Aegilock Security Whitepaper

Version 1.0 | Mai 2025

1. Einleitung

Die digitale Bedrohungslandschaft entwickelt sich stetig weiter. Aegilock wurde entwickelt, um Webanwendungen und digitale Infrastrukturen effektiv vor automatisierten Angriffen, bösartigen Bots und anderen schädlichen Zugriffen zu schützen. Dieses Whitepaper beschreibt die Sicherheitsarchitektur von Aegilock, die eingesetzten Schutzmechanismen sowie die Grundsätze des Datenschutzes und der Compliance.

2. Zielsetzung

Ziel von Aegilock ist es, einen hochgradig skalierbaren, zuverlässigen und flexiblen Schutz vor vielfältigen Bedrohungen wie DDoS-Angriffen, Credential Stuffing, Scraping und Brute-Force-Attacken zu bieten. Dabei steht die Minimierung von False Positives und eine optimale Nutzererfahrung für legitime Anwender im Vordergrund.

3. Systemarchitektur

3.1 Reverse Proxy Layer

Aegilock fungiert als Reverse Proxy, der sämtlichen eingehenden Traffic auf Webanwendungen analysiert und filtert. Dies ermöglicht eine zentrale Stelle zur Durchsetzung von Sicherheitsrichtlinien, ohne die Backend-Systeme zu belasten.

3.2 Sicherheitskomponenten

IP- und GeoIP-Blocklisten: Dynamische und statische Blockierung von IPs basierend auf Bedrohungsdaten und geografischen Parametern.

User-Agent-Filter: Validierung und Filterung von HTTP-Headern zur Erkennung von automatisiertem Traffic.

Rate Limiting: Schutz vor Überlastungsangriffen und Brute-Force durch Begrenzung der Anfragerate je Client.

Dynamische Verhaltensanalyse: Unser System erfasst typische Nutzeraktivitäten wie Mausbewegungen, Klickmuster, Scroll-Verhalten und die Interaktionsgeschwindigkeit. Bots können diese natürlichen Bewegungen kaum authentisch nachahmen.

Zusätzlich berücksichtigt unser Modell technische Merkmale wie Browsertyp (User-Agent), Geräte-Fingerabdrücke und die geografische Herkunft der Anfragen. So erkennen wir verdächtige Traffic-Quellen und manipulierte Umgebungen.

Echtzeit-Scoring: Die gesammelten Daten werden automatisch in Echtzeit ausgewertet. Jeder Besucher erhält einen Vertrauensscore, der aussagt, wie wahrscheinlich es sich um einen echten Nutzer oder einen Bot handelt.

Automatisierte Schutzmaßnahmen: Bei hoher Bot-Wahrscheinlichkeit reagiert Aegilock sofort – durch Blockierung, Captcha-Herausforderungen oder andere individuell konfigurierbare Sicherheitsmechanismen.

Logging und Monitoring: Detailliertes Monitoring aller relevanten Ereignisse zur Nachvollziehbarkeit und Auswertung.

4. Detaillierte Schutzmechanismen

4.1 IP- und GeoIP-Filtering

GeoIP-Filter erlauben gezielte Blockaden oder Einschränkungen basierend auf Ländern oder Regionen, die besonders häufig als Quelle von Angriffen identifiziert werden.

4.2 HTTP-Header-Validierung

Durch strenge Überprüfung von HTTP-Headern, insbesondere des User-Agent-Feldes, erkennt Aegilock automatisierte Tools und Bot-Traffic. Ungewöhnliche oder gefälschte Header lösen Warnungen oder Blockaden aus.

4.3 Rate Limiting

Eine granular konfigurierbare Begrenzung der Anfragerate schützt vor DDoS- und Brute-Force-Attacken. Die Limits können je nach Anwendungsfall und Sensitivität des Endpunkts individuell eingestellt werden.

4.4 Verhaltensbasierte Bot-Erkennung

Aegilock analysiert in Echtzeit das Verhalten von Clients, wie z. B. Klickmuster, Request-Intervalle und Navigationspfade, um Bots von menschlichen Nutzern zu unterscheiden. Verdächtige Aktivitäten werden automatisiert blockiert oder mit zusätzlichen Prüfungen versehen.

4.5 Sichere Kommunikation

Alle Verbindungen zwischen Client und Aegilock sowie zwischen Aegilock und Backend-Servern erfolgen ausschließlich verschlüsselt mittels TLS 1.3. Dies gewährleistet Vertraulichkeit und Integrität der übertragenen Daten.

5. Datenschutz & Compliance

Aegilock verarbeitet **keine personenbezogenen Daten**.

Durch diese Architektur stellt Aegilock sicher, dass der Schutz der Webanwendung gewährleistet ist, ohne Datenschutzbestimmungen zu verletzen oder personenbezogene Daten zu erfassen. Somit ist Aegilock vollständig DSGVO-konform im Sinne der Nichtverarbeitung personenbezogener Daten.

6. Deployment und Betrieb

6.1 Flexible Bereitstellung

Aegilock kann sowohl als SaaS-Lösung als auch als Self-Hosted-Variante in der eigenen Infrastruktur betrieben werden. Dies ermöglicht eine optimale Anpassung an individuelle Sicherheitsanforderungen und Compliance-Richtlinien.

6.2 Updates und Wartung

Regelmäßige Sicherheitsupdates sorgen für Schutz vor neuen Bedrohungen. Aegilock unterstützt Zero-Downtime-Deployments, um den Betrieb ohne Unterbrechungen zu gewährleisten.

6.3 Hochverfügbarkeit und Skalierbarkeit

Durch redundante Architekturen und horizontale Skalierung wird eine hohe Verfügbarkeit und Performance auch unter Last sichergestellt.

7. Incident Management & Support

Im Falle eines Sicherheitsvorfalls bietet Aegilock umfassende Analysewerkzeuge und detaillierte Logfiles für die Ursachenforschung. Ein erfahrenes Support-Team steht zur Verfügung, um schnell auf Vorfälle zu reagieren und mit individuellen Maßnahmen zu unterstützen.

8. Fazit

Aegilock stellt eine leistungsfähige, flexible und sichere Lösung zum Schutz moderner Webanwendungen dar. Die Kombination aus präziser Traffic-Analyse, bewährten Sicherheitsmechanismen und DSGVO-konformer Datenverarbeitung schafft Vertrauen und Sicherheit in einem sich ständig wandelnden Bedrohungsumfeld.

8.1 Vorteile für Ihr Business

Reduzierte Angriffsflächen: Automatisierte Angriffe wie Credential Stuffing, Scraping oder DDoS werden frühzeitig erkannt und abgewehrt.

Bessere Nutzererfahrung: Echte Nutzer surfen ungestört und ohne unnötige Sicherheitsabfragen.

Skalierbarkeit & Flexibilität: Unser KI-Modell lernt kontinuierlich aus neuen Daten und passt sich sich verändernden Angriffsmustern an.

Transparenz & Kontrolle: Sie behalten jederzeit die Übersicht über erkannte Bots und Schutzmaßnahmen über unser Dashboard.

9. Kontakt und weitere Informationen

Aegilock Security Team
Email: kontakt@aegilock.de
Web: https://aegilock.de