt. Anschließend werden einzelne Kapitel kurz vorgestellt und Strukturentscheidungen begründet.
Für diese Arbeit werden Begriffe aus dem Bereich der IT- und Cybersicherheit hauptsächlich mit ihren Bezeichnern aus dem englischsprachigen Umfeld genutzt, falls für diese keine etablierte deutsche Übersetzung existiert.

1.1 Motivation

Zu Zeiten der Globalisierung wird es für Unternehmen immer wichtiger, das Internet zu nutzen. Eine Vielzahl der Unternehmen in Deutschland ist demnach mit dem Internet verbunden und bildet Prozesse darüber ab. Ungenügend geschützte Systeme stellen ein Risiko für Unternehmen dar und sind ein Ziel von Angreifern.
Diese Systeme können anhand von vorhandenen Schwachstellen durch Schadsoftware infiziert werden. Eine Infektion kann große Schäden für das Unternehmen nach sich tragen. Die Angreifer können durch eine Vielzahl von monetären Zielen motiviert sein, welche sie durch die Übernahme von (Firmen)Computern und die Infektion von Netzwerken versuchen zu erreichen.
So erpressen sie Zahlungen von den Opfern zum Entsperren ihrer Computer, oder werden durch Dritte pro übernommenen Computer bezahlt. Ebenso ist die Spionage von Firmengeheimnissen oder ein Finanz- und Reputationsschaden am Unternehmen ein mögliches Ziel. Auch der in der Hackerszene vorhandene Prestigegewinn für möglichst viele infizierte Opfer kann treibende Kraft sein.[10]
Ein Client Honeypot ist eine Sicherheitsressource, die automatisiert versucht, sich anhand ihrer Schwachstellen ausnutzen zu lassen, um Informationen über diese Schwachstellen zu erhalten. Sie sind ein Mittel von Sicherheitsforschern, um sich beim Wettrüsten gegen Angreifer[18] über deren Methoden zu informieren.[21]

Client Honeypots sind in den letzten 15 Jahren ein wirksames Mittel geworden, um schadhafte Webseiten ausfindig zu machen, welche ein mögliches Angriffsmittel von Angreifern sind. Dabei setzt sich der Client Honeypot aktiv potentiell gefährlichen Inhalten, wie schadhaften Webseiten oder Mails, aus und versucht in einer geschützten Umgebung herauszufinden, ob und wie seine Schwachstellen ausgenutzt werden.
Für Unternehmen ist es also zur Vermeidung von Reputationsschäden, Erpressungsgeldern und sonstigen Schäden wichtig, ihre Systeme vor Angriffen zu schützen. Client Honeypots können dabei unterstützen, indem sie gefahrenlos Inhalte untersuchen, die Schwachstellen ausnutzen könnten.

1.2 Ziele

Das Ziel der Arbeit ist es, eine Einschätzung zu liefern, ob sich die Nutzung von Client Honeypots für Unternehmen lohnt, um ihre IT-Sicherheit zu verbessern.
Dabei wird sowohl die Funktionsweise und das von Client Honeypots verfolgte Ziel definiert. Es wird auf die zurzeit zur Verfügung stehenden Client Honeypots eingegangen.
Für den Rahmen dieser Arbeit werden keine expliziten Implementationen vorgestellt, stattdessen werden Client Honeypots im allgemeinen Kontext der Verteidigung gegen Bedrohungen betrachtet. Anhand von drei Fragestellungen wird an das Thema herangegangen:

- Was ist der Nutzen von Client Honeypots?
- Ist die Nutzung von Client Honeypots zur Verbesserung der IT-Sicherheit in Unternehmen praktikabel?
- Welche Client Honeypots stehen zum Zeitpunkt der Erstellung der Arbeit zur Verfügung?

1.3 Struktur der Arbeit

Die restliche Arbeit hat folgenden Aufbau:
Im zweiten Kapitel wird die angewandte Forschungsmethode beschrieben und begründet. Zudem wird die genutzte Literatur besprochen und mit der ausgewählten Forschungsmethode in Kontext gesetzt.

Das dritte Kapitel befasst sich mit den grundlegenden Begriffen und Definitionen. Relevante Angriffsmethoden und Schutzmittel, wie Honeypots und Client Honeypots, werden dort erläutert.
Im vierten Kapitel wird die genutzte Analysemethode eingeführt und erörtert. Hier wird zunächst ein fiktives Unternehmen beschrieben, auf Basis dessen die Analyse der Anwendungsmethoden von Client Honeypots analysiert werden können.
Das fünfte Kapitel bietet eine Beschreibung der vorgeschlagenen Anwendungsmöglichkeiten für Client Honeypots und analysiert sie anhand der Fragestellungen und dem fiktiven Unternehmen aus Kapitel 4. Hier wird untersucht, ob Unternehmen einen Nutzen aus Client Honeypot Technologien ziehen können und wie sich dies auf Praktikabilität auswirkt.
Die Analyseergebnisse werden im sechsten Kapitel diskutiert. Hier wird auch auf die frei verfügbare Client Honeypot-Software eingegangen.
Das siebte Kapitel zieht ein abschließendes Fazit anhand der Leitfragen. Im Ausblick wird dann ein Konzept vorgeschlagen, Client Honeypot für Unternehmen in der Praxis attraktiver zu gestalten.
Schließlich gibt das achte Kapitel noch einen Überblick über weiterführende Quellen, die für die Forschung im Bereich Client Honeypots von Bedeutung sind. Unter anderem werden vorgeschlagene Messgrößen und die Wirkung von Client Honeypot-Technologie auf andere Forschungsgebiete aufgezeigt .

2 Methodik

Dieses Kapitel befasst sich mit der beim Erstellen dieser Arbeit angewandten Forschungsmethodik. Zunächst wird sie in ihren Grundzügen vorgestellt und im Kontext dieser Arbeit beschrieben. Anschliessend wird begründet, warum diese Methode genutzt wurde.

2.1 Verwendete Methodik

Für diese Arbeit wurde eine Methode der Sekundärforschung, die qualitative Literaturanalyse, gewählt. Auf Basis bestehender literarischer Quellen wird, anhand der Forschungsfragen und der grundlegenden Hypothese, das Themengebiet analysiert. Aus der Wahl des Forschungsgebiets ergeben sich Kernbegriffe, die Basis der Recherche sind.
In dieser Arbeit bilden folgende Begriffe den Kern der Recherche:

- Client Honeypot / Honeyclient
- Honeypot Defense

Die Ergebnisse der Recherche wurden dann schematisch aufgearbeitet und etwaige Folgequellen ausfindig gemacht. Wenn eine Publikation weitere Begriffe eingeführt hat, wurde anhand dieser das jeweilige Themenfeld weiter erarbeitet.

2.2 Begründung

Die grundlegenden Forschungsfragen lassen eine empirische Analyse nur unter hohem Zeit- und Kostenaufwand oder mit Fokus auf einen Teilaspekt des Themas zu. Eine einzelne Bachelorarbeit würde der empirischen Studie aller Anwendungsgebiete aufgrund ihres Umfanges nicht gerecht werden. Jede Anwendungsmöglichkeit selbst ist komplex genug, um eine eigene Arbeit gewährleisten zu können.

Das Ziel dieser Arbeit ist es, einen Überblick über Client Honeypots, im Kontext eines Wirtschaftsunternehmens, zu vermitteln.
Um diesem Überblick gerecht zu werden, konzentriert sich die Arbeit somit nicht nur auf eines der Anwendungsgebiete von Client Honeypots.

2.3 Literatur im Kontext der Methodik

Jede Quelle im Zusammenhang mit zuvor aufgeführten Kernbegriffen wurde zunächst auf das Vorhandensein dieser Begriffe geprüft. Eine Quelle, die nicht den Begriff "Client Honeypot" oder eine seiner Abwandlungen enthält, hat eine geringere Wahrscheinlichkeit relevant zu sein.
Im Verlaufe der Recherche haben sich veröffentlichte Doktor- und Masterarbeiten als wichtige Quellen für grundlegende Zusammenhänge, Zusammenfassungen und Weiterentwicklungen im Themengebiet herausgestellt.
Konferenzpapiere machten in der letztendlich verwendeten Literatur den größten Anteil aus. Sie haben den Vorteil, dass sie oft die aktuellsten Erkenntnisse der Forschung aufzeigen.
Um die Validität der Quellen zu bestätigen, wurde im Rahmen dieser Arbeit zu jeder genutzten Quelle geprüft, ob und in welcher Form andere Forscher auf diese verwiesen haben. Um möglicherweise vorhandene Kontroversen in Erfahrung zu bringen, die das Forschungsergebnis in Frage stellen könnten, fand eine allgemeine Überprüfung der führenden Autoren statt.

3 Grundlagen

Im Verlauf dieses Kapitels werden Kernbegriffe und Konzepte dieser Arbeit definiert. Insbesondere wird auf Client Honeypots und die relevanten Arten von Cyber-Angriffen eingegangen.

3.1 Cyber-Raum

"[Der]Cyber-Raum umfasst [...] sämtliche mit dem globalen Internet verbundene IT und IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen und Intelligenzen."[29] Es handelt sich somit um einen Begriff, der sämtliche Ereignisse, die digital und im Zusammenhang mit global verbundenen IT-Systemen geschehen, einschließt. Er bildet die Grundlage auf der weitere Begriffe aufbauen.

3.2 Cyber-Angriff

In der Cyber-Sicherheitsstrategie für Deutschland aus dem Jahre 2016 definiert die Bundesregierung Cyber-Angriffe als "[...] eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen."[8] Diese Definition fasst somit alle Interaktionen aus dem Cyber-Raum mit den IT-Systemen des Unternehmens zusammen, die zum Ziel haben, das Unternehmen zu stören oder zu schädigen. Solche Interaktionen können über eine Vielzahl von Wegen stattfinden. An dieser Stelle wird nur auf die Interaktions- bzw. Angriffsarten eingegangen, die im weiteren Verlauf dieser Arbeit Relevanz zeigen werden.

3.2.1 Exploit

"Ein Exploit stellt eine systematische Möglichkeit dar, aufgrund von Schwachstellen oder Sicherheitslücken der Software in Computersysteme einzudringen."[22] Exploits können genutzt werden, um Systeme Tätigkeiten verrichten zu lassen, die nicht ursprünglich gewollt oder direkt schadhaft sind. Beispielsweise kann ein Onlineshop Opfer eines Exploits werden, wenn dieser Nutzereingaben im Suchfeld nicht überprüft. Wenn Serverbefehle in die Suchzeile geschrieben werden, besteht die Möglichkeit, dass diese ausgeführt werden.[26]
Sollte ein Angreifer Wissen über die internen Abläufe eines Systems erhalten, etwa durch Kenntnis über den Quellcode, ermöglicht es dem Angreifer einen Exploit gezielt zu nutzen. Kenntnis über Exploits kann auch explorativ durch den Angreifer erlangt werden.

3.2.2 Drive-By-Download

Ein Drive-By-Download Angriff lädt Software auf den Computer des Opfers herunter, die später dann verschiedene Funktionen ausführen kann. Dieser Download wird allerdings nicht vom Opfer willentlich gestartet, sondern wird unter Ausnutzung von Exploits des Browsers, Plugins oder Betriebssystems des Opfers beim Laden von Webseiten im Hintergrund durchgeführt.
Eine weitere Möglichkeit, wie sich Drive-By Downloads propagieren, ist innerhalb von zunächst legitim erscheinenden Dateien, die der Anwender wissentlich herunter lädt, oder als Anhang von E-Mails.[32] So besteht die Möglichkeit, die Funktion von programmierbaren Abläufen in Dateien gängiger Office-Suites(etwa Microsoft Office oder OpenOffice) zu nutzen, um nachträglich schadhafte Schritte einzuleiten, wie etwa das Herunterladen von weiterer Schadsoftware.
Drive-By-Downloads sind eine Angriffsart, die von Client Honeypots detektiert werden können.

3.2.3 Zeitbomben-Angriff

Als Zeitbomben-Angriffe werden Exploits verstanden, die auf einer schadhaften Webseite erst nach Ablauf einer bestimmten Zeitspanne ausgelöst werden. Sie sind ein Mittel, das von Angreifern genutzt wird, um nicht direkt von einem Client Honeypot entdeckt zu werden. Um diesen Angriffen gerecht zu werden, sind Client Honeypots oft im Bereich

von 25 bis 35 Sekunden mit einer möglicherweise schadhaften Webseite beschäftigt.[37] Der Begriff ist zudem ein Homonym mit Schadsoftware, die erst nach dem Ablauf eines Zeitfensters, oder dem Eintreffen einer bestimmten Bedingung, ihre schadhafte Tätigkeit beginnt. Ebenso tragen absichtlich in legitime Software hinein programmierte, schadhafte Mechanismen den Begriff Zeitbomben-Angriff, wenn sie zeit- oder ereignisgesteuert fungieren.
In dieser Arbeit wird der Begriff jedoch lediglich für die erstgenannte Definition verwendet.
Ein Zeitbomben-Angriff ist eine Angriffsmethode, die effektiv gegen Client Honeypots eingesetzt werden kann.[36] Er kann einen Client Honeypot zu einer falschen Klassifikation bewegen, da ein Client Honeypot nur für eine bestimmte Zeit Ressourcen aufwendet, um das Angriffsmittel zu überprüfen. Sie spielen somit auf eine bekannte Schwäche der Client Honeypots an.

3.2.4 Zero-Day-Angriff

Als Zero-Day-Angriff werden Angriffe bezeichnet, die Exploits in Systemen ausnutzen, die noch nicht allgemein bekannt sind.[6] Angreifer handeln ganze Listen von noch nicht veröffentlichten Exploits untereinander. Diese werden nur nach und nach ausgenutzt, um möglichst lange profitabel zu bleiben. Somit besteht für Angreifer gegenüber den Herstellern und Sicherern von Systemen häufig ein gewisser Vorteil.[13]
Client Honeypots haben sich als ein Werkzeug etabliert, welches es ermöglicht, diese Angriffe bei ihrem ersten Auftreten zu identifizieren.

3.2.5 Aktive Ausspähung

Aktive Ausspähung ist eine Taktik, die ein Angreifer anwenden kann, um Schwächen, Ressourcen oder das größte Schadenspotential in Zielen zu entdecken. Ein Angreifer kann durch gezielte Anfragen die Netzwerk- oder auch die Hardwareadressen von Zielen in Erfahrung bringen. Ebenso können mit einem Portscan die offenen Ports und angebotenen Services untersucht werden. Zudem ist es möglich, die benutzten Versionen von Betriebssystemen und Anwendungen herauszufinden.[39] An dieser Stelle wird jedoch nicht weiter auf die verschiedenen Ausspähungstechniken eingegangen.
Aktive Ausspähung hat den Nachteil für den Angreifer, dass seine Aktivitäten vom Ziel

bemerkt werden können. Für eine hohe Informationsdichte opfert der Angreifer also potentiell seine Deckung und gibt dem Ziel die Möglichkeit, seine Absichten zu erkennen und sich zu schützen. Die aktive Ausspähung lässt sich durch herkömmliche Honeypots erkennen.[31] Das Gegenstück zu aktiven Ausspähung ist die passive Ausspähung.

3.2.6 Passive Ausspähung

Im Gegensatz zur aktiven Ausspähung, birgt die passive Ausspähung ein geringes Risiko für den Angreifer entdeckt zu werden. Netzwerkkommunikation kann abgehört werden, wenn es dem Angreifer gelingt, sich innerhalb des Netzwerks zu platzieren. Er kann aber auch versuchen Datenmüll oder informationshaltige Abfälle, wie unsachgemäß entsorgte Ausdrucke oder Endgeräte, auszuwerten. Diese Techniken können dem Angreifer Informationen über die interne Abläufe des Ziels geben. Im Verlaufe der Arbeit wird eine Möglichkeit genannt, wie eine bestimmte Art der passiven Ausspähung durch Client Honeypots entdeckt werden kann.

3.2.7 Phishing und Spear-Phishing

Phishing ist einer Art des Cyber-Angriffs, bei dem Personen über verschiedene Medien, etwa telefonisch, per Post oder per E-Mail, kontaktiert werden. Ihnen wird vorgetäuscht, dass es sich um einen legitimen Anbieter handelt, wie etwa eine Bank, eine Abteilung in der Firma oder eine Behörde. Der Zweck des Phishings ist es, dass das Ziel sensible Informationen, wie Passwörter oder Kreditkartendaten preis gibt. Phishing ist in der Regel eine breit gestreute Angriffsart, in der möglichst viele Personen kontaktiert werden, in der Hoffnung, dass der Angriff bei einem geringen Anteil gelingt.[19] Phishing ist manipulativ lässt sich unter Social Engineering kategorisieren, der Manipulation von Menschen zugunsten eine bestimmten Zweckes.
Spear-Phishing ist eine Form des Phishings, in der gezielt eine Person oder Personengruppe unter Zunahme von Kontextinformationen dazu gebracht wird, Schadsoftware herunter zu laden, Daten preiszugeben oder böswillige Webseiten zu besuchen.
Daten über das Ziel können über Monate hinweg, durch aktive und passive Ausspähung, gesammelt werden.
Der Angreifer kann beispielsweise versuchen E-Mails zu fälschen, die für den Nutzer legitim erscheinen. Der Nutzer soll diese Mail öffnen und mit deren Inhalten, wie etwa Links oder Anhängen, interagieren. Der Zeitaufwand für den Angreifer und die personalisierte

Art dieses Angriffs hebt Spear-Phishing vom regulären Phishing ab. [48]
Client Honeypots, die E-Mails überprüfen können, sind ein Mittel, um Anwender vor (Spear-) Phishing Angriffen zu schützen.

3.3 Blacklist

Eine Blacklist ist im Kontext dieser Arbeit eine Liste von IP-Adressen und URLs, die als bereits schadhaft erkannt wurden. In der Regel wird ein Verbindungsversuch zu einem Ziel, das sich auf einer Blacklist befindet, aus Sicherheitsgründen abgebrochen. Blacklisting ist ein effizienter Ansatz, um bereits als gefährlich bekannt gewordene Webseiten und IP-Adressen zu sammeln und mit anderen zu teilen.[2] Es gibt frei verfügbare geteilte Blacklists, welche von Organisationen veröffentlicht werden. Solche Organisationen werden im weiteren Verlauf Reputationsanbieter genannt.
Als Alternative zum Blacklisting, steht das Whitelisting. Während Blacklisting alle Verbindungen zulässt, die nicht auf der Blacklist stehen, lässt Whitelisting nur Verbindungen zu, die sich auf der Whitelist befinden. Whitelisting reduziert die potentielle Angriffsfläche mehr als Blacklisting. Derzeit gibt es noch keine Forschungsergebnisse, die Client Honeypots explizit mit der Erstellung oder Wartung von Whitelists in Zusammenhang bringen.

Client Honeypots können jedoch genutzt werden, um Blacklists zu verifizieren und zu erweitern.[44]

3.4 Honeypot

Honeypots sind passive Systeme, deren Ziel es ist, angegriffen zu werden und Informationen über das Angriffsverhalten zu erlangen. Sie können viele Formen annehmen, wie etwa Server, Services, Fake-Produktionssysteme usw. Gemein haben sie allerdings, dass sie keine wichtigen Aufgaben übernehmen oder Services anbieten, sondern als Sicherheitswerkzeug dienen. Eine potenzielle Kompromittierung des Honeypots ist ein zu erwartendes Ereignis.
Der Honeypot verfügt über Aufzeichnungsmechanismen, anhand derer versucht wird, Angriffsmuster und Ziele des Angreifers zu identifizieren.
Honeypots leiden derzeit am Fehlen einer eindeutigen Definition. So ist es unter anderem

schwer, sie von einer Firewall mit Fokus auf Aufzeichnung, oder einem, sich im Netzwerk befindenden Log-Servers, abzugrenzen.
Weitläufig wird die Definition von Lance Spitzner[41] genutzt. Thomas Schwenkler übersetzt sie aus dem Englischen folgendermaßen: „Ein Honeypot ist ein Informationssystem, dessen Wert in der unbefugten oder rechtswidrigen Benutzung dieser Ressource liegt.“[33] Da ein Honeypot keine Services anbietet oder an wertschöpfenden Prozessen beteiligt ist, kann jeder Verbindungsversuch oder Interaktion mit dem Honeypot generell als eine schadhafte Intention betrachtet werden. Honeypots unterscheiden sich untereinander in ihrer Implementation, werden aber in der Literatur überwiegend anhand ihres Interaktionslevels in drei Klassen eingeteilt: Low Interaction Honeypots, Medium Interaction Honeypots und High Interaction Honeypots.

3.4.1 Low Interaction Honeypot

Low Interaction Honeypots bieten nur eine geringe Anzahl von Schnittstellen an. Ihre Services, also die von Ihnen angebotenen Dienste, sind nicht vollständig implementiert, sondern in der Regel nur emuliert. So wird möglicherweise nur auf bestimmte Anfragen geantwortet, oder es werden nur eine geringe Anzahl von statischen Antworten verschickt. Selbiges trifft auf das Betriebssystem des Low Interaction Honeypots zu.
Resultierend aus dem geringen Implementierungsgrad, kann ein Low Interaction Honeypot nicht als Ausgangspunkt für weiterführende Angriffe genutzt werden.[9] Sie sind relativ simpel in ihrer Implementierung und Wartung, können aber den Angreifer nicht lange beschäftigen. Falls ein Angreifer nicht implementierte Services oder Befehle abfragt, kann sich dieser schnell erschließen, dass es sich um einen Honeypot handelt.[5]
Zwar kann der Low Interaction Honeypot den Angreifer nur kurz täuschen, die Interaktion mit dem Honeypot an sich ist allerdings bereits ein starkes Indiz für einen Angriff. Der Verteidiger erhält somit die Möglichkeit, darauf zu reagieren.

3.4.2 Medium Interaction Honeypot

Ähnlich wie die Low Interaction Honeypots, haben die Medium Interaction Honeypots nicht alle Services und das Betriebssystem implementiert. Damit sie jedoch nicht so schnell vom Angreifer als Honeypot identifiziert werden können, sind einige Services mehr implementiert, als in der Low Interaction Honeypot Variante.
Während ein Angreifer, je nach Implementierungsgrad, länger für die Identifikation des

Honeypots benötigt, steigt damit auch direkt der Aufwand für den Nutzer des Honeypots. Ebenso erhöht sich das Risiko, dass der Honeypot übernommen wird.[5]

3.4.3 High Interaction Honeypot

Im Gegensatz zu den Low Interaction und Medium Interaction Honeypots, sind High Interaction Honeypots in einer viel größeren Tiefe implementiert. Sie verfügen über ein reales Betriebssytem und implementierte Services.[5] Sie bieten dem Angreifer ein großes Interaktionsspektrum und sind mit dem Ziel aufgesetzt, diesen möglichst lange zu beschäftigen. Ihre Erkennbarkeit ist durch die komplette Implementierung für den Angreifer gering.
Der Honeypot kann jedoch unter Umständen durch den Angreifer übernommen werden. Hierdurch wäre der Honeypot dann ein Werkzeug für den Angreifer, um weitere Angriffe in das Netzwerk hinein zu starten. High Interaction Honeypots sind somit mit einem höheren Risiko verbunden, als ihre Low und Medium Interaction-Varianten. Es können jedoch deutlich mehr Daten über die vom Angreifer verwendeten Methoden gesammelt werden. Dem Verteidiger wird zudem mehr Zeit gegeben, sich zu schützen.[9]
Ein High Interaction Honeypot ist mit hohen Aufwänden für Implementierung, Wartung und Administration verbunden.[5]

3.5 Client Honeypot

Reguläre Honeypots haben sich als Verteidigungswerkzeug bewährt. Jedoch sind sie insoweit limitiert, dass sie auf einen Angreifer warten müssen. Angriffe werden aber auch auf anderen Wegen durchgeführt. Ein Nutzer, der sich beispielsweise im Internet bewegt und eine Webseite öffnet, bietet Angriffsfläche für Angreifer.
Ein regulärer Honeypot hat konzeptuell keine Möglichkeit auf Angriffe zu reagieren, die auf ein Ziel außerhalb des Netzwerkes gerichtet sind. Aus diesem Grund wurde der Client Honeypot als aktives Ködersystem vorgeschlagen. Der Begriff wird synonym mit "Honeyclient" oder auch "aktiver Honeypot" verwendet. In dieser Arbeit wird sich auf Client Honeypot festgelegt. Kathy Wang hat in 2004 das erste Client Honeypot-Tool öffentlich zugänglich gemacht.[49]
Client Honeypots sind in erster Linie ein Werkzeug, das dabei hilft, potentiell gefährliche

Server zu identifizieren. Dies kann Webseiten betreffen, aber auch Instant Messaging-Dienste oder den Inhalt von E-Mails. Mit Client Honeypots können Proben von Schadsoftware gesichert werden, die später von Experten analysiert werden können.
Der Unterschied von Client Honeypots zu regulären Honeypots ist, dass der Client Honeypot aktiv versucht angegriffen zu werden, statt passiv darauf zu warten. Potentiell gefährliche Webseiten werden aufgerufen und Links werden gefolgt, Spam- und Phishingmails werden geöffnet und Anhänge heruntergeladen. So wird versucht Schwachstellen zu erkennen, die von Angreifern ausgenutzt werden, um diese dann zu schließen.
In der Praxis werden Client Honeypots in erster Linie für die Überprüfung von HTTP-Verbindungen genutzt. Es ist aber anzumerken, dass sich das Konzept des Client Honeypots auf jedes Client-Server basierende Protokoll anwenden lässt.[49]

3.5.1 Vorgehensweise von Client Honeypots

Jede Art von Client Honeypot lässt sich in drei distinkte Komponenten unterteilen. Seifert et al. identifizieren hier zum einen die Visitor-Komponente, welche mit dem potentiell gefährlichen Inhalten interagiert. Hinzu kommt eine Warteschlangen-Komponente(auch Queuer genannt), die aus einer Liste von Inhalten den nächsten zu untersuchenden auswählt. Die letzte Komponente ist die Analysis-Engine, welche entscheidet, ob es sich um einen gefährlichen Inhalt handelt.[36]
Die Warteschlangen-Komponente kann eine Liste von URLs verwalten, oder auf auf einem Mailserver hinterlegte Mails zeigen. Beispielsweise kann ein Webcrawler als Warteschlangen-Komponente für einen Client Honeypot agieren.
Damit die Analysis-Engine einschätzen kann, ob der untersuchte Inhalt eine böswillige Aktion ausgeführt hat, sind definierte Sicherheitsrichtlinien erforderlich. Anhand dieser können unbefugte Aktionen, wie etwa das Abspeichern oder Verändern von Dateien in unüblichen Verzeichnissen und Veränderungen an unbeteiligten Prozessen, entdeckt werden.
Über die Visitor-Komponente kann gesteuert werden, welcher Untersuchungsalgorithmus für die Untersuchung ausgewählt wird, wie schnell die Interaktionsgeschwindigkeiten sind oder wie lange eine Untersuchung dauert. Die Implementierung der Visitor-Komponente legt fest, wie das Interaktionslevel des Client Honeypots definiert ist. Ähnlich wie die regulären Honeypots, lassen sich auch Client Honeypots anhand ihres Interaktionslevels untergliedern.

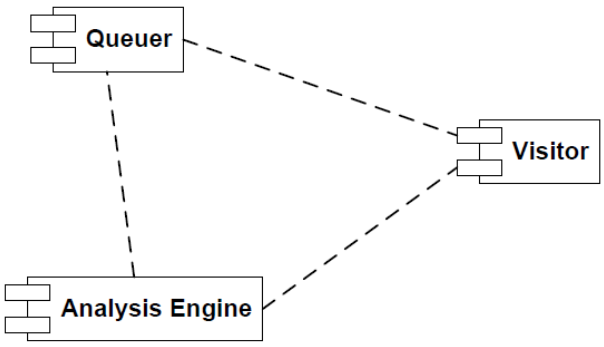

Abbildung 3.1: Darstellung der Client Honeypot-Komponenten [36]

3.5.2 High Interaction Client Honeypot

High Interaction Client Honeypots sind, historisch betrachtet, die erste Variante von Client Honeypots. Sie emulieren Browser oder Betriebssysteme, die eine Verbindung, meist zu einer Webseite, herstellen. Durch ihre hohe Interaktionsfähigkeit sind sie in der Lage, das Verhalten von echten Nutzern nachzustellen. So können Schaltflächen betätigt oder Links verfolgt werden.
Ihre Analysis-Engine ist darauf ausgelegt, die Erstellung oder Manipulation von Daten und Dateien zu beobachten, wo das beobachtete Programm (Browser, E-Maildienst) in der Regel keine Änderungen vornimmt. So wird von einem Browser zwar erwartet, dass eventuelle Cookies auf dem Gerät des Nutzers gespeichert werden, nicht jedoch Datenobjekte im Bereich des Betriebssystems oder dem Registry-Verzeichnisses. In solchen Fällen erstellt der Honeypot einen Report, bevor er sich dann selbstständig auf seinen zuvor festgelegten Stand zurücksetzt. Auf diese Art und Weise können neben bekannten Exploits auch Zero-Day-Angriffe registriert werden.
Durch ihre Eigenschaft, das gesamte System zu überwachen, sind High Interaction Client Honeypots sehr genau. Ihre Falsch-positiv-Rate liegt bei fast 0, d.h., dass die Wahrscheinlichkeit sehr gering ist, dass sie fälschlicherweise das normale Vorgehen einer seriösen Webseite als schadhaft einstufen.

3.5.3 Low Interaction Client Honeypot

High Interaction Client Honeypots müssen nach Erkennung eines Angriffs auf einen früheren Stand zurückgesetzt werden, um Sicherheitsrisiken zu vermeiden und Analyseergebnisse nicht zu verfälschen. Dieser Vorgang nimmt Zeit in Anspruch und muss auch bei bereits bekannten Angriffen vorgenommen werden. Hierdurch sind High Interaction Client Honeypots inherent langsam.
Seifert et al. haben deshalb in 2006 den Low Interaction Client Honeypot vorgeschlagen.[34] Um eine höhere Geschwindigkeit zu erreichen, wird auf die Überwachung des Betriebssystems und des Dateisystems verzichtet. Mittelpunkt der Analyse sind die Antwort des jeweiligen Servers und vor allem die mit der Webseite versandten Dateien wie Javascript oder Flash-Skripte. Low Interaction Client Honeypots arbeiten mit Heuristiken und Pattern-Matching-Methoden, um eine gefährliche Seite anhand ihres Verhaltens und des Codes innerhalb der übersandten Dateien zu erkennen. Die Webseite selbst wird in der Regel nicht gerendert, stattdessen wird der Datenfluss der Anfrage analysiert.
Hierdurch sind sie deutlich schneller als High Interaction Client Honeypots. Sie weisen jedoch die Schwäche auf, Zero-Day-Angriffe nicht erkennen zu können. Zudem ist ihre Falsch-positiv-Rate höher, da auch seriöse Webseiten Muster aufweisen können, die dem von unseriösen Webseiten gleichen. Ebenso können sie nicht alle der potentiellen Angriffe analysieren, was aus dem Fehlen der nötigen Interaktion und der Ausführung von Dateien folgt. Es ist demnach auch eine Falsch-negativ-Rate aufzuführen, die höher ist, als die des High Interaction Client Honeypots.

3.5.4 Hybrider Client Honeypot

Um den Schwachstellen der Low Interaction Client Honeypots entgegen zu wirken, haben Seifert et al.[36] einen hybriden Client Honeypot vorgeschlagen. In diesem wird ein Low Interaction Client Honeypot benutzt, um URLs zu überprüfen. Nach der Analyse des Low Interaction Client Honeypot werden alle als potentiell gefährlich eingestuften Ergebnisse erneut von einem High Interaction Client Honeypot überprüft. Abbildung 3.2 visualisiert dieses Zusammenspiel der zwei Client Honeypots.
Durch die Kombination der zwei Honeypots, wird die Menge der zu überprüfenden Webseiten für den High Interaction Client Honeypot reduziert. Abhängig von der Anzahl der durch den Low Interaction Client Honeypot identifizierten böswilligen Webseiten, kann der High Interaction Client Honeypot auf einer handhabbaren Geschwindigkeit arbeiten.

Wenn jedoch der zugrundeliegende Anteil von böswilligen Webseiten hoch ist, muss noch immer ein signifikanter Anteil der Ergebnisse durch den langsameren High Interaction Client Honeypot untersucht werden. In dieser Situation erzielt der hybride Client Honeypot keine Geschwindigkeitsverbesserung.

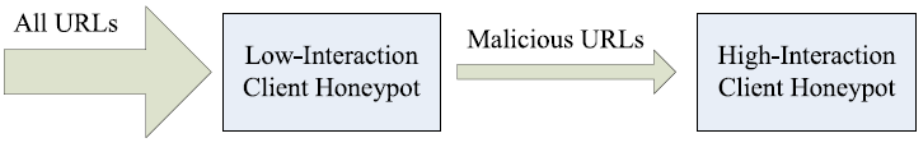

Abbildung 3.2: Vereinfachter Aufbau eines Hybriden Client Honeypot-Systems [36]

3.6 Schwächen von Client Honeypots

Client Honeypots, insbesondere High Interaction Client Honeypots, haben eine sehr geringe Falsch-positiv-Rate. Diese Analyse nimmt allerdings erhebliche Zeit in Anspruch. Sie kann im Bereich von mehreren Minuten pro untersuchter URL liegen.
Es müssen mehrere Client Honeypots parrallel laufen, um einen Bruchteil des bekannten Internets überprüfen zu können. Dies wird anhand eines Beispiels verdeutlicht: Es wird angenommen, dass ein Client Honeypot eine Webseite in 2 Minuten überprüft und fünf virtuelle Maschinen gleichzeitig auf dem Gerät laufen. Das Ziel ist es, 10% aller Webseiten im Internet wenigstens ein mal zu überprüfen. Nach [15] existieren zum Zeitpunkt der Erstellung dieser Arbeit 1,8 Milliarden Webseiten im Internet, 10% davon sind 180 Millionen. Um diese 180 Millionen Webseiten in einer Woche zu überprüfen, müssten 17 Client Honeypots mit der angenommenen Konfiguration dauerhaft laufen.
Zudem kann jeder Client Honeypot nur eine bestimmte Konfiguration überprüfen. Eine auf Windows 7 SP 1 eingestellte böswillige Webseite wird in der Regel keinen Client Honeypot angreifen, der mit Windows 7 SP 2 konfiguriert ist, da der abgezielte Exploit möglicherweise dort bereits behoben ist. Daraus ergibt sich, dass ein Client Honeypot immer nur eine Stichprobe nehmen kann. Auch der Standort des Honeypots kann das Ergebnis beeinflussen.
Nach Yen et al.[52] werden für bestimmte Angriffsarten oft nur bestimmte Länder und

Regionen anvisiert. Ein Client Honeypot, der sich anhand der IP-Adresse nicht in diesem Zielgebiet befindet, wird auch nicht als Ziel ausgewählt. Deshalb sollte dies in der Nutzung von Client Honeypots bedacht werden. Über Proxy-Server kann gegebenenfalls die Lokation des Client Honeypots nach außen hin angepasst werden.
Eine Webseite wird kein schädliches Verhalten zeigen, wenn sich das Ziel nicht innerhalb der gewünschten Lokation befindet oder die falsche Systemkonfiguration aufweist.
Ein einzelner Client Honeypot genügt somit nur für eine Analyse einer einzelnen Systemkonfiguration an einer bestimmten Lokation. Das vorangegangene Beispiel würde demnach nur einen Bruchteil der Schadsoftware ausfindig machen, wenn dessen Verteiler Systemkonfiguration und Lokation beachten.
Nicht jeder Angriffsversuch überprüft diese Parameter. Jedoch kann die Aussage getroffen werden, dass ein vielfaches des berechneten Aufwandes benötigt werden würde, um Lokations- und Konfigurationsgerecht mit Client Honeypots das Internet zu durchsuchen. Der Faktor beträgt L * K, wobei L die Anzahl der zur Untersuchung ausgewählten Lokationen (IP-Adressen, Länder) und K die Anzahl der verschiedenen Systemkonfigurationen repräsentiert.
Desweiteren lassen sich Client Honeypots von dem Verteiler der Schadsoftware erkennen. So wird unter anderem überprüft, ob sich bestimmte Dateien auf dem Betriebssystem befinden, die auf eine virtuelle Maschine hindeuten könnten.
Ebenso kann der Exploit durch eine Interaktion mit der Benutzeroberfläche der Webseite ausgelöst werden. Die Visitor-Komponente des Client Honeypots kann zwar die Interaktion mit Schaltflächen emulieren, es scheitert in der Regel aber an semantisch passenden Eingaben, die ein Mensch möglicherweise machen würde. Auch das Verhalten eines Client Honeypots ähnelt nicht immer dem eines Menschen. Falls der Client Honeypot innerhalb einiger Millisekunden dutzende Links auf der Seite überprüft, kann das für den Betreiber der Seite ein Hinweis darauf sein, dass es sich um einen Client Honeypot handelt.
Angreifern steht eine Vielzahl von Möglichkeiten zur Verfügung, Client Honeypots zu entgehen. Client Honeypots können nur begrenzt viele Angriffsziele nachbilden. Um mehrere Angriffsziele darstellen zu können, sind mehrere Client Honeypots notwendig. Sie sind somit ein Werkzeug, das für eine flächendeckende Analyse einen sehr hohen Aufwand generiert.

4 Analysemethode

Im Folgenden wird die Methode vorgestellt, anhand derer die Anwendungsmöglichkeiten der Client Honeypots für Wirtschaftsunternehmen untersucht werden. Hierzu wird sich zunächst auf eine Art von Unternehmen festgelegt und dieses anhand von bestehenden statistischen Daten modelliert.

4.1 Analyse anhand eines fiktiven Unternehmens

Zum Zeitpunkt der Erstellung dieser Arbeit ist noch keine offizielle, frei verfügbare Fallstudie publiziert, die Client Honeypots in einem Unternehmen einsetzt. Somit ist es nicht möglich, sich auf echte Erfahrungen zu stützen. Dieser Ansatz ist demnach lediglich eine Annäherung und dient der Eingrenzung und Veranschaulichung der Anwendungsmöglichkeiten von Client Honeypots.
Es wird dennoch versucht, sich in der Modellierung des Unternehmens an realitätsnahen Werten und Aufstellungen zu orientieren. Hierzu wurden Daten des Statistischen Bundesamtes[42] und Internetquellen[46][51] herangezogen.

4.2 Beschreibung des fiktiven Unternehmens

Der Einfachheit halber wird sich das Unternehmen in Deutschland befinden und nur dort Kapital, Mitarbeiter, Kunden und weitere Vermögenswerte besitzen. Es wird angenommen, dass es sich um ein Beratungsunternehmen handelt, dessen Fokus nicht die IT-Sicherheit ist.
Laut Statistischem Bundesamt[42] sind mehr als 99% aller Firmen in Deutschland mit Computern ausgestattet und auch mit dem Internet verbunden. Das fiktive Unternehmen wird somit auch über Computer und einen Internetanschluss verfügen.

Kennzahl	**Wert**
Anzahl Mitarbeiter	200
Mitarbeiter mit Internetzugriff	200
Obergrenze gleichzeitig arbeitender Mitarbeiter	150
Über VPN arbeitende Mitarbeiter	bis zu 50
Größe der IT-Abteilung	10

Tabelle 4.1: Das fiktive Unternehmen in Zahlen

Während zwar nur etwas mehr als 1% aller Unternehmen mehr als 50 Mitarbeiter beschäftigen, wird in diesem Fall ein Unternehmen mit etwa 200 Mitarbeitern gewählt, da Unternehmen in diesem Größenbereich im Regelfall eine kompliziertere IT-Infrastruktur aufweisen, als Klein- und Kleinstunternehmen.
Zudem wird davon ausgegangen, dass jeder Mitarbeiter über freien Zugriff auf das Internet an seiner Arbeitsstation verfügt. Es existieren mehrere Wireless-Lan-Zugriffspunkte. Diese sind auch für Gäste nutzbar.
Zu Stoßzeiten arbeiten bis zu 150 Mitarbeiter zugleich, davon etwa 30% über einen VPN Tunnel von einem mobilen Arbeitsplatz aus.
Dieses Unternehmen betreibt eine eigene IT-Abteilung und hostet ihre Services und administriert einen Teil der IT-Sicherheit selbstständig. Letzterer Aspekt wurde gewählt, da ein Unternehmen dieser Größe ihre IT-Sicherheit auf einen Rechenzentrum-Anbieter auslagern kann, wenn die komplette Verwaltung der Sicherheit ein zu hohes Risiko für das Unternehmen bergen könnte.
Sollte das Unternehmen die IT-Sicherheit komplett auslagern, wäre die übergeordnete Fragestellung möglicherweise nicht länger relevant, da anzunehmen ist, dass ein großer Reputationsanbieter bereits Client Honeypots einsetzt, oder die Nutzung von Client Honeypots für das Unternehmen vertraglich untersagt sein könnte.
Ferner gab es keine öffentliche Quelle, die einen verlässlichen Anteil von IT-Mitarbeitern pro regulärem Mitarbeiter darstellt.
Für diese Arbeit wird davon ausgegangen, dass die IT-Abteilung mit 10 Mitarbeitern besetzt ist. Diese sind hauptsächlich in den Bereichen Helpdesk(Support) und Administration tätig. Während die IT-Abteilung einige unterschiedliche Systeme nutzt, sind die Endgeräte der Abteilungen einheitlich gestaltet. Sie unterscheiden sich lediglich in den Zugriffsrechten der Mitarbeiter.
Die IT-Abteilung kümmert sich darum, dass alle Systeme regelmäßig die aktuellen Updates und Patches erhalten.
Die hier beschriebene Mitarbeiteraufteilung ist in Tabelle 4.1 zusammengefasst.

4.3 Bewertung der Analysemethode

Anhand eines Beispielunternehmens wird die Analyse innerhalb dieser Arbeit veranschaulicht. Es ist unpraktikabel, alle möglichen Unternehmensgrößen, -strukturen und Branchen abzudecken. Ebenso unterscheiden sich Unternehmen über Branchen- und Ländergrenzen hinweg sehr in ihrem Aufbau. Es wird von der Betrachtung des Unternehmens als IT-Sicherheitsanbieter Abstand genommen. Dadurch können Client Honeypots im Kontext eines Unternehmens betrachtet werden, das seine Sicherheit durch neue Technologien verbessern möchte.
Es ist jedoch nicht von der Hand zu weisen, dass diese Analysemethode große Lücken aufweist. Die Analyse begrenzt sich auf ein Mittelstandsunternehmen und aufbauend darauf wird eine Aussage über den Nutzen der Anwendungsmöglichkeit des Client Honeypots getroffen. Für ein multinationales Unternehmen würde, aufgrund der vorhandenen IT-Expertise, ein anderes Analyseergebnis vorliegen.
Diese Analysemethode ist ein erster Schritt, um die Analyseergebnisse mit späteren Auswertungen vergleichen zu können. Es werden Hypothesen über Praktikabilität und Nutzen aufgestellt, die in Folgearbeiten empirisch überprüft werden können.

5 Einsatzmöglichkeiten von Client Honeypots und Analyse

In den folgenden Kapiteln werden die Einsatzmöglichkeiten von Client Honeypots zum aktuellen Stand der Technik erläutert. Zunächst werden die einzelnen Methoden vorgestellt. Anschließend findet eine Evaluation statt, die sich auf das in Kapitel 4 eingeführte fiktive Unternehmens stützt.
Ähnliche Ansätze werden in den einzelnen Kapiteln zusammengetragen. Ihre größte Stärke spielen Client Honeypots im Identifizieren von Drive-By-Downloads aus, welches eines der Hauptbestandteile der Forschung ist.

5.1 Einsatzmöglichkeiten von Client Honeypots

Die folgenden Kapitel beschreiben verschiedene Einsatzmöglichkeiten von Client Honeypots. Eine Evaluierung der jeweiligen Einsatzmöglichkeit findet im zweiten Teil des vorstellenden Kapitels statt.
Dort werden jeweils die aufgeführten Anwendungsmöglichkeiten, im Kontext des in Kapitel 4.2 vorgestellten Unternehmens, diskutiert. Fokus wird an dieser Stelle der Nutzen sein, den das Unternehmen aus einer Implementation und Einführung eines Client Honeypots, einzig und allein zu der jeweiligen Anwendungsmöglichkeit, ziehen kann.
Anschließend wird im Einzelnen eine Einschätzung gegeben, ob das Unternehmen in Anbetracht von Aufwand und Nutzen eine Einführung in Betracht ziehen sollte. Hierfür werden Praktikabilität und Nutzen als primäre Bewertungskriterien herangezogen.
Praktikabilität ist eine vereinfachte Darstellungsform des Aufwandes, die die jeweilige Einsatzmöglichkeit dem Unternehmen bereitet. Faktoren sind für das Unternehmen anfallende Wartungsaufwände, Anschaffungskosten und insbesondere die durch das Unternehmen durchzuführende Forschung.

Nutzen: / **Praktikabilität:**	viel	wenig	keiner
niedrig			
mittel			
hoch			

Tabelle 5.1: Bewertungstabelle der Einsatzmöglichkeiten

Diese Metrik wird anhand bestehender Informationen als niedrig, mittel und hoch bewertet. "Hoch" bedeutet, dass eine Verwendung der Einsatzmöglichkeit sehr praktikabel, also mit relativ geringen Aufwänden verbunden ist.
Nutzen beschreibt, in welchem Maße das Unternehmen, durch die Verwendung eines Client Honeypots, seine Sicherheit erhöhen kann. Faktoren sind hier primär die Reduzierung des Risikos erfolgreicher Angriffe und die Minderung der Angriffsfläche.
Mögliche Werte für Nutzen sind viel, wenig und keiner. Wobei "keiner" bedeuten würde, dass Risiken entweder gar nicht reduziert werden, oder bereits durch andere Sicherheitsmaßnahmen genügend gemindert werden können.
Die Bewertung wird am Ende jeder Evaluation zu Visualisierungszwecken in einer Tabelle eingetragen. Das Tabellenformat ist der Tabelle 5.1 zu entnehmen.

5.1.1 Blacklisting von gefährlichen Webseiten und IP-Adressen

Client Honeypots werden zur Erzeugung von Blacklists eingesetzt, um automatisiert und in einer sicheren Umgebung Webseiten anzufragen. Da Client Honeypots allen Links auf einer Webseite folgen können und eine gefährliche Webseite häufig auf eine weitere führt[2], ist es mit Hilfe von Blacklists und Honeypots möglich, weitere bösartige Webseiten zu entdecken.
Anhand einer sogenannten Seed-Liste, einer Ursprungsliste von zu besuchenden Webseiten, werden über Verlinkungen weitere Seiten besucht. Wenn eine von ihnen ein gefährliches Verhalten aufweist, wird sie in die Blacklist aufgenommen.
Die so erstellten Blacklists dienen dem Schutz von Internetnutzern. Sie können in Browser integriert werden, oder im Internet einem weiten Spektrum an Nutzern zur Verfügung gestellt werden.

Evaluation Client Honeypots werden erfolgreich eingesetzt, um Blacklists zu erstellen und aktuell zu halten. Aufgrund der kurzen Lebensdauer von bösartigen Webseiten, sind

diese Seiten oft gar nicht mehr erreichbar, wenn die Blacklist weitergeleitet wird.[47] Zudem können ursprünglich legitime Webseiten, die infiziert wurden oder eine auf einem bösartigen Server gehostete Werbung anzeigten, auf einer solchen Blacklist eingetragen sein. Dies hätte zum Nachteil, dass sie auch nach einer Bereinigung durch den Betreiber oftmals auf dieser Liste stehen. Somit müssten Seiten regelmäßig überprüft werden, um Falsch-positiv-Ergebnisse zu minimieren. Dies erhöht den Aufwand.
Der Administrator der Client Honeypots hat die Möglichkeit, diesen auf die in seinem Unternehmen vorkommenden Systemkonfigurationen, wie Betriebssystemversion, Browser-Plug-Ins oder installierte Software einzustellen, um so nur für sein Unternehmen relevante Treffer zu erhalten.
Die Nutzung von Blacklists ist zudem überaus einfach zu implementieren und bereits ein Standard von IT-Dienstleistern, die auch Sicherheitspakete anbieten. Es ist jedoch davon auszugehen, dass ein Unternehmen in der Größe wie das in Kapitel 4 beschriebene, die IT-Sicherheit nicht komplett selbst übernimmt, sondern Dienstleister beauftragt. Dadurch ist es möglich, dass dieser Blacklist bereits verwendet.
Somit würde das Unternehmen die Arbeit, für die es bereits zahlt, selbstständig erneut durchführen. Da ein Client Honeypot für das Überprüfen einer Seite zwischen 5 und 300 Sekunden[1] benötigt, kann eine repräsentative Blacklist nur mit mehreren Client Honeypots in Tandem generiert werden.
Dem untersuchten Unternehmen kommt zugute, dass die Regionalität ignoriert werden kann, da sich alle Geräte in Deutschland befinden. Zudem sind die Endgeräte homogen konfiguriert, wodurch nur eine Konfigurationsvariante überprüft werden müsste. Dennoch würde signifikanter Aufwand für die Bereitstellung, Wartung und Nutzung von Client Honeypots für die Blacklisterstellung anfallen.
Der Client Honeypot stellt bei falscher Konfiguration ein gewisses Sicherheitsrisiko dar, da von ihm aus weitere Angriffe auf das Firmennetzwerk gestartet werden können. Möglicherweise entsteht doppelter Aufwand, da bereits Blacklists durch den Sicherheitsanbieter bereitgestellt werden.
Für das Unternehmen stellt sich somit ein geringer Nutzen dar, der mit erheblichen Aufwänden verbunden ist.
Blacklisting wird somit mit niedriger Praktikabilität und keinem Nutzen bewertet.

Nutzen: / **Praktikabilität:**	viel	wenig	keiner
niedrig			X
mittel			
hoch			

Tabelle 5.2: Bewertung von Client Honeypots für Blacklisting

5.1.2 Schadsoftwareproben extrahieren

Schadsoftwareproben können aus dem Internet, über Webseiten oder böswilligen Mails extrahiert werden.[43] Wenn ein High Interaction Client Honeypot einen Drive-by-Download identifiziert, besteht die Möglichkeit, die herunter geladene Software von ihrer Ausführung zu stoppen und als Schadsoftwareprobe zu speichern.
Lin et al.[21] haben mit Client Honeypots bereits in 2013 erfolgreich Schadsoftwareproben erhalten können, die zu dem Zeitpunkt noch nicht bekannt waren. Sie konnten auch nachweisen, dass Client Honeypots andere Schadsoftware untersuchen können, als herkömmliche, passive, Honeypots.[21] Es ist somit möglich, auch noch nicht öffentlich bekannte Schadsoftware zu untersuchen.

Evaluation Über Proben von sich im Umlauf befindender Schadsoftware lassen sich Muster, Strategien und Verschleierungsmechanismen studieren, um sich zukünftig gegen sie zu schützen. Es können Signaturen erstellt werden, um diese und sehr ähnliche Software schnell statisch erkennen zu können.
Zusätzlich können diese Proben auch genutzt werden, um Teststrukturen zu entwickeln, mit denen Systeme zukünftig getestet werden können. Die Analyse dieser Proben kann sich allerdings als aufwendig erweisen, wenn Verschleierungsmechanismen die Datei schwer zu interpretieren machen. Zudem stellt sich oftmals heraus, dass es sich bei der extrahierten Software um bereits bekannte Signaturen handelt. Dies wird aber erst nach dem Download durch den Client Honeypot erkannt.
Ein Unternehmen, dessen Fokus nicht die Analyse von Schadsoftware ist, hat ohne in dieses Feld zu investieren eine sehr limitierte Bandbreite an Nutzungsmöglichkeiten. Die extrahierte Schadsoftware an eine dafür zuständige Organisation weiterzuleiten, stellt sich als eine sicherheitstechnisch fragwürdige Aktion dar.
Die Proben auf einem Server zu speichern ist ein Risiko für das Unternehmen. Ein potentieller Insider-Angreifer, der Zugriff auf diese Software bekommt, hat die Möglichkeit Schäden anzurichten, ohne selbst Schadsoftware einschleusen zu müssen. Sollte durch

Nutzen: / Praktikabilität:	viel	wenig	keiner
niedrig			X
mittel			
hoch			

Tabelle 5.3: Bewertung von Client Honeypots zur Gewinnung von Schadsoftwareproben

einen erfolgreichen Angriff der Speicherserver übernommen werden, kann die Schadsoftware im Netzwerk möglicherweise per Fernsteuerung gestartet werden.

Auf Basis der angegebenen Gründe ist die Verwendung von Client Honeypots um Schadsoftwareproben für das Unternehmen zu erhalten mit weiteren Risiken für das Unternehmen verbunden, ohne einen großen strategischen Vorteil zu bieten. Die Extraktion von Schadsoftwareproben wird mit niedriger Praktikabilität und keinem Nutzen bewertet.

5.1.3 Zero-Day-Exploit Detektion

Client Honeypots können, wie auch herkömmliche Honeypots, eingesetzt werden, um Zero-Day-Exploits zu detektieren. Zero-Day-Exploits sind, wie in Kapitel 3.2.4 beschrieben, das Ausnutzen von Schwachstellen in Systemen und Software, die bis zu diesem Zeitpunkt unbekannt sind. So kann es also für diese noch keinen behebenden Systemaktualisierungen (sog. Patches) geben. Wenn es für einen detektierten Angriff keine bekannte Signatur gibt, ist davon auszugehen, dass dieser Angriff eine bisher unbekannte Schwachstelle ausnutzt.
Hier unterscheiden sich Client Honeypots und herkömmliche Honeypots anhand der Quelle des Angriffs. Während der herkömmliche Honeypot auf einen Angriff wartet, kann der Client Honeypot Angriffsquellen ausnutzen, die auf einen aktiven Nutzer ausgelegt sind.[21] Dies ist somit eine ergänzende Anwendungsmethode.
Per Definition muss für die Erkennung von Zero-Day-Exploits ein High Interaction Client Honeypot genutzt werden, da Low Interaction Client Honeypots auf Signaturen aufbauen, die bekannte Muster widerspiegeln.[34]

Evaluation Mit Hilfe des Client Honeypots kann das Unternehmen Exploits und Schwachstellen in Ihren Systemen finden, die noch nicht bekannt sind. Durch diesen Vorteil kann die Behebung der Sicherheitslücken der eigenen Systeme mit geringerer Verzögerung gestartet werden. Auch eine Meldung der Exploits an die Hersteller der betroffenen Systeme

Nutzen: / Praktikabilität:	viel	wenig	keiner
niedrig	X		
mittel			
hoch			

Tabelle 5.4: Bewertung von Client Honeypots zur Zero-Day-Exploit Detektion

ist denkbar. Ebenso kann die individuelle Systemkonfiguration des Unternehmens überprüft werden und gewisse Nischen-Exploits gefunden werden. Für den Fall, dass das Unternehmen keine gängige Kombination von Systemen nutzt, besteht die Möglichkeit, dass hierfür unbekannte Exploits existiert und genutzt werden.
Die Analyse der Exploits birgt einen gewissen Aufwand, den das Unternehmen aufbringen müsste. Auch ist nicht garantiert, dass ein Zero-Day-Exploit gefunden wird. Um eine nutzbare Menge an Daten zu sammeln, müsste das Internet aktiv durchsucht werden, was einen großen Aufwand bedeuten würde.
Während ein gewisser Vorteil gegeben wäre, wenn ein Zero-Day-Exploit gefunden wird, ist dieser mitunter minimal. Das Unternehmen müsste eine Meldeinfrastruktur aufbauen, über welche es gefundene Exploits an die richtige Stelle mit geringer zeitlicher Verzögerung weiterleitet.
Somit stellt diese Anwendungsmöglichkeit für ein nicht in IT-Sicherheit involviertes Unternehmen einen finanziellen und organisatorischen Aufwand dar, der sich nicht mit dem potentiellen Gewinn an Sicherheit durch eine Umsetzung dieser Maßnahme decken würde. Die Zero-Day-Exploit Detektion wird mit niedriger Praktikabilität und hohem Nutzen bewertet.

5.1.4 Identifizierung von schädlichen Webseiten im laufenden Betrieb

Während Client Honeypots zwar in der Lage sind, das Netz nach schädlichen Webseiten abzusuchen, ist ihr primäre Ziel nicht der Schutz des Nutzers. Um den Client Honeypot als ein aktives Verteidigungselement zu nutzen, haben Taylor et al. Client Honeypot-Analyse „on the wire“ vorgeschlagen. So wird im laufenden Betrieb der Internetverkehr der Nutzer analysiert und die Kommunikation mit dem angefragten Server über einen Client Honeypot zurückgespielt.[45] Falls der Client Honeypot angegriffen wird, kann der Nutzer vom Besuchen der Webseite oder der Kommunikation mit dem Server gestoppt

werden. Taylor et al.[45] beschreiben einen Vier-Schritt Ablauf unter der Voraussetzung, dass der HTTP Verkehr an der Netzwerkgrenze überwacht wird. Netzwerkgrenzen können beispielsweise Geräte wie Router sein. Der Ablauf nach Taylor et al. wird in den folgenden Absätzen beschrieben.

1) Aus Sicherheits- und Datenschutzgründen können keine echten URLs genutzt werden, da dort eventuell Nutzerdaten enthalten sein können, oder bestimmte Funktionen am Server angestoßen werden könnten, wie etwa der Kauf eines Objektes. Aus diesem Grund wird hier der Cache der Netzwerkgrenze(Router) genutzt, um aus dem aus- und eingehenden Netzwerkverkehr TCP-Sitzung-Streams zu ermitteln. Aus diesen werden dann die entsprechenden HTTP-Anfragen und Objekte rekonstruiert. Diese Objekte werden in einem separaten Cache gespeichert. So lassen sich beispielsweise Javascript oder Flash-Dateien rekonstruieren, die der Server an den Client gesendet hat.

2) Alle gespeicherten Objekte werden gefiltert, um eine zeitnahe Analyse durch den Client Honeypot zu gewährleisten. Lediglich die Objekte, die zu einem Download von häufig durch Schadsoftware belastete Dateiformaten führen, werden in der Analysekette weitergegeben. So kann ein Fokus auf beispielsweise Flash- oder Javascript-Objekte gelegt werden.

3) Im dritten Schritt müssen Informationen über den Client, den Server und auch die für den Dialogstrom verantwortliche Ursprungs-URL ermittelt werden. Anhand von bekannten Information oder in den gesammelten HTTP-Objekten hinterlegten Daten, können Informationen über den verantwortlichen Client gesammelt werden. So lassen sich oft das Betriebssystem, der Browser, genutzte Plugins etc. ermitteln, da diese bereits von dem Server angefragt worden sind. Unter Verwendung dieser Daten kann der Honeypot möglichst exakt die Identität des Clients replizieren.
Durch einen eigens entwickelten Algorithmus wird die, für den Dialog verantwortliche, Quell-URL ermittelt. Mit Hilfe der aus der Kommunikation erhaltenen Daten wird versucht, den Server zu imitieren. Da nicht mit dem echten Server oder Client interagiert werden kann, können so möglicherweise nicht alle Reaktionen des Servers korrekt nachgestellt werden.

4) Ein Client Honeypot wird gewählt, der den Client imitiert, mit einer Simulation des Servers interagiert und versucht zu ermittelten, ob der ursprüngliche Server schadhafte Intentionen hatte.

Es ist anzumerken, dass ein großer Teil des Aufwandes in der Bereitstellung und Filterung der Daten für den Client Honeypot liegt. Ein weiteres Konzept, den Nutzer im laufenden Betrieb zu schützen, sind Honeyscouts.
Honeyscouts sind ein von Christian Seifert vorgeschlagenes Konzept, einen echten Client mit einem High Interaction Client Honeypot zu schützen.[11] Hierbei wird die Systemkonfiguration des Clients so genau wie möglich kopiert. Der Idealfall für größere Institute wäre also hier, wenn möglichst viele Arbeitsplätze dieselbe Systemkonfiguration aufweisen.
Im laufenden Betrieb fungiert der Honeyscout dann als Proxy-Server für den zu schützenden Client. Wenn der Client eine Webseite öffnet, wird sie zunächst durch den Honeyscout überprüft. Dort können Sicherheitsvorfälle erkannt und der Nutzer von der Interaktion mit dem Server gestoppt werden. Für den Nutzer ist die Zwischenschaltung von Honeyscout über eine Verzögerung in der Anfragebeantwortung spürbar.[11]

Evaluation "On the wire" lässt sich der Verkehr des eigenen Unternehmensnetzwerks überwachen, in einer Art und Weise, die die Privatsphäre der Nutzer versucht zu beachten.
Die Überwachung "on the wire" überprüft nur die Verbindungen, die tatsächlich aus dem Unternehmen heraus getätigt werden und entfernt somit unnötige Untersuchungen im gesamtem Internet. Die Dateien befinden sich bereits im Netzwerk und müssen nur zur Überprüfung durch den Client Honeypot weitergeleitet werden. Zudem ist diese Untersuchungsmethode nicht darauf angewiesen, dass Server, die möglicherweise schadhafte Software verteilen, zum Untersuchungszeitpunkt erreichbar sind.
In ihrem Paper[45] haben es Taylor et al. geschafft, das gesamte Netzwerk ihrer Universität mit einem dedizierten Client Honeypot zu überwachen. Somit lässt sich die Annahme treffen, dass auch das Unternehmen mit einem Client Honeypot auskommen müsste, da sich in diesem Unternehmen im Vergleich deutlich weniger Nutzer befinden. Es wurde jedoch darauf hingewiesen, dass es zu einem hohen Filteraufwand kommt, da es zu viele zu überprüfende Objekte gibt, die hätten überprüft werden müssen.
Diese Anwendungsmethode bietet eine Möglichkeit, zielgerichtet und in einem kurzen zeitlichen Rahmen die sich im Unternehmen befindliche Schadsoftware zu erkennen. Ebenso können, wie Taylor et al. gezeigt haben, auch Zero-Day-Exploits entdeckt werden. Dies würde dem Unternehmen die Möglichkeit geben, sich weiter zu schützen.
Honeyscouts wäre ebenfalls ein System, das das Unternehmen schützen kann. Es kann im Gegensatz zur "on the wire"-Analyse den Nutzer sogar im Augenblick den Angriffs schützen, statt den Angriff nur nachvollziehen zu können.

Nutzen: / Praktikabilität:	viel	wenig	keiner
niedrig	X		
mittel			
hoch			

Tabelle 5.5: Bewertung der Identifizierung von schädlichen Webseiten im laufenden Betrieb durch Client Honeypots

Als Nebeneffekt ist die Verzögerung für den Nutzer ein für das Unternehmen mit zu betrachtender Aspekt. Eine Verzögerung von mehreren Sekunden ist nicht für jede Art von Anfrage oder Arbeitsplatzumgebung vertretbar.

Zum Zeitpunkt der Erstellung dieser Arbeit ist dem Autor jedoch keine Instanz bekannt, in der eine dieser Methoden erfolgreich angewandt oder weiterentwickelt wurden. Somit müsste das Unternehmen selbstständig die Implementation, Überwachung und Weiterentwicklung vornehmen.
Da dies einen großen Aufwand voraussetzt, der sich nur schwer bis gar nicht kalkulieren lässt und die Identifizierung "on the wire" keinen direkten Schutz darstellt, ist zu argumentieren, dass der Nutzen für das Unternehmen nicht gegeben ist. Honeyscouts kann den Nutzer direkt schützen, die vorangegangenen Aufwandsargumente greifen allerdings auch hier.
Für beide Methoden ist zudem die Datenschutzfrage noch offen. Das Unternehmen befindet sich in Deutschland. Es gibt Datenschutzrichtlinien, die den Mitarbeiter vor Spionage durch den Arbeitgeber schützen. Inwieweit die vorgestellten Methoden überhaupt legal wären, steht offen. Das Unternehmen müsste sich zur Implementierung deshalb Datenschutz- und IT-Rechtsbeistand dazu ziehen. Dies hat negative Auswirkungen auf die Praktikabilität.
Eine Überwachung im laufenden Betrieb durch Client Honeypots, wird mit niedriger Praktikabilität und hohem Nutzen bewertet.

5.1.5 Rollenbasierte Täuschung innerhalb von Unternehmensnetzwerken

Während sich die zuvor genannten Anwendungsfelder mit der Verteidigung oder der Identifikation von Gefahren befasst, die sich außerhalb des Netzwerkes befinden, stellen

Anjum et al.[3] eine Strategie vor, die bereits an einen Angreifer verloren gegangenen Netzwerkknoten als solche erkennen kann. Client Honeypots werden genutzt, um Clients zu imitieren, jedoch nicht um einen Webserver zu täuschen, sondern um sich im Netzwerk befindliche Router, Server oder Switche zu überprüfen. Eines der Hauptziele ist es zudem, die in Kapitel 3.2.6 beschriebene passive Aufklärung zu stören.

Für jede Unternehmensrolle, wie IT-Administrator, Manager, Sachbearbeiter etc. wird ein Profil angelegt, welches die üblichen Netzwerkströme dokumentiert. Datenvolumen, relevante Server und Arbeitszeiten können mit anderen Metriken zusammen gespeichert und statistisch analysiert werden. Ziel ist es, einen Client zu erzeugen, der sich auf Netzwerkebene nicht von echten Nutzern unterscheiden lässt. Dieser Client wird im weiteren Verlauf zur besseren Unterscheidung als Honeyrole-Client bezeichnet.

Diese Honeyrole-Clients werden dann an echten Arbeitsstationen über eine virtuelle Maschine eingesetzt und interagieren mit dem aus dem Nutzerprofil ermittelten Servern. Um eine möglichst hohe Netzwerkabdeckung zu gewährleisten, wird gezielt der Pfad vom Client zum Server dynamisch über die Netzwerkknoten angepasst. Diese Einstellung gilt auch für die echten Clients, da sie sich von einem Beobachter auf Netzwerkebene sonst von den Honeyrole-Clients anhand ihrer Pfadnutzungen unterscheiden lassen könnten.
Jeder Client versendet in regelmäßigen Abständen Lebenszeichen an eine zentrale Controller-Einheit. Hierbei ist lediglich der Inhalt der Lebenszeichennachrichten der Honeyrole-Clients relevant. In diesen Nachrichten sind Reports dekodiert, die auch Alerts, also Warnungen, enthalten. Alerts werden ausgelöst, wenn Pakete über einen Switch länger brauchen als über andere, Pakete verloren gehen oder verfälscht ankommen. Auf dieser Basis kann statistisch berechnet werden, wie wahrscheinlich es ist, dass ein Netzwerkknoten durch einen Widersacher übernommen worden ist.

Evaluation Rollenbasierte Täuschung durch Honeyrole-Clients gibt dem IT-Administrator einen Überblick darüber, wie wahrscheinlich es ist, dass ein bestimmter Knoten sich auffällig verhält. Zudem wird weiterer Verkehr im Netzwerk erzeugt, was es den Angreifern erschwert, die realen Nachrichten abzufangen. Ebenso wird es erschwert herauszufinden, zu welchem Mitarbeiter die jeweilige Verbindung gehört, was zu einer Verminderung des Risikos von Spear-Phishing oder anderen Social-Engineering-Attacken auf Basis des beobachteten Verkehrs führen kann.
Sollte ein Angreifer erfahren, dass diese Methode eingesetzt wird, dann weiß dieser, dass sich sein Aufwand erhöhen wird, um mit den erschwerten Bedingungen im Netzwerk zu arbeiten. Dies führt zu einer Erhöhung der Kosten für den Angreifer und erhöht das

Risiko entdeckt zu werden. Demnach kann es sein, dass es zu einigen Angriffen gar nicht erst kommt, da sich der Nutzen für den Angreifer erübrigt hat.[25]
Um den gefälschten Netzverkehr nutzen zu können, muss dieser generiert werden, was eine stärkere Netzauslastung zu Folge hat. Netzwerke, die bereits an ihrem Limit agieren, könnten überlasten. Somit muss dafür gesorgt werden, dass auch zu Stoßzeiten die Verbindungen der Honeyrole-Clients genutzt werden können und das Netz der Auslastung standhalten kann.
Es müssen echte Clients installiert werden, die Verbindungen mit Servern im Netzwerk aufnehmen. Es ist möglich eine oder mehrere Clients in einer virtuellen Maschine auf einem existierenden Gerät laufen zu lassen. Ein Aufwand für die IT-Abteilung zur Installation und Wartung ist zu beachten. Der Stromverbrauch der jeweiligen Geräte erhöht sich als Folge.[40] Bei Änderungen an der Arbeitsplatzstruktur, beispielsweise beim Umzug einer Abteilung in ein anderes Büro, müssen Teile des Netzwerkes gewartet werden. Falls ein Angreifer Wissen über diesen Umzug erlangt, könnte dieser Informationen über echte Clients und Honeyrole-Clients erhalten. Der Miteinbezug der Honeyrole-Infrastruktur ist somit ein Aspekt, der beachtet werden muss. Demnach muss die IT-Abteilung, die diese Täuschung nutzt, darauf achten, dass sich schwer zu schätzende zusätzliche Aufwände und Kosten in anderen Projekten entwickeln können.
Während die rollenbasierte Täuschung eine sensible Möglichkeit bietet, Angreifer zu entdecken, muss auch mit Falsch-positiv-Ergebnissen umgegangen werden. Die Reparatur eines Netzwerkknotens ist oft nicht mit dem Zurücksetzen auf Werkseinstellungen erledigt, sondern involviert oft auch einen Austausch des Gerätes selbst. Ebenso ist der Teil des Netzwerks, der über den Knoten kommuniziert, für den Zeitraum der Bereinigung möglicherweise nicht nutzbar.

Die Anwendung der rollenbasierten Täuschung ist derzeit in nur einer Veröffentlichung diskutiert. Sie bietet allerdings eine direkte Verteidigungsmechanik, die das Unternehmen schützen kann. Kosten für Angreifer werden gesteigert, die Wahrscheinlichkeit eines Nutzens für den Angreifer senkt sich und die Entdeckung eines Angreifers kann in kurzer Zeit erfolgen. Es bietet sich ein klarer Nutzen beim Einsatz dieser Client Honeypot-Applikation. Dem entgegen stehen die hohen Installationskosten, erhöhte Netzwerkauslastung, Stromverbrauch und resultierende Aufwände in Projekten, die hierzu nicht direkt in Bezug stehen.
Rollenbasierte Täuschung durch Client Honeypots wird mit mittlerer Praktikabilität und hohem Nutzen bewertet.

Nutzen: / Praktikabilität:	viel	wenig	keiner
niedrig			
mittel	X		
hoch			

Tabelle 5.6: Bewertung der Rollenbasierten Täuschung mit Hilfe von Client Honeypots

5.1.6 Überprüfung von Mailinhalten

Eine große Menge von Malware wird über E-Mail versandt. Ein Nutzer wird durch z.B. Social Engineering dazu gebracht, einen Anhang herunterzuladen, der sich dann als Schadsoftware entpuppt. Auch kann es schon ausreichen, den Nutzer dazu zu bringen, die in der Mail enthaltenen Verlinkungen zu öffnen, welche dann auf eine schadhafte Webseite verweisen.[50]

Client Honeypots, wie SHELIA[32], können eingesetzt werden, bevor die Mail dem Nutzer zugänglich gemacht wird, um die Anhänge herunterzuladen, zu überprüfen und dabei den Client zu imitieren. In dem Fall, in dem ein vermeintlicher Angriff erkannt wird, wird die Mail dem Nutzer vorenthalten und dieser daran gehindert, die gefährlichen Inhalte zu laden.

Evaluation Schadsoftware verbreitet sich über E-Mail und oft lassen sich auch geschulte Nutzer dazu verleiten, auf Links zu schadhaften Webseiten zu klicken oder Dateien herunterzuladen, die Angriffe ausüben.
Demnach ist es wichtig, diese Mails dem Nutzer vorzuenthalten, um solchen potentiellen Gefahren entgegen zu wirken. Der Nutzer spart Arbeitszeit, indem er die Mail nicht manuell identifizieren, löschen und eventuell noch der IT-Abteilung melden muss. Wird ein Client Honeypot auf Mails angesetzt, dann kann dieser das System des Rezipienten nachstellen und Dateianhänge in einer Sandbox-Umgebung überprüfen und allen Links folgen. Hierdurch entsteht nur so viel Aufwand wie notwendig, da die Überprüfung zielgerichtet und anlassbezogen stattfindet.
Die Untersuchung von jeder Mail führt allerdings zu einer Verzögerung in der Ankunftszeit der Mail. Ein wichtiger Report mit vielen Anhängen, der dringend benötigt wird, kann möglicherweise für einige Minuten in der Analyse des Client Honeypots stecken oder sogar als Falsch-positiv-Ergebnisse in die Quarantäne verschoben werden.
Der Client Honeypot kann zentral stehen und lässt sich mit geringem Aufwand an die Infrastruktur anschließen. Falls der Honeypot fester Bestandteil der Infrastruktur sein

Nutzen: / **Praktikabilität:**	viel	wenig	keiner
niedrig			
mittel			
hoch	X		

Tabelle 5.7: Bewertung der Überprüfung von Mailinhalten durch Client Honeypots

sollte, ist mit einem Ausfallen des Honeypots zu rechnen. In diesem Fall kann der Mailverkehr des Unternehmens gestört werden.
Möglicher zusätzlicher Personalaufwand kann im Störungsfall anfallen, wenn die Mitarbeiter Probleme an die IT-Abteilung melden. Hinzu kommen möglicherweise auftretende Verzögerungen im Betriebsablauf. Eine Redundanz des Client Honeypots, als Maßnahme, das Ausfallrisiko zu reduzieren, erhöht die Anschaffungskosten des Systems.
Einen Client Honeypot zu nutzen, um ins Unternehmensnetzwerk eingehende Mails zu überprüfen ist eine Methode die Nutzer vor Angriffen zu schützen und das schwächste Glied in der Sicherheitskette, den Nutzer, von schadhaftem Verhalten abzuhalten. Für das Unternehmen sollte es möglich sein, solch einen Client Honeypot einzusetzen, um die Sicherheit zu erhöhen. Die Überprüfung von Mailinhalten durch Client Honeypots wird mit hoher Praktikabilität und hohem Nutzen bewertet.

5.2 Zusammenfassung

Die zuvor vorgestellten Anwendungsmöglichkeiten von Client Honeypots sind für ein Unternehmen in Nischensituationen tragbar. Für keinen genannten Bereich gibt es jedoch Erfahrungsberichte, die eine genauere Einschätzung gewährleisten. Damit sich ein Nutzen für die Verbesserung der IT-Sicherheit eines Unternehmens bilden kann, ist weitere Forschung in diesen Bereichen notwendig. Oftmals ist zu einem Anwendungsgebiet nur eine Quelle veröffentlicht, zu der etwaige Folgequellen das Kernkonzept nicht weiter vertiefen.
In Tabelle 5.8 sind die Bewertungen der vorigen Kapitel zusammengetragen. Ersichtlich ist, dass überwiegend "viel" Nutzen für die Anwendungsmöglichkeiten von Client Honeypots ermittelt wurde. Gegenteiliges ergibt sich jedoch auch für die Praktikabilität. Lediglich eine Anwendungsmöglichkeit ist sowohl "hoch" Praktikabel und hat "viel" Nutzen.
Für die meisten Anwendungsmöglichkeiten müsste das Unternehmen, das die Client

Honeypot-Anwendungsmöglichkeiten einzusetzen plant, einen Großteil der Forschung beisteuern. Es kann sich dabei nicht an Vorreitern orientiert werden. Wenngleich es einen Wettbewerbsvorteil bedeuten könnte, haben Unternehmen für gewöhnlich nicht vor, komplett neue Systeme zu entwickeln, um ihre IT-Sicherheit zu verbessern. Oftmals sind Versicherungen und Verträge mit Sicherheitsanbietern mit einem höheren Nutzen verbunden.
Als Ergebnis der Analyse zeigt sich, dass Client Honeypots einen hohen Nutzen für die IT-Sicherheit des vorgestellten Unternehmens haben können. Die Praktikabilität stellt jedoch ein großes Hindernis dar. Lediglich die Überprüfung von Mails hat sich als wirklich praktikabel herausgestellt.

Nutzen: / **Praktikabilität:**	viel	wenig	keiner
niedrig	2	0	2
mittel	1	0	0
hoch	1	0	0

Tabelle 5.8: Übersicht der Analyseergebnisse im Bezug zu Nutzen und Praktikabilität

Für ein Unternehmen, dessen Schwerpunkt nicht in IT-Sicherheitsprodukten liegt, ist es demnach eine komplizierte Entscheidung, ob Client Honeypots als aktive Verteidungswerkzeuge eingesetzt werden können. Wenn die Forschung hier weiter voranschreitet und auch Fallstudien zu diesen Themen veröffentlicht werden, kann sich dieses Bild zukünftig ändern.

6 Diskussion

In diesem Kapitel werden Aspekte, die diese Arbeit betreffen, kritisch aufgearbeitet. Zunächst werden die verwendeten Methoden bewertet. Anschließend wird auf das Fehlen von Fallstudien im Bereich Client Honeypots hingewiesen. Client Honeypot-Software, die frei im Internet verfügbar ist, wird in Kapitel 6.3 aufgeführt. Kapitel 6.4 wird einen Ausblick über zukünftige Ergebnisse im Bereich Client Honeypot vermitteln.

6.1 Angewandte Analysemethode

Die Analyse der Client Honeypot-Anwendungsmethoden in Kapitel 5.1 hat sich auf ein fiktives Unternehmen gestützt, welches anhand von verfügbaren Daten zusammengestellt wurde. Darüber hinaus konnten keinerlei Kosten ermittelt werden, um verschiedene Client Honeypot-Anwendungsmethoden anhand ihrer tatsächlichen Aufwände vergleichen oder bewerten zu können. Somit konnten Analyseergebnisse lediglich angenähert werden. Es müssten weitere Untersuchungen angestellt werden, um die angegebenen Kriterien zu verifizieren und zu gewichten.
Die Zusammenarbeit mit einem Unternehmen wäre eine Möglichkeit, die Analyse auf reale Daten zu beziehen.

6.2 Fallstudien zu Client Honeypots

Zum Zeitpunkt der Erstellung dieser Arbeit wurde noch keine Fallstudie veröffentlicht, die Client Honeypots in einem Unternehmen einsetzt oder einführt.
Lediglich Taylor et al.[45] haben in ihrer Vorstellung der Client Honeypot-Analyse "on the wire" ihr Ergebnis an ihrem Universitätsnetzwerk testen und Ergebnisse sammeln können. Jedoch gibt es noch keine Forschung, die die Ergebnisse verifiziert hat. Taylor et al. haben ihren Client Honeypot und ihr Framework nicht veröffentlicht, was eine Hürde

in der Überprüfung ihrer Forschungsergebnisse darstellt.
Diese Sachlage lässt sich bei einem großen Teil der Client Honeypot-Forschung antreffen. Häufig wird in der Vorstellung der Forschung auf eine empirische Testphase verwiesen, die genutzten Testdaten oder entwickelte Software werden aber nicht veröffentlicht.
Diese Arbeit hätte von Fallstudien profitiert, da diese eine Basis geschaffen hätten, um die verschiedenen Anwendungsmethoden miteinander zu vergleichen. Anhand von Erfahrungsberichten und einer eigenen, zielgerichteten Nutzenanalyse hätte die Qualität der Analyse in Kapitel 5.1 verbessert werden können.
Insbesondere in einem wirtschaftlichen Kontext sind Fallstudien ein wichtiges Medium, um Technologien bewerten zu können. Sie geben Unternehmen die Chance, einschätzen zu können, ob die Implementation einer neuen Technologie aus Management-Sicht vertretbar ist.
Dass es zur Nutzung von Client Honeypots zu vielen der Anwendungsgebiete aus Kapitel 5.1 keine Fallstudien gibt, kann ein Indiz dafür sein, dass die Technologien von Unternehmen nicht für die wirtschaftliche Nutzung in Betracht gezogen werden. Mögliche Gründe hierfür sind vielseitig. In der Analyse wurden folgende identifiziert:

- Das Unternehmen muss eigene Client Honeypot-Software entweder von Grund auf entwickeln, oder muss bestehende Software aktualisieren. Es besteht ein Mangel an aktueller frei verfügbarer Client Honeypot-Software. Für Unternehmen kann die Kombination aus unklarem tatsächlichem Nutzen und der benötigten Investition abschreckend wirken.

- Hardwarekosten fallen an. Die Bereitstellung und Wartung von Clients für den Client Honeypot-Gebrauch ist mit Kosten verbunden. Für eine Testphase müsste Hardware genutzt werden, die womöglich erst eingekauft werden muss. Die Möglichkeit, dass diese Hardware nach Ablauf einer Testphase zu Zwecken einer Fallstudie nicht mehr benötigt wird, ist gegeben.

- Client Honeypot-Anwendungsmöglichkeiten, wie etwa die rollenbasierte Täuschung aus Kapitel 5.1.5, können das Unternehmensnetzwerk stark beeinflussen. Eine Umstellung des Netzwerks auf die Nutzung von Client Honeypots kann die Struktur stark verändern. Es lohnt sich möglicherweise nicht für ein Unternehmen, solche Änderungen an der Netzwerkstruktur für eine Fallstudie durchzuführen.

- Der Mangel an rechtlicher Sicherheit, insbesondere im Bereich Datenschutz für Mitarbeiter, ist ein in der Forschung noch wenig beachteter Aspekt. Insbesondere Unternehmen, die sich in Ländern mit strengeren Datenschutzrichtlinien befinden,

benötigen ein gewisses Maß an Sicherheit. Verstöße können Schäden am Unternehmen nach sich ziehen.

- Client Honeypot-Anwendungsmöglichkeiten in Unternehmen sind bisher wenig erforscht. Ein Unternehmen kann nicht abschätzen, wie hoch das Risiko ist, wenn die Technologie nicht korrekt verwendet wird.

Diese Hypothesen lassen sich derzeit nicht anhand einer Quelle belegen und bilden Material für zukünftige Forschungen.

6.3 Derzeit verfügbare Client Honeypot-Software

In diesem Kapitel werden Client Honeypots, die zum Zeitpunkt der Erstellung dieser Arbeit im Internet frei verfügbar sind, vorgestellt. Es wird zwischen zwei Kategorien unterschieden: Client Honeypots, die innerhalb der letzten zwei Jahre aktualisiert worden sind und die, bei denen die letzte Aktualisierung weiter zurück liegt. Zwei Jahre sind in diesem Fall arbiträr gewählt, sie dienen einer Kennzeichnung von aktuelleren Client Honeypots.
Für jeden dieser Client Honeypots wird untersucht, welche der in Kapitel 5.1 beschriebenen Anwendungsmöglichkeiten sie unterstützen. Die Ergebnisse werden in einer Tabelle zur besseren Übersicht abgebildet. Mögliche Werte sind: ✔, um anzuzeigen, dass die Technologie unterstützt wird und ✕, wenn dies nicht der Fall ist.
Es ist anzumerken, dass die in Kapitel 5.1.5 beschriebene rollenbasierte Täuschung nicht überprüft wird. Hierfür werden keine Client Honeypots im eigentlichen Sinne benötigt und diese Anwendungsmöglichkeit wird dementsprechend von keinem bisher veröffentlichten Client Honeypot unterstützt.

Anwendung: / **Honeypot:**	Blacklisting	Schadsoftware-proben	Zero-Day -Exploit Detektion	Analyse "on the wire"	Mailinhalt-überprüfung

Tabelle 6.1: Bewertungstabelle der Client Honeypot-Software im Bezug auf Unterstützung der Anwendungsmethoden aus Kapitel 5.1

6.3.1 Mit Update innerhalb der letzten Jahre

- "Thug" ist ein auf Python basierender Low Interaction Client Honeypot, geschrieben und gewartet von Angelo Dell'Aera. Dieser Client Honeypot ist Open-Source und wird aktuell weiter entwickelt.[12] Thug kann genutzt werden, um Webseiten zu analysieren. Somit können Blacklists überprüft und erstellt werden.
  Durch die vorhandene API, kann Thug auch für eine Honeyscout-Anwendung[11] genutzt werden. Ebenso werden Proxy-Server-Verbindungen unterstützt, was Thug für die Verwendung der Analyse im laufenden Betrieb zulässig macht.[45] Da es sich um einen Low Interaction Client Honeypot handelt, ist die Suche nach Zero-Day-Exploits keine Kernanwendung.

- "YALIH" (Yet Another Low Interaction Honeyclient) ist ein Low Interaction Client Honeypot der Victoria University of Wellington. Die derzeit letzte Aktualisierung war im Jahre 2019.[24] YALIH unterstützt die Websuche nach bösartigen Webseiten und ist auch darauf ausgelegt, Mails zu überprüfen. Ebenso wie Thug steht die Entdeckung von Zero-Day-Exploits aufgrund des Interaktionslevels nicht im Fokus. Proxy-Server-Verbindungen werden unterstützt und somit ist eine Anwendung "on the wire" möglich.

- "miniC" der Low Interaction Client Honeypot miniC ist darauf ausgelegt mit möglichst wenigen Abhängigkeiten zu arbeiten. MiniC ist ein Kooperationsprojekt der Victoria University of Wellington und dem New Zealand Honeynet Chapter.[23] Die Anwendungsmöglichkeiten von miniC sind etwas begrenzter als die von Thug oder YALIH, da zur Analyse ein Antivirenprogramm Dritter hinzugezogen wird. Derzeit gibt es keine Unterstützung für Proxy-Server-Verbindungen. Eine "on the wire" Analyse ist somit nicht möglich.

Anwendung: / **Honeypot:**	Blacklisting	Schadsoftware-proben	Zero-Day -Exploit Detektion	Analyse "on the wire"	Mailinhalt-überprüfung
Thug	✔	×	✔	✔	×
YALIH	✔	×	✔	✔	✔
miniC	✔	×	×	×	✔

Tabelle 6.2: Unterstützung der Anwendungsgebiete durch aktuelle Client Honeypots

6.3.2 Ohne Update innerhalb der letzten Jahre

- "Trigona" ist ein Produkt des Australian Honeynet Project, in dem ein Zeitgeber um eine Sandboxing Software herum aufgebaut wurde. In Essenz handelt es sich hier um einen High Interaction Client Honeypot.[4] Trigona kann Schadsoftware-proben sammeln und Webseiten auf ihre Schädlichkeit prüfen. Als High Interaction Client Honeypot, kann Trigona auch Zero-Day-Exploits entdecken. Die Überprüfung von Mailinhalten ist jedoch nicht direkt unterstützt. Trigona ist darauf ausgelegt, eine große Anzahl von URLs gleichzeitig zu überprüfen und dann eine Analyse des Speichers durchzuführen. Eine Verwendung im laufenden Betrieb "on the wire" ist demnach nicht möglich.

- "Honeyspider Network Capture-HPC NG" ist die für das Honeyspider Network angepasste Version von Christian Seiferts Capture HPC Client Honeypot.[16] Es handelt sich um einen High Interaction Client Honeypot. Die Überprüfung von Mails wird nicht unterstützt. Nutzung des Honeypots "on the wire" ist keine mögliche Funktionalität.

- "HoneyC" ist ein Low Interaction Client Honeypot, entwickelt an der Victoria University of Welligton von Christian Seifert.[35] Veröffentlicht in 2006 ist es eines der ältesten verfügbaren Low Interaction Client Honeypots. Somit ist die Verfügbarkeit für die in Kapitel 5 diskutierten Client Honeypot-Anwendungsmöglichkeiten gering. Lediglich die Überprüfung von Webseiten auf schädliche Aktionen wird unterstützt.

- "Honeyspider Network 2.1" ist eine Sammlung von Client Honeypots und zugehöriger Software. Es ist aus einer Kooperation aus dem NASK/CERT Polska (Polen) und dem National Cyber Security Centre (Niederlande) entstanden. Die Arbeit an diesem Projekt wurde im Jahre 2016 eingestellt.[27] Es enthält Low Interaction, sowie High Interaction Client Honeypots, darunter ältere Versionen von Thug und Capture HPC.
  Es handelt sich aber nicht explizit um einen Hybriden Client Honeypot. Extraktion von Schadsoftware, die Entdeckung von Zero-Day-Exploits und Blacklisting werden unterstützt. Mails sind akzeptierte Überprüfungsformate.
  Eine Proxy-Server-Anbindung ist nicht möglich.

- "Monkey-Spider", erstellt von Ikinci et al., ist ein Low Interaction Client Honeypot der Universität von Mannheim. Der Fokus der Forschung lag darin, die Crawler-Aktivität von der Untersuchungsaktivität zu trennen.[14] Webseitenüberprüfung

und Blacklisterstellung sind ein zentrales Ziel von Monkey-Spider. Auch die Überprüfung von Mails wird unterstützt. Ebenso kann Monkey-Spider für eine "on the wire" Analyse genutzt werden.

- "PhoneyC" wurde 2009 von Jose Nazario entwickelt. Es handelt sich um einen Low Interaction Client Honeypot.[28] Es wird in erster Linie das Internet nach böswilligen Webseiten untersucht.

- "MCEDP HoneyClient" ist ein High Interaction Client Honeypot, mit dem Ziel, eine Infektion des Client Honeypots zu verhindern.[17] Es wird aktiv versucht, keine Schadsoftwareproben zu entnehmen. Möglichst viele Webseiten zu untersuchen und Zero-Day-Exploits zu entdecken ist das zentrale Untersuchungsziel von MCEDP. Die Überprüfung von Mails und die Nutzung von Proxy-Servern werden somit auch nicht unterstützt.

- "Shelia" ist ein High Interaction Client Honeypot der Vrije Universiteit Amsterdam und konzentriert sich darauf, Spam-Mails zu überprüfen.[7] Die Untersuchung von Webseiten ist kein zentrales Anwendungsgebiet, wird aber zur Überprüfung von Mails unterstützt. Shelia kann Schadsoftwareproben sammeln, hat allerdings keine integrierte Proxy-Server-Kompatibilität.

Anwendung: / **Honeypot:**	Blacklisting	Schadsoftware-proben	Zero-Day -Exploit Detektion	Analyse "on the wire"	Mailinhalt-überprüfung
Trigona	✔	✔	✔	×	×
Honeyspider Network Capture-HPC NG	✔	✔	✔	×	×
HoneyC	✔	×	×	×	×
Honeyspider Network 2.1	✔	✔	✔	×	✔
Monkey-Spider	✔	×	×	✔	✔
PhoneyC	✔	×	×	×	×
MCEDP HoneyClient	✔	×	✔	×	×
Shelia	✔	✔	×	×	✔

Tabelle 6.3: Unterstützung der Anwendungsgebiete durch nicht mehr aktuelle Client Honeypots

6.4 Zukunft von Client Honeypots

Da Client Honeypots ein wichtiges Werkzeug in der Erkennung von schadhaften Verhalten von Webseiten sind, zeichnet sich zu diesem Zeitpunkt auch noch nicht ab, dass die Forschung und Entwicklung in diesem Bereich in naher Zukunft aufhört.

Während der Literaturrecherche ist auffällig geworden, dass die Anwendung von maschinellem Lernen für die Erkennung von Angriffen in den letzten Jahren einen großen Zuwachs erhalten hat. Die Zusammenwirkung von Client Honeypots und maschinellem lernen, insbesondere für den Bereich von Low Interaction Client Honeypots, bleibt abzuwarten.
Ob Client Honeypots als aktives Verteidigungsinstrument in Unternehmen zum Einsatz kommen, ist derzeit unwahrscheinlich. Hierfür spricht auch das vermeintlich fehlende Interesse von Wirtschaftsunternehmen, was sich, wie in Kapitel 6.2 beschrieben, auch am Fehlen von Fallstudien zeigt.

7 Fazit

In dieser Arbeit wurden sechs verschiedene Anwendungsmethoden für Client Honeypots in einem fiktiven Unternehmen untersucht. Lediglich eine dieser Methoden hat sich im Laufe der Analyse als eine Technologie herausgestellt, die ein mittelständisches Unternehmen mit vertretbarem Aufwand implementieren könnte.
Client Honeypots zur Überprüfung von eingehenden Mails zu nutzen ist somit hervorzuheben. Diese Anwendungsmöglichkeit bietet eine skalierbare Möglichkeit, die Anwender im Unternehmen vor Phishing oder anderen böswilligen Mails zu schützen, ohne, dass die Nutzer mit diesen Mails interagieren müssen.
Jede vorgestellte Anwendungsmethode benötigt jedoch weitere Forschung, um Kosten und Effektivität besser bewerten zu können. Die Veröffentlichung von Fallstudien und Daten aus Unternehmen, welche eine der betrachteten Client Honeypot-Anwendungsmethoden einsetzen, bleibt abzuwarten.
Es gibt eine Vielzahl von Client Honeypots, die frei im Internet verfügbar sind. Von ihnen jedoch nur drei, die in den letzten zwei Jahren aktualisiert worden sind. Nur einer davon, Thug, ist noch im Jahre 2020 aktiv. Client Honeypot-Software ist, wie in Kapitel 6.3 aufgezeigt, auch für die analysierten Anwendungsbereiche verfügbar, aber entweder veraltet oder nicht mit Sicht auf die Anwendungsmöglichkeiten entwickelt. Ferner müsste die Koexistenz der Client Honeypot-Anwendungsmethoden mit den rechtlichen Rahmenbedingungen des Bereichs Datenschutz weiter erforscht werden.
Abschließend ist zu sagen, dass Client Honeypots in der Forschung einen wichtigen Teil dazu beitragen, Cyber-Kriminalität zu bekämpfen. Eine Nutzung für Unternehmen, um ihre Cybersicherheit zu verbessern, benötigt allerdings noch weitere Forschung, insbesondere Fallstudien und mehr aktuelle, frei verfügbare Client Honeypot-Software.
Diese Arbeit hat einen Teil dazu beigetragen, diesen Bedarf aufzudecken. An dieser Stelle wird erneut auf den dringenden Bedarf an Fallstudien im Bereich Client Honeypots hingewiesen.

7.1 Ausblick

Die in dieser Arbeit durchgeführte Analyse konnte sich nicht auf Echtdaten aus Unternehmen stützen. Um zukünftig eine Basis für weitere Analysen des Themengebiets zu schaffen, wird ein Konzept vorgestellt, welches Anreize für die Erstellung von Fallstudien in Unternehmen geben soll.
Ziel ist es, Ansatzpunkte für weitere Projekte und Arbeiten im Bereich Client Honeypots zu schaffen.
In Kapitel 6.2 wurden mögliche Gründe genannt, die Unternehmen davon abhalten können, Fallstudien durchzuführen und zu veröffentlichen. Im Folgenden wird auf diese Punkte eingegangen und anschließend das ausgearbeitete Konzept vorgestellt.
Es wurde der aufzuwendende Selbstanteil im Bereich Forschung und Implementierung als Hemmnis des Nutzens für das Unternehmen aufgeführt. Wenn sich dieser Anteil verringern lässt, kann es sich für ein Unternehmen möglicherweise als nützlich erweisen, Client Honeypots als Sicherheitswerkzeug einzusetzen oder gar erst in Betracht zu ziehen.
Um dies zu erreichen ist es notwendig, die Technologie für Unternehmen zugänglich zu machen. Wenn ein Unternehmen einen bereits existierenden Client Honeypot einsetzt, verringert sich der Forschungsaufwand für das Unternehmen. Zudem können Erfahrungswerte auf Basis gleicher oder ähnlicher Systeme gesammelt und verglichen werden. Damit kann der Fokus der Forschung auf die Evaluation von Konzepten, statt auf die Implementation eines lauffähigen und aktuellen Client Honeypot gerichtet werden.
Ein mögliches Szenario ist, dass ein Forschungsinstitut, beispielweise eine Hochschule oder Universität, selbst einen Client Honeypot zu einem bestimmten Anwendungsgebiet erstellt. Wie in Kapitel 6.3 aufgezeigt, stehen mehrere Client Honeypots im Internet zur Verfügung, welche frei genutzt und verändert werden dürfen.
Für den Forschungserfolg auf dem Gebiet der Client Honeypots ist es wichtig, dass Daten und Software mit der Wissenschaftsgemeinde geteilt werden.
Nachdem das Institut Forschungserfolge erzielt hat, werden Unternehmen für Partnerschaften angefragt. Hier ist es wichtig, dass die Unternehmen von möglichen Risiken unterrichtet werden. Wenn anschließend eine Fallstudie zustande kommt, dann ist eine Veröffentlichung dieser für den weiteren Verlauf der Forschung wichtig.

8 Weiterführende Quellen

Dieses Kapitel führt Quellen auf, die zur weiteren Forschung im Bereich Client Honeypots relevant sind. An dieser Stelle wird sich auf eine kurze Zusammenfassung der Arbeiten beschränkt.

- **Client-side threats and a honeyclient-based defense mechanism, Honeyscout:** In dieser Arbeit stellt Seifert eine Möglichkeit vor, Client Honeypots als direktes Schutzwerkzeug für Anwender einzusetzen. Dieser Mechanismus wird Honeyscout genannt. Ein Client Honeypot lädt die vom Anwender besuchten Webseiten oder heruntergeladenen Dateien in einer sicheren Umgebung vor und warnt den Nutzer, wenn eine schadhafte Aktion erkannt wird.[11]
- **SeedsMiner: Accurate URL Blacklist-Generation Based on Efficient OSINT Seed Collection:** Tanaka et al. nutzen Client Honeypots, um aus öffentlich zugänglichen Quellen (Open Source Intelligence, kurz OSINT) verbesserte Blacklists zu erstellen. Es wird auf das Problem eingegangen, dass öffentlich zugängliche Quellen eine hohe Ungenauigkeit aufweisen.[44]
- **Taxonomy of Honeypots:** Der Forschungsbereich von Honeypots leidet darunter, dass Begriffe nicht einstimmig definiert sind. Seifert et al. führen eine Taxonomy ein, um Honeypot Studien einheitlicher zu gestalten. Die Ergebnisse dieser Ausarbeitung werden weitläufig eingesetzt.[38]
- **A Novel Scoring Model to Detect Potential Malicious Web Pages:** Le et al. führen ein Bewertungsverfahren ein, um gefährliche Webseiten anhand des Grades ihrer Böswilligkeit einordnen zu können. Dies liefert eine Technik, um einschätzen zu können, ob eine potentiell gefährliche Webseite zur Überprüfung an einen langsamen High Interaction Client Honeypot weitergeleitet werden soll.[20]

- **A behavioural study in run-time analysis environments and drive-by-download attacks:** Potaroo gibt in dieser Ausarbeitung Einblicke in das Verhalten von Drive-By-Download Angriffen. Diese werden dann für die Verbesserung der Effizienz von High Interaction Client Honeypots genutzt. Zudem wird gezeigt, dass sich Angriffe auf distinkte Weise, selbst zwischen sehr ähnlichen Systemkonfigurationen, unterscheiden.[30]
- **True Positive Cost Curve: A Cost-Based Evaluation Method for High-Interaction Client:** Die True Positive Cost Curve ist eine Methode, um die Effizienz eines Client Honeypots anhand der generierten Kosten zu messen. Die Kosten werden pro wahrhaft positivem Treffer berechnet. Seifert et al. geben somit eine Basis, um mehrere Client Honeypots auch in einem wirtschaftlichen Aspekt zu vergleichen.[37]
- **The Art of False Alarms in the Game of Deception: Leveraging Fake Honeypots for Enhanced Security:** Böswillige Webseiten versuchen Client Honeypots zu erkennen, um sich diesen Gegenüber als legitim ausgeben zu können, damit die Webseite auf keiner Blacklist landet. Zarras schlägt eine Sicherheitsmechanik vor, die sich dieses Verhalten zu Nutze macht, um Nutzer zu schützen. Einer potentiell gefährlichen Webseite werden absichtlich Informationen übermittelt, die auf die Anwesenheit eines Client Honeypots schliessen könnten.[53]

Literaturverzeichnis

[1] Akiyama, Mitsuaki ; Kawakoya, Yuhei ; Hariu, Takeo: Scalable and Performance-Efficient Client Honeypot on High Interaction System. In: *2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet*, 2012. – ISBN 978-0-7695-4737-4

[2] Akiyama, Mitsuaki ; Yagi, Takeshi ; Itoh, Mitsutaka: Searching Structural Neighborhood of Malicious URLs to Improve Blacklisting. In: *2011 IEEE/IPSJ International Symposium on Applications and the Internet*, 2011. – ISBN 978-0-7695-4423-6

[3] Anjum, Iffat ; Zhu, Mu ; Polinsk, Isaac ; Enck, William ; Reiter, Michael K. ; Sing, Munindar: Role-Based Deception in Enterprise Networks. In: *Proceed-ings of ACM Conference, Washington, DC, USA, July 2017 (Conference'17)*, 2018. – ISBN 978-1-4503-4992-5

[4] Australian Honeynet Project: *Trigona*. – URL http://www.honeynet.org.au/tools/. – Zugriffsdatum: 21.12.2020, 18:00

[5] Bhumika ; Sharma, Vivek: Use of Honeypots to Increase Awareness regarding Network Security. In: *International Journal of Recent Technology and Engineering (IJRTE)*, 2012

[6] Bilge, Leyla ; Dumitras, Tudor: Before We Knew It An Empirical Study of Zero-Day Attacks In The Real World. In: *CCS '12: Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, S. 833–844. – ISBN 978-1-4503-1651-4

[7] Bos, Herbert ; Roscapana, Joan R.: *SHELIA*. – URL https://www.cs.vu.nl/~herbertb/misc/shelia/. – Zugriffsdatum: 21.12.2020, 18:00

[8] Bundesministerium des Inneren: *Cyber-Sicherheitsstrategie für Deutschland 2016*

[9] Campbell, Ronald M. ; Padayachee, Keshnee ; Masombuka, Themba: A Survey of Honeypot Research: Trends and Opportunities. In: *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015. – ISBN 978-1-9083-2052-0

[10] Cayubit, Ryan Francis O. ; Rebolledo, Kevin M. ; Kintanar, Romulo Gabriel A. ; Pastores, Angelissa G. ; Santiago, Alen Josef A. ; Valles, Paula Bianca V.: A Cyber Phenomenon: A Q-Analysis on the Motivation of Computer Hackers. In: *Psychological Studies* 62 (2017), Nr. 1, S. 386–394

[11] Clementson, Christian: *Client-side threats and a honeyclient-based defense mechanism, Honeyscout.* 2009 - Linköping University, Schweden

[12] Dell'Aera, Angelo: *thug.* – URL https://github.com/buffer/thug/. – Zugriffsdatum: 21.12.2020, 18:00

[13] Egelman, Serge ; Herley, Cormac ; Oorschot, P. C. van: Markets for zero-day exploits: ethics and implications. In: *NSPW '13: Proceedings of the 2013 New Security Paradigms Workshop*, 2013. – ISBN 978-1-4503-2582-0

[14] Ikinci, Ali ; Holz, Thorsten ; Freiling, Felix C.: Monkey-Spider: Detecting Malicious Websites with Low-Interaction Honeyclients. In: *Sicherheit 2008 – Sicherheit, Schutz und Zuverlassigkeit. Beitrage der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft fur Informatik e.V. (GI)*, 2008, S. 407–422. – ISBN 978-3-88579-222-2

[15] InternetLiveStats.com: *Total number of Websites.* – URL https://www.internetlivestats.com/total-number-of-websites/. – Zugriffsdatum: 21.12.2020, 19:00

[16] Jacewicz, Pawel ; Jantura, Jaroslaw ; Kijewski, Piotr ; Krzesniak, Pawel ; Lewandowski, Piotr ; Mielniczek, Marcin: *HoneySpider Network Capture-HPC NG.* – URL https://github.com/CERT-Polska/HSN-Capture-HPC-NG. – Zugriffsdatum: 21.12.2020, 18:00

[17] Jalayeri, Shahriyar: *MCEDP.* – URL https://github.com/jamu/MCEDP. – Zugriffsdatum: 21.12.2020, 18:00

[18] Kahana, Yoni ; Hulzinga, Sjoerd: *Security Has Become an Arms Race.* – URL https://www.cpomagazine.com/cyber-security/security-has-become-an-arms-race. – Zugriffsdatum: 21.12.2020, 22:00

[19] Khonji, Mahmoud ; Iraqi, Youssef ; Jones, Andrew: Phishing Detection: A Literature Survey. In: *IEEE Communications Surveys Tutorials* 4 (2013), Nr. 1, S. 2091 – 2121

[20] Le, Van L. ; Welch, Ian ; Gao, Xiaoying ; Komisarczuk, Peter: A Novel Scoring Model to Detect Potential Malicious Web Pages. In: *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012, S. 254–263. – ISBN 978-1-4673-2172-3

[21] Lin, Ying-Dar ; Lee, Chia-Yin ; Wu, Yu-Sung ; Ho, Pei-Hsiu ; Wang, Fu-Yu ; Tsai, Yi-Lang: *Active versus Passive Malware Collection*. 2014. – IEEE Computer Society

[22] Luber, Stefan ; Schmitz, Peter: *Was ist ein Exploit?*. – URL https://www.security-insider.de/was-ist-ein-exploit-a-618629/. – Zugriffsdatum: 26.12.2020, 20:00

[23] Mansoori, Masood: *miniC*. – URL https://github.com/Masood-M/miniC. – Zugriffsdatum: 21.12.2020, 18:00

[24] Mansoori, Masood ; Wei, Lai Q. ; Qiaowei, Ritchie L.: *YALIH (Yet Another Low Interaction Honeyclient)*. – URL https://github.com/Masood-M/yalih. – Zugriffsdatum: 21.12.2020, 18:00

[25] Mizzi, Adrian: *Return on Information Security Investment*. 2005. – University of Malta

[26] Mookhey, K. K.: *Common Security Vulnerabilities in e-commerce Systems*. – URL https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=efa45bfc-a6d6-48fd-a588-e07d6f44e7eb. – Zugriffsdatum: 21.12.2020, 22:00

[27] NASK/CERT Polska (Poland) ; National Cyber Security Centre (Netherlands): *Honeyspider Network 2.1*. – URL https://github.com/CERT-Polska/hsn2-bundle. – Zugriffsdatum: 21.12.2020, 18:00

[28] Nazario, Jose: *PhoneyC*. – URL https://github.com/honeynet/phoneyc. – Zugriffsdatum: 21.12.2020, 18:00

[29] Pohlmann, Norbert: *Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung.* Springer Vieweg, 2019. – ISBN 978-3-658-25398-1

[30] Puttaroo, Mohammad Ally R.: *A behavioural study in runtime analysis environments and drive-by download attacks.* 2017. – University of West London

[31] Rapid7: *What is a Honeypot? How it Increases Security.* – URL https://www.rapid7.com/de/cybersecurity-grundlagen/honeypots. – Zugriffsdatum: 21.12.2020, 21:00

[32] Rocaspana, Joan R.: *SHELIA: A Client HoneyPot For Client-Side Attack Detection.* 2007. – Vrije University Amsterdam

[33] Schwenkler, Thomas: *Sicheres Netzwerkmanagement.* Springer-Verlag Berlin Heidelberg, 2006. – ISBN 978-3-540-31287-1

[34] Seifert, Chrisitan ; welch, Ian ; Komisarczuk, Peter: *Improving Detection Speed and Accuracy with Hybrid Client*, Victoria University of Wellington, Dissertation, 2006

[35] Seifert, Christian: *HoneyC.* – URL https://www.honeynet.org/projects/old/honeyc/. – Zugriffsdatum: 21.12.2020, 18:00

[36] Seifert, Christian: *Cost-effective Detection of Drive-by-Download Attacks with Hybrid Client Honeypots*, Victoria University of Wellington, Dissertation, 2010

[37] Seifert, Christian ; Komisarczuk, Peter ; Welch, Ian: True Positive Cost Curve: A Cost-Based Evaluation Method for High-Interaction Client Honeypots. In: *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, 2009

[38] Seifert, Christian ; Welch, Ian ; Komisarczuk, Peter: Taxonomy of Honeypots / Victoria University of Wellington. 2006. – Forschungsbericht

[39] Shaikh, Siraj A. ; Chivers, Howard ; Nobles, Philip ; Clark, John A. ; Chen, Hao: Network reconnaissance. In: *Network Security* 11 (2008), Nr. 1, S. 12–16

[40] Shea, Ryan ; Wang, Haiyang ; Liu, Jiangchuan: Power Consumption of Virtual Machines with Network Transactions: Measurement and Improvements. In: *2014 IEEE Conference on Computer Communications, INFOCOM 2014*, 2014. – ISBN 978-14799-3360-0

[41] Spitzner, Lance: Honeypots: Catching the Insider Threat. In: *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003)*, 2003. – ISBN 978-0-7695-2041-4

[42] Statistisches Bundesamt (Destatis): *Erhebung über die Nutzung von Informations- und Kommunikationstechnologien (IKT) in Unternehmen(EVAS-Nr.52911)*. – URL https://www-genesis.destatis.de/genesis/. – Zugriffsdatum: 12.01.2021, 20:47, Datenlizenz Deutschland – Namensnennung – Version 2.0, www.govdata.de/dl-de/by-2-0

[43] Sun, Xiaoyan ; Wang, Yang ; Ren, Jie ; Zhu, Yuefei ; Liu, Shengli: Collecting Internet Malware Based on Client-side Honeypot. In: *2008 The 9th International Conference for Young Computer Scientists*, 2008

[44] Tanaka, Yasuyuki ; Kashima, Shingo: SeedsMiner: Accurate URL Blacklist-Generation Based on Efficient OSINT Seed Collection. In: *WI '19 Companion: IEEE/WIC/ACM International Conference on Web Intelligence - Companion Volume*, 2019, S. 250–255. – ISBN 978-1-4503-6988-6

[45] Taylor, Teryl ; Snow, Kevin Z. ; Otterness, Nathan ; Monrose, Fabian: Cache, Trigger, Impersonate: Enabling Context-Sensitive Honeyclient Analysis On-the-Wire. In: *Network and Distributed System Security Symposium 2016*, 2016

[46] Verber, Mark: *Estimating IT Staffing*. – URL https://verber.com/it-staffing/. – Zugriffsdatum: 20.01.2021. 23:00

[47] Vissers, Thomas ; Spooren, Jan ; Agten, Pieter ; Jumpertz, Dirk ; Janssen, Peter ; Wesemael, Marc V. ; Piessens, Frank ; Joosen, Wouter ; Desmet, Lieven: Exploring the ecosystem of malicious domain registrations in the .eu TLD. In: *Research in Attacks, Intrusions, and Defenses 20th International Symposium, RAID 2017*, 2017

[48] Wang, Jingguo ; Herath, Tejaswini ; Chen, Rui ; Vishwanath, Arun ; Rao, H. R.: Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. In: *IEEE Transactions on Professional Communication* 55 (2012), Nr. 4, S. 345 – 362

[49] Wang, Kathy: Using Honeyclients to Detect New Attacks. In: *RECON 2005*, 2005

[50] Wen, Sheng ; Zhou, Wei ; Zhang, Jun ; Xiang, Yang ; Zhou, Wanlei ; Jia, Weijia ; Zou, Cliff C.: Modeling and Analysis on the Propagation Dynamics of Modern Email

Malware. In: *IEEE Transactions on Dependable and Secure Computing* 11 (2014), Nr. 4, S. 361–374

[51] Workforce.com: *Ratio of IT Staff to Employees*. – URL https://www.workforce.com/news/ratio-of-it-staff-to-employees. – Zugriffsdatum: 20.01.2021, 23:00

[52] Yen, Tsai-Fa ; Heorhiadi, Victor ; Oprea, Alina ; Reiter, Michael K. ; Juels, Ari: An Epidemiological Study of Malware Encounters in a Large Enterprise. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014. – ISBN 978-1-4503-2957-6

[53] Zarras, Apostolis: The Art of False Alarms in the Game of Deception: Leveraging Fake Honeypots for Enhanced Security. In: *2014 International Carnahan Conference on Security Technology (ICCST)*, 2014. – ISBN 978-1-4799-3532-1

Erklärung zur selbstständigen Bearbeitung einer Abschlussarbeit

Gemäß der Allgemeinen Prüfungs- und Studienordnung ist zusammen mit der Abschlussarbeit eine schriftliche Erklärung abzugeben, in der der Studierende bestätigt, dass die Abschlussarbeit „— bei einer Gruppenarbeit die entsprechend gekennzeichneten Teile der Arbeit [(§ 18 Abs. 1 APSO-TI-BM bzw. § 21 Abs. 1 APSO-INGI)] — ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt wurden. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich zu machen."

Quelle: § 16 Abs. 5 APSO-TI-BM bzw. § 15 Abs. 6 APSO-INGI

Erklärung zur selbstständigen Bearbeitung der Arbeit

Hiermit versichere ich,

Name: _____

Vorname: _____

dass ich die vorliegende Bachelorarbeit – bzw. bei einer Gruppenarbeit die entsprechend gekennzeichneten Teile der Arbeit – mit dem Thema:

Client Honeypots: Einsatzmöglichkeiten in Unternehmen und Analyse des Nutzens

ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

_____	_____	_____
Ort	Datum	Unterschrift im Original