Duale Hochschule Sachsen
Staatliche Studienakademie Leipzig

Vergleich eines kommerziellen Intrusion-Prevention Systems und einer Open-Source-Lösung

Bachelorthesis

zur Erlangung der staatlichen Abschlussbezeichnung eines
Bachelor of Science (B. Sc.)

im Studiengang Informatik

Eingereicht von: Leon Baumgarten
Traupitzer Dorfstraße 23, 06729 Elsteraue
CS22-1
5002213

Erstgutachter: B.Sc. Oliver Hels
WBS IT-Service GmbH

Zweitgutachter: Diplom IT Carsten Nitsch
Duale Hochschule Sachsen

6. Juli 2025

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation und Problemstellung

Die Digitalisierung durchdringt unaufhaltsam alle Bereiche von Wirtschaft und Gesellschaft. Während sie Effizienzgewinne, neue Geschäftsmodelle und eine globale Vernetzung ermöglicht, schafft sie gleichzeitig eine ebenso wachsende wie komplexe Angriffsfläche für Kriminalität. Die Bedrohungslage im Cyberraum hat sich in den letzten Jahren dramatisch verschärft und ist von einer Randnotiz für IT-Spezialisten zu einer strategischen Herausforderung für Unternehmen jeder Größenordnung geworden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet die Lage in seinem jährlichen Bericht als „angespannt bis besorgniserregend“ und verweist auf eine zunehmende Professionalisierung und Arbeitsteilung in der cyberkriminellen Schattenwirtschaft . [1]

Die Angriffsvektoren sind vielfältig und reichen von Denial-of-Service-Angriffen (DoS), die gezielt die Nichtverfügbarkeit von Diensten herbeiführen, über die Infiltration von Netzwerken mittels Schadsoftware (Malware) wie Viren und Trojanern, bis hin zur aktiven Ausnutzung von Software-Schwachstellen durch Exploits. Insbesondere Ransomware-Angriffe, bei denen Daten verschlüsselt und nur gegen Lösegeld wieder freigegeben werden, haben sich zu einer der größten Bedrohungen für die deutsche Wirtschaft entwickelt. Laut einer Studie des Digitalverbands Bitkom entstanden hierdurch allein im Jahr 2024 Schäden in einer Höhe von 266,6 Milliarden Euro, wobei ein Großteil der Angriffe auf kleine und mittelständische Unternehmen (KMU) zielte. [3]

Gerade KMU stehen vor einer besonderen Herausforderung: Sie verfügen oft nicht über die gleichen finanziellen und personellen Ressourcen wie Großkonzerne, um sich umfassend zu schützen. Gleichzeitig sind sie aufgrund ihrer Rolle in Lieferketten und als Träger der regionalen Wirtschaft ein attraktives Ziel. Der traditionelle Schutz des Unternehmensnetzwerks durch eine reine Paketfilter-Firewall, die den Verkehr nur anhand von Ports und IP-Adressen kontrolliert, ist angesichts der modernen Bedrohungslage nicht mehr ausreichend. Angriffe finden heute oft auf der Anwendungsebene statt und verstecken sich im legitimen Datenverkehr, beispielsweise über den standardmäßigen Web-Port 443.

An dieser Stelle setzen Intrusion Prevention Systeme (IPS) an. Als Weiterentwicklung von Intrusion Detection Systemen (IDS), die Angriffe nur erkennen und melden, sind IPS in der Lage, bösartigen Datenverkehr aktiv zu analysieren, zu klassifizieren und in Echtzeit zu blockieren, bevor er Schaden im internen Netzwerk anrichten kann. Diese Systeme agieren als wachsame "Torwächter", die den Inhalt der Datenpakete tiefgehend inspizieren (Deep Packet Inspection) und mit bekannten Angriffsmustern (Signaturen) oder anormalem Verhalten abgleichen.

Für Unternehmen, die eine solche Schutztechnologie implementieren möchten, stellt sich eine grundlegende strategische Frage: Soll auf eine kommerzielle „All-in-One"-Lösung eines etablierten Herstellers gesetzt werden, oder kann eine flexiblere und potenziell kostengünstigere Open-Source-Lösung einen vergleichbaren Schutz bieten? Kommerzielle Produkte, oft als Next-Generation Firewalls (NGFW) vermarktet, versprechen eine hohe Integration, professionellen Support und eine einfache Verwaltung aus einer Hand. Demgegenüber stehen Open-Source-Alternativen, die durch Transparenz, Anpassbarkeit und den Wegfall von Lizenzgebühren überzeugen, jedoch oft ein höheres Maß an technischem Know-how in der Implementierung und Wartung erfordern.

1.2 Stand der Technik und Forschungslücke

Die vorliegende Arbeit positioniert sich exakt in diesem Spannungsfeld. Sie zielt darauf ab, den in der Praxis relevanten Entscheidungsprozess zwischen einem kommerziellen und einem Open-Source-System durch einen systematischen, technischen und praktischen Vergleich zu objektivieren.

Als Repräsentant für die kommerzielle Welt wird eine FortiGate 70F der Firma Fortinet herangezogen. Fortinet ist einer der weltweiten Marktführer im Bereich der Netzwerksicherheit. Die FortiGate-Serie integriert Firewall-, VPN-, und IPS-Funktionen in einer einzigen Hardware-Appliance, die durch den Einsatz spezialisierter Security Processors (SPs) eine hohe Performance verspricht. Die

Als Gegenstück wird OPNsense untersucht, eine weit verbreitete und aktiv weiterentwickelte Open-Source-Firewall-Distribution, die auf dem robusten Betriebssystem FreeBSD basiert. OPNsense kann auf Standard-Hardware betrieben werden und integriert für die IPS-Funktionalität das leistungsfähige Open-Source-Engine Suricata. Suricata ist ein hochperformantes IDS/IPS, das von der Open Information Security Foundation (OISF) entwickelt wird. Im Gegensatz zum kommerziellen Ansatz ist der Anwender hier selbst dafür verantwortlich, die Hardware zu dimen-

sionieren und die Regelwerke (Signaturen) aus verschiedenen freien oder auch kostenpflichtigen Quellen zu beziehen und zu verwalten.

Während es zahlreiche Marketing-Vergleiche und allgemeine Gegenüberstellungen von Vor- und Nachteilen beider Ansätze gibt, fehlt es an detaillierten, praxisorientierten und reproduzierbaren Vergleichsstudien. Oft bleiben solche Analysen an der Oberfläche und vergleichen lediglich Feature-Listen, ohne die tatsächliche Schutzwirkung und die betrieblichen Aspekte in einer kontrollierten Umgebung zu testen. Diese Arbeit schließt diese Lücke, indem sie nicht nur die theoretischen Konzepte, sondern die konkrete Implementierung und Leistungsfähigkeit von FortiGate und OPNsense in einem eigens aufgebauten Testlabor direkt gegenüberstellt.

1.3 Zielsetzung und Forschungsfragen

Das primäre Ziel dieser Bachelorarbeit ist es, eine fundierte und objektive Entscheidungsgrundlage vor allem für KMU zu schaffen, die vor der Wahl eines geeigneten IPS stehen. Es soll ermittelt werden, inwieweit die Open-Source-Lösung OPNsense eine technisch ebenbürtige und praktikable Alternative zum kommerziellen Marktführer FortiGate darstellt.

Um dieses Ziel zu erreichen, wird die Untersuchung von folgender zentraler Forschungsfrage geleitet:

Inwieweit kann das Open-Source-System OPNsense in Bezug auf Schutzwirkung, Performance und Verwaltungsaufwand eine effektive Alternative zur kommerziellen Next-Generation-Firewall FortiGate für den Einsatz in kleinen und mittelständischen Unternehmen darstellen?

Zur systematischen Beantwortung dieser Hauptfrage werden die folgenden untergeordneten Forschungsfragen untersucht:

Worin liegen die konzeptionellen und architektonischen Unterschiede bei der Implementierung der IPS-Funktionalität in der FortiGate-Appliance und dem OPNsense-System mit Suricata?

Wie effektiv erkennen und blockieren beide Systeme eine Reihe definierter, praxisnaher Angriffe aus den Kategorien Malware, Exploits und Denial-of-Service in einer kontrollierten Testumgebung?

Welche qualitativen Unterschiede bestehen hinsichtlich des Konfigurationsaufwands,

der Benutzerfreundlichkeit der Verwaltungsoberflächen und der Qualität der Protokollierungs- und Reporting-Funktionen?

Welche quantifizierbaren Auswirkungen hat die Aktivierung der IPS-Funktionen auf den Netzwerkdurchsatz und die Latenz bei beiden Systemen?

1.4 Aufbau der Arbeit

Die Struktur der vorliegenden Arbeit orientiert sich konsequent an der Beantwortung der formulierten Forschungsfragen.

Das erste Kapitel legt die theoretischen Grundlagen. Es wird ein Überblick über die aktuelle Bedrohungslage gegeben und die Funktionsweise sowie die technologischen Konzepte von Intrusion Detection und Prevention Systemen erläutert. Anschließend werden die beiden zu vergleichenden Systeme, FortiGate und OPNsense, mit ihren jeweiligen Architekturen und Besonderheiten vorgestellt.

Im zweiten Kapitel wird der Aufbau der Testumgebung detailliert beschrieben. Dies umfasst die Auswahl der Hardware- und Softwarekomponenten, die entworfene Netzwerkarchitektur sowie die grundlegende Konfiguration der beiden IPS-Systeme, um eine transparente und nachvollziehbare Testbasis zu schaffen.

Das dritte Kapitel widmet sich dem Testing. Hier werden die konkreten Testfälle, die zur Überprüfung der Schutzwirkung und Performance dienen, definiert und deren Durchführung systematisch protokolliert.

Die im Praxisteil gewonnenen Daten werden im vierten Kapitel ausgewertet. Zunächst werden die Testergebnisse analysiert und anschließend die beiden Systeme anhand der zuvor definierten Kriterien wie Erkennungsrate, Performance und Benutzerfreundlichkeit verglichen.

Das fünfte und letzte Kapitel fasst die Erkenntnisse in einem Fazit zusammen, beantwortet die Forschungsfragen und gibt eine abschließende Bewertung sowie eine Handlungsempfehlung ab.

2 Theoretische Grundlagen

2.1 Bedrohungslage

Die Kernaufgabe eines jeden technischen Sicherheitssystems, insbesondere eines Intrusion Prevention Systems (IPS), ist die Erkennung und Abwehr konkreter Angriffe. Eine systematische Analyse und ein aussagekräftiger Vergleich solcher Systeme, wie er in dieser Arbeit angestrebt wird, setzen daher zwingend ein klares Verständnis der zu bekämpfenden Bedrohungen voraus.

Bevor die Fähigkeiten der Testsysteme praktisch evaluiert werden können, muss dieses theoretische Fundament geschaffen werden. Aus diesem Grund konzentriert sich dieser Abschnitt auf drei fundamentale Angriffskategorien, die für die Prüfung eines IPS zentral sind: Denial-of-Service-Angriffe, die Infiltration durch Malware und die Ausnutzung von Exploits.
Die nachfolgenden Unterkapitel widmen sich jeweils einer dieser Kategorien. Es werden die technischen Grundlagen, gängige Varianten und die charakteristischen Merkmale erläutert, anhand derer ein Schutzsystem den jeweiligen Angriff erkennen kann. Dieses Wissen ist die Voraussetzung, um die Konfiguration der Systeme im Testaufbau nachzuvollziehen und die Ergebnisse der praktischen Tests zu analysieren. [4]

2.1.1 Denial-of-Service-Angriff

Ein Denial-of-Service-Angriff (DoS), oder in seiner heute weitaus verbreiteteren Form als Distributed-Denial-of-Service-Angriff (DDoS), zielt fundamental auf die Beeinträchtigung der Verfügbarkeit eines IT-Dienstes ab. Das Ziel ist die Sabotage des regulären Betriebs, indem die endlichen Ressourcen des Zielsystems gezielt erschöpft werden. Bei einem DDoS-Angriff wird diese Überlastung durch eine Vielzahl kompromittierter Systeme, einem sogenannten Botnetz, gleichzeitig herbeigeführt. Diese massive Parallelisierung macht eine simple Abwehr durch das Blockieren einzelner IP-Adressen praktisch unmöglich.

Technisch lassen sich diese Angriffe in drei Hauptkategorien unterteilen, die auf unterschiedliche Schichten des OSI-Modells abzielen:

Volumetrische Angriffe (Schicht 3/4): Diese Angriffe zielen darauf ab, die gesamte zur Verfügung stehende Netzwerkbandbreite der Internetanbindung des Ziels zu sättigen. Eine Flut von Paketen wird an ein Ziel gerichtet. Ein klassisches Beispiel ist der UDP-Flood, bei dem eine riesige Menge an UDP-Paketen an zufällige Ports des Zielsystems gesendet wird. Da UDP ein verbindungsloses Protokoll ist, muss der Server für jedes eingehende Paket prüfen, ob eine Anwendung auf dem Port lauscht, und eine ICMP-Antwort "Destination Unreachable"generieren, was seine Ressourcen bindet. Ein ICMP-Flood (oder Ping-Flood) funktioniert nach einem ähnlichen Prinzip, indem er das Ziel mit ICMP-Echo-Request-Paketen überflutet und es zwingt, eine ebenso große Anzahl von Echo-Reply-Paketen zu senden. Das primäre Ziel ist hier die reine Masse an Traffic.

Protokoll-Angriffe (Schicht 4): Diese Angriffe nutzen Schwachstellen in der Implementierung von Netzwerkprotokollen aus, um die Ressourcen von Netzwerkkomponenten wie Firewalls oder Load Balancern zu erschöpfen. Der bekannteste Vertreter ist der TCP-SYN-Flood. Er missbraucht den drei-Wege-Handshake von TCP (SYN, SYN-ACK, ACK). Der Angreifer sendet eine hohe Zahl von SYN-Paketen, oft von gefälschten Quell-IP-Adressen. Das Zielsystem antwortet mit SYN-ACK und reserviert Ressourcen in seiner Verbindungstabelle (Backlog Queue) für die erwartete ACK-Antwort. Da diese Antwort niemals eintrifft, bleiben die Verbindungen "halboffen", bis die Tabelle voll ist und keine neuen, legitimen Verbindungsanfragen mehr angenommen werden können und überlastet ist.

Angriffe auf der Anwendungsebene (Schicht 7): Diese Angriffe sind subtiler und oft schwerer zu erkennen, da sie scheinbar legitimen Traffic imitieren. Sie zielen nicht auf die Netzwerkbandbreite, sondern auf die CPU- und Speicherressourcen des Servers ab. Beispiele hierfür sind das wiederholte Anfordern sehr großer Dateien oder das Ausführen komplexer Suchanfragen über eine Website, die serverseitig aufwändige Datenbankoperationen auslösen. Auch Angriffe auf Login-Schnittstellen durch massenhafte POST-Requests oder das Ausnutzen rechenintensiver API-Endpunkte fallen in diese Kategorie. Da diese Angriffe oft mit einer relativ geringen Datenrate auskommen, können sie unter dem Radar traditioneller, rein volumetrisch arbeitender Schutzsysteme hindurchgehen.
[4, 5]
Für ein Intrusion Prevention System besteht die Herausforderung darin, die Muster dieser unterschiedlichen Angriffsarten von legitimen Lastspitzen zu unterscheiden und sie präzise zu blockieren, ohne den regulären Nutzerverkehr zu beeinträchtigen.

2.1.2 Malware

Der Begriff Malware, eine Kurzform für "malicious software", dient als Oberbegriff für jegliche Art von Software, die mit der Absicht entwickelt wurde, auf einem Computersystem unerwünschte oder schädliche Aktionen auszuführen, Daten zu entwenden oder unautorisierten Zugriff zu erlangen. Die Ziele sind dabei vielfältig und reichen vom Diebstahl sensibler persönlicher oder geschäftlicher Informationen über die Störung von Betriebsabläufen, bis hin zur vollständigen Übernahme der Kontrolle über ein System, um es beispielsweise als Teil eines Botnetzes für DDoS-Angriffe zu missbrauchen. Die Infektion eines Netzwerks erfolgt oft mit einem mehrstufigen Prozess.

Zuerst muss die Malware auf das Zielsystem gelangen (Zustellung), was meist durch das Öffnen von manipulierten E-Mail-Anhängen (Phishing), das Klicken auf Links zu kompromittierten Websites (Drive-by-Downloads) oder über infizierte externe Speichermedien geschieht. Anschließend wird die Malware durch eine Benutzerinteraktion oder eine Sicherheitslücke aktiviert (Ausführung) und installiert sich fest im System, um einen Neustart zu überdauern (Persistenz). In vielen Fällen kontaktiert die Schadsoftware danach einen externen Command-and-Control-Server des Angreifers, um Anweisungen zu empfangen oder gestohlene Daten zu übermitteln.

Je nach Vorgehensweise und primärer Funktion lässt sich Malware in verschiedene Haupttypen klassifizieren, deren Grenzen jedoch zunehmend verschwimmen. Eine grundlegende Unterscheidung ist für das Verständnis der Bedrohungslandschaft unerlässlich.

Viren:
Klassische Viren sind Programmsegmente, die sich nicht eigenständig ausführen können, sondern eine legitime, ausführbare Wirtsdatei benötigen, um sich zu verbreiten. Sobald der Nutzer diese infizierte Datei startet, wird auch der virale Code aktiviert, der sich dann in weitere Dateien auf dem System oder auf verbundenen Netzlaufwerken kopiert. Die Schadfunktion, die von der reinen Replikation bis zur Zerstörung von Daten reichen kann, wird erst durch diese Nutzerinteraktion ausgelöst.[1]

Würmer:
Im Gegensatz dazu sind Würmer eigenständige Schadprogramme, die sich aktiv und ohne Zutun des Nutzers über Netzwerke verbreiten. Sie nutzen gezielt Sicherheitslücken in Betriebssystemen oder Anwendungen aus, um sich von einem infizierten System auf andere, verwundbare Systeme zu replizieren. Dieser autonome Verbreitungsmechanismus kann zu einer extrem schnellen, kaskadenartigen Infekti-

onswelle führen, die ganze Unternehmensnetzwerke lahmlegt. Ein prominentes Beispiel hierfür ist der Wurm WannaCry, der 2017 die "EternalBlue"-Schwachstelle im SMB-Protokoll von Windows-Systemen ausnutzte, um sich weltweit zu verbreiten und auf den infizierten Systemen Ransomware zu installieren.[2]

Trojaner:
Trojaner, benannt in Anlehnung an das Trojanische Pferd der griechischen Mythologie, tarnen sich als nützliche oder legitime Software, um den Nutzer zur Installation zu bewegen. Sie enthalten jedoch eine versteckte, bösartige Funktion. Nach der Ausführung installieren sie oft eine Hintertür (Backdoor), die Angreifern einen permanenten und unbemerkten Fernzugriff auf das System ermöglicht. Solche Remote Access Trojans (RATs) erlauben es Angreifern, Daten zu stehlen, das System zu überwachen oder es als Teil eines Botnetzes für weitere Angriffe zu missbrauchen.[6]

Ransomware:
Eine besonders profitable und schädliche Form ist die Ransomware. Diese Malware verschlüsselt die Dateien des Opfers, sodass auf sie nicht mehr zugegriffen werden kann. Anschließend wird eine Lösegeldforderung angezeigt, meist zahlbar in Kryptowährungen, um die Anonymität der Täter zu wahren. In den letzten Jahren hat sich das Vorgehen zur sogenannten "Double Extortion"(doppelte Erpressung) weiterentwickelt. Hierbei werden die Daten vor der Verschlüsselung zusätzlich vom System des Opfers auf Server der Angreifer kopiert. Wird das Lösegeld nicht gezahlt, drohen die Täter nicht nur mit der permanenten Zerstörung der Daten, sondern auch mit deren Veröffentlichung.[7]

Spyware:
Davon abzugrenzen ist Spyware, deren Hauptziel es ist, verdeckt Informationen über den Nutzer, dessen Verhalten und die auf dem System gespeicherten Daten zu sammeln. Eine der bekanntesten Unterarten sind Keylogger, die jeden Tastaturanschlag protokollieren. Auf diese Weise können Angreifer sensible Informationen wie Passwörter, Kreditkartennummern oder private Nachrichten mitschneiden und an ihre Server übermitteln.

Durch die Analyse von bekannten Malware-Signaturen, das Erkennen von Anomalien im Protokollverfahren und das Blockieren von Verbindungen zu IP-Adressen und Domains können IPS-Systeme diese Bedrohungen erkennen und unterbinden.

2.1.3 Exploits

Der Begriff Exploit bezeichnet ein spezifisches Software-Fragment, einen Datenblock oder eine Befehlssequenz, die gezielt einen Programmierfehler oder eine konzep-

tionelle Schwachstelle in einem Computersystem oder einer Anwendung ausnutzt. Es ist entscheidend, zwischen der Schwachstelle, bei der es sich um einen passiven, latenten Fehler im Code handelt, und dem Exploit, dem aktiven Werkzeug zur Ausnutzung dieses Fehlers, zu unterscheiden. Das Ziel eines Exploits ist es, erhöhte Rechte zu erlangen (Privilege Escalation), beliebigen Code auf dem Zielsystem auszuführen (Arbitrary Code Execution) oder einen Denial-of-Service-Zustand auszulösen. Dies macht Exploits zu einem primären Vektor für den erstmaligen Einbruch in ein Netzwerk.[9]

Der Prozess eines Angriffs, der auf der Ausnutzung von Schwachstellen basiert, lässt sich in die sieben Phasen der Cyber Kill Chain unterteilen, die den Ablauf aus der Perspektive des Angreifers strukturieren. Die erste Phase ist die **Reconnaissance**, in der ein Angreifer Informationen über das Ziel sammelt, um potenzielle Angriffsvektoren zu finden. In der zweiten Phase, der **Weaponization**, wird ein passender Exploit-Code mit einer Nutzlast (Payload) – dem eigentlichen Schadcode – gekoppelt. Anschließend erfolgt die **Delivery**, bei der der vorbereitete Exploit an das Zielsystem übermittelt wird, beispielsweise über eine Phishing-Mail oder einen verwundbaren Netzwerkdienst.

In der vierten Phase, der **Exploitation**, wird der Exploit-Code zur Ausführung gebracht und löst den Fehler in der verwundbaren Software aus. Dies ermöglicht die Ausführung des mitgelieferten Payload. Darauf folgt die **Installation**, in der die Payload Persistenz auf dem System etabliert, um nach einem Neustart noch auf dem Zielsystem vorhanden zu sein. In der sechsten Phase, **Command and Control** (C2), baut die installierte Schadsoftware eine ausgehende Verbindung zu einem vom Angreifer kontrollierten Server auf. Über diesen Kanal kann der Angreifer das System fernsteuern. In der letzten Phase, **Actions on Objectives**, verfolgt der Angreifer seine eigentlichen Ziele, wie zum Beispiel den Diebstahl von Daten, die Ausbreitung im internen Netzwerk, oder die Verschlüsselung von Systemen zur Erpressung von Lösegeld.[8]

Zero-Day-Exploit:
Die gefährlichste Kategorie sind Zero-Day-Exploits. Der Begriff „Zero-Day“ leitet sich aus der Perspektive des Softwareherstellers ab: Ab dem Moment, in dem ein Exploit für eine bisher unbekannte Schwachstelle aktiv ausgenutzt wird, hat der Hersteller null Tage Zeit gehabt, einen entsprechenden Sicherheitspatch zu entwickeln und bereitzustellen. Diese Unkenntnis aufseiten der Verteidiger verschafft den Angreifern ein kritisches Zeitfenster, in dem ihre Angriffe mit sehr hoher Wahrscheinlichkeit erfolgreich sind.
Die besondere Gefahr von Zero-Day-Exploits liegt in ihrer Fähigkeit, traditionel-

le, signaturbasierte Schutzmechanismen wie die meisten Antivirenprogramme und Intrusion Prevention Systeme vollständig zu umgehen. Da der Angriff neu und unbekannt ist, existiert keine Signatur, kein Muster und kein Hashwert, nach dem ein solches System suchen könnte. Der Exploit ist für die Verteidigungslinie demnach quasi unsichtbar.
Die Abwehr von Zero-Day-Angriffen erfordert daher fortschrittlichere Sicherheitsstrategien, die über die reine Signaturerkennung hinausgehen. Dazu gehören verhaltensbasierte Analyse (Heuristik) und Anomalieerkennung, bei denen ein System nicht nach bekannten Mustern, sondern nach ungewöhnlichem und potenziell bösartigem Verhalten sucht. Eine weitere wichtige Technik ist das Sandboxing, bei dem verdächtiger Code in einer isolierten, virtuellen Umgebung ausgeführt wird, um seine Aktionen zu beobachten, ohne das eigentliche System zu gefährden.

2.2 IDS / IPS Grundlagen

Nach der detaillierten Betrachtung der vielfältigen Bedrohungslandschaft im vorherigen Kapitel, werden nun die Systeme näher beleuchtet, die entwickelt wurden, um Netzwerke vor genannten Angriffen zu schützen. Während klassische Firewalls den Verkehr primär anhand von Adressen und Ports (Schicht 3 und 4 des OSI-Modells) filtern, gehen moderne Schutzmechanismen einen entscheidenden Schritt weiter, indem sie den Inhalt des Datenverkehrs analysieren. Im Zentrum dieser erweiterten Sicherheitsarchitektur stehen Intrusion Detection- und Intrusion Prevention-Systeme (IDS/IPS).
In den folgenden Absätzen werden dazu die theoretischen Grundlagen dieser Technologien erklärt. Es wird die evolutionäre Entwicklung vom rein passiven Erkennen eines Angriffs (Detection) hin zum aktiven Verhindern (Prevention) nachgezeichnet, um die grundlegenden Unterschiede und die Motivation hinter der Entwicklung von IPS zu beleuchten. Anschließend wird das technische Funktionsprinzip der Deep Packet Inspection (DPI) erläutert, das es diesen Systemen überhaupt erst ermöglicht, den Inhalt von Datenpaketen zu analysieren. Abschließend folgt die Vorstellung der verschiedenen Erkennungsmethoden, auf deren Basis ein System die Entscheidung trifft, ob es sich um legitimen oder bösartigen Datenverkehr handelt.

2.2.1 Vom passiven Detektieren zum aktiven Verhindern

Die historischen Vorläufer moderner Angriffserkennungssysteme sind die Intrusion Detection Systeme (IDS). Ihr grundlegendes Funktionsprinzip ist die der passiven Überwachung. Ein IDS wird im Netzwerk so implementiert, dass es eine Kopie des gesamten zu überwachenden Datenverkehrs erhält, ohne selbst Teil des aktiven Datenpfades zu sein. Technisch wird dies meist über einen sogenannten Mirror-Port (auch SPAN-Port genannt) an einem Netzwerk-Switch realisiert, der den gesamten

Verkehr eines oder mehrerer anderer Ports auf den Port des IDS spiegelt. Das IDS agiert somit wie ein Beobachter, der den Verkehr analysiert, ihn jedoch nicht direkt beeinflusst. Stellt das System eine potenzielle Bedrohung fest, die einer seiner vordefinierten Signaturen oder Verhaltensregeln entspricht, ist seine primäre Aufgabe das Auslösen eines Alarms. Dieser Alarm kann in Form eines Eintrags in einer Log-Datei, einer Benachrichtigung per E-Mail an einen Systemadministrator oder einer Meldung an ein übergeordnetes Security Information and Event Management (SIEM) System erfolgen. Die Kernfunktion eines IDS ist also die reine Detektion; es beantwortet die Frage: „Passiert hier gerade etwas Bösartiges?“ [10].

Die entscheidende Schwäche dieses passiven Ansatzes liegt in der systembedingten Latenz zwischen der Erkennung eines Angriffs und der Einleitung einer Gegenmaßnahme. Nachdem ein IDS einen Alarm ausgelöst hat, ist eine Reaktion erforderlich, um den Angriff zu stoppen. Diese Reaktion kann manuell durch einen Administrator erfolgen, der beispielsweise eine neue Regel in der Firewall konfiguriert, oder durch ein nachgeschaltetes, automatisiertes System. In der Zeit, die dieser Prozess unweigerlich in Anspruch nimmt, kann der Angriff sein Ziel bereits erreicht und erheblichen Schaden verursacht haben.

Um diese kritische Schutzlücke zu schließen wurden Intrusion Prevention Systeme (IPS) entwickelt. Im Gegensatz zu einem IDS wird ein IPS aktiv und ”in-line” im Netzwerk platziert und behebt damit dessen grundlegende Schwäche. Damit muss der gesamte Datenverkehr das IPS passieren, um sein Ziel zu erreichen.

Diese Positionierung ermöglicht es einem IPS, nicht nur zu erkennen, sondern auch unmittelbar zu handeln. Erkennt es einen Angriff, kann es eine Reihe von vordefinierten, automatisierten Aktionen durchführen. Die Palette dieser Reaktionsmöglichkeiten ist breit und reicht von dem einfachen Blockieren oder Verwerfen (Block/Drop) einzelner bösartiger Datenpakete, über das aktive Zurücksetzen von TCP-Verbindungen (Reset), bis hin zur reinen Alarmierung (Alert), bei der der Verkehr zu Testzwecken bewusst durchgelassen wird.[11, 12]

Darüber hinaus bieten viele Systeme erweiterte, oftmals herstellerabhängige Reaktionsmöglichkeiten. Dazu zählt beispielsweise die temporäre Sperrung der angreifenden IP-Adresse oder die Umleitung des Angriffs auf ein Ködersystem zur weiteren Analyse (Quarantäne). Die genaue Auswahl der verfügbaren Aktionen sind ein wesentliches Merkmal des jeweiligen Produkts. Welche dieser Funktionen von den in dieser Arbeit untersuchten Systemen, FortiGate und OPNsense, im Detail unterstützt werden, wird im Rahmen ihrer jeweiligen Vorstellung in Kapitel 2.3 erläutert.

2.2.2 Funktionsprinzip: Deep Packet Inspection (DPI)

2.2.3 Zentrale Erkennungsmethoden

2.3 Vorstellung der Systeme

2.3.1 Der kommerzielle Vertreter: FortiGate

2.3.2 Die Open-Source-Alternative: OPNsense

2.3.3 Synoptische Gegenüberstellung

3 Aufbau der Testumgebung

3.1 Physische und Virtuelle Komponenten

3.1.1 Test-Hardware

3.1.2 Virtualisierungssoftware

3.1.3 Virtuelle Maschinen (VMs)

3.2 Logische Netzwerkarchitektur

3.3 Grundkonfiguration der IPS-Systeme

3.3.1 Konfiguration der FortiGate 70F

3.3.2 Konfiguration von OPNsense

4 Testing

4.1 Definition der Testfälle

4.2 Durchführen der Tests

5 Auswertung

5.1 Analyse der Testergebnisse

5.2 Vergleich der IPS-Systeme

6 Fazit und Ausblick

7 Abkürzungsverzeichnis

BSI - Bundesamt für Sicherheit in der Informationstechnik
DoS - Denial of Service
DDoS - Distributed Denial of Service
KMU - Kleine und Mittelständige Unternehmen
IPS - Intrusion Prevention System
IDS - Intrusion Detection System
NGFW - Next Generation Firewall
VPN - Virtual Private Network
DPI - Deep Packet Inspection

8 Selbstständigkeitserklärung

Ich versichere, dass ich die vorliegende Hausarbeit 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. Die Arbeit wurde bisher in gleicher oder ähnlicher Form weder veröffentlicht, noch einer anderen Prüfungsbehörde vorgelegt.

Leipzig, 6. Juli 2025 _____

Leon Baumgarten

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik
Die Lage der IT-Sicherheit in Deutschland 2024
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html
Abgerufen am: 02.07.2025

[2] Bundesamt für Sicherheit in der Informationstechnik
Viren und Würmer
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Viren-und-Wuermer/viren-und-wuermer_node.html
Abgerufen am: 04.07.2025

[3] Bitkom e.V.
Wirtschaftsschutz 2024
https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf
Abgerufen am: 02.07.2025

[4] *Was ist ein DDoS-Angriff?*
https://www.cloudflare.com/de-de/learning/ddos/what-is-a-ddos-attack/
Abgerufen am: 02.07.2025

[5] Wesley M. Eddy
TCP SYN Flooding Attacks and Common Mitigations
https://www.rfc-editor.org/rfc/rfc4987.html
Abgerufen am: 03.07.2025

[6] *Was ist Schadsoftware?*
https://www.kaspersky.de/resource-center/definitions/what-is-malware
Abgerufen am: 04.07.2025

[7] European Union Agency for Cybersecurity
ENISA Threat Landscape 2023

https://www.enisa.europa.eu/publications/
enisa-threat-landscape-2023
Abgerufen am: 04.07.2025

[8] Wikipedia (2025)
Cyber Kill Chain
https://de.wikipedia.org/wiki/Cyber_Kill_Chain
Abgerufen am: 04.07.2025

[9] Wikipedia (2025)
Exploits
https://de.wikipedia.org/wiki/Exploit Abgerufen am: 04.07.2025

[10] Claudia Eckert
IT-Sicherheit: Konzepte - Verfahren - Protokolle
Walter de Gruyter GmbH & Co KG, 2014

[11] Open Information Security Foundation
Suricata Documentation – Rules.
https://docs.suricata.io/en/latest/rules/intro.html#action
Abgerufen am: 06.07.2025

[12] Karen Scarfone, Peter Mell (NIST)
Guide to Intrusion Detection and Prevention Systems (IDPS)
https://csrc.nist.gov/pubs/sp/800/94/final
Abgerufen am: 06.07.2025