LINK11

MIT 6 SCHRITTEN IN EINER STUNDE ZUR VOLLSTÄNDIGEN WEB APPLICATION & API PROTECTION

Von der Backend-Definition bis zum Live-Gang

In der heutigen digitalen Landschaft bilden Webanwendungen und APIs das Tor zu Ihrem Unternehmen. Gleichzeitig stellen sie aber auch ein Hauptangriffsziel für Cyberkriminelle dar. Der proaktive und umfassende Schutz dieser kritischen Assets muss jedoch weder komplex noch zeitaufwendig sein: Mit der Link11 WAAP-Plattform lässt sich eine All-in-One-Lösung, die mehrschichtigen Schutz vor DDoS-Angriffen, bösartigen Bots, Zero-Day-Exploits und weiteren Bedrohungen bietet, unkompliziert in wenigen Schritten einrichten.

Diese schnelle und einfache Implementierung ermöglicht es IT-Teams, höchste Sicherheitsstandards sofort, ressourcenschonend und ohne langwierige Prozesse zu etablieren.

Der Einrichtungsprozess

1

Definition des Backend Services

Das Fundament der Verbindung

Zunächst erfolgt die Festlegung der Datenquelle für die WAAP. Es wird definiert, ob die Kommunikation über Domain-Namen oder IP-Adressen stattfindet, sowie das verwendete Protokoll (HTTP, HTTPS oder Port Bridge Mode). Dies gewährleistet die saubere Weiterleitung des Traffics an die Ursprungsserver.

2

Bereitstellung des Zertifikats & Konfiguration des Load Balancers

Sichere SSL-Terminierung

Zur Analyse von verschlüsseltem Traffic ist das Hochladen eines SSL-Zertifikats erforderlich. Dies kann durch Kopieren und Einfügen der Datei oder durch Extrahierung einer PFX File passieren.

Entscheidend: Das Zertifikat muss anschließend zwingend dem Load Balancer zugewiesen werden. Nur so kann das redundante Proxy-Netzwerk die Entschlüsselung und Prüfung auf allen Instanzen weltweit konsistent durchführen.

3

Anpassung der Security Policy

Individuelles Regelwerk

Durch Kopieren der „Default Policy“ wird eine solide Basis geschaffen. In dieser neuen Richtlinie erfolgt die Verknüpfung der Anwendungspfade mit dem in Schritt 1 definierten Backend-Service. Zudem lassen sich hier granulare Ausnahmen definieren oder kritische Bereiche (wie Login-Seiten) mit speziellen Schutzregeln versehen.

4

Erstellung der Server Group

Die logische Klammer

In diesem Schritt werden alle Komponenten zusammengeführt. Eine „Server Group“ wird erstellt, in der die exakten zu schützenden Domains oder Hosts hinterlegt sind. Diese Gruppe wird mit der angepassten Security Policy (aus Schritt 3) und dem konfigurierten Zertifikat (aus Schritt 2) verknüpft, um das Schutzprofil zu schließen.

5

Umstellung des DNS-Routings

Der Traffic-Switch

Der Besucherstrom wird auf den Schutzschild umgeleitet. Hierfür ist eine Änderung des A-Records der Domain im DNS-Management erforderlich, sodass dieser auf die IP-Adresse der Link11 WAAP zeigt. Ab diesem Zeitpunkt fließt jeder Aufruf durch die Filter der WAAP.

6

Veröffentlichung der Konfiguration

Go Live

Alle Einstellungen befinden sich zunächst in einer Staging-Umgebung, was finale Tests ermöglicht. Erst mit dem Klick auf „Publish“ wird das Regelwerk auf das weltweite Netzwerk übertragen und aktiviert. Sobald die DNS-Änderung propagiert ist, ist die Infrastruktur vollständig geschützt.

Ihre Vorteile auf einen Blick:
Maximaler Schutz bei minimalem Aufwand

- **Schnelles Setup:** Dank der intuitiven Oberfläche und simplen Prozessen ist die WAAP in nur einer Stunde vollständig einsatzbereit. Ohne langwierige Integrationsprojekte.
- **All-in-one-Schutz:** Profitieren Sie von einer leistungsstarken Kombination aus Web Application Firewall, Web DDoS Protection, Bot-Management und API-Security.
- **Automatisierte Echtzeit-Abwehr:** Unmittelbar nach der Einrichtung wird Ihr gesamter Datenverkehr in Echtzeit analysiert, um Bedrohungen sofort zu blockieren.
- **Ressourcenschonende Ausfallsicherheit:** Effektiver Schutz vor Ausfallzeiten, Reputationsschäden und finanziellen Verlusten bei minimalem administrativem Aufwand, der IT-Teams entlastet.
- **Nahtlose System-Integration:** Die WAAP lässt sich mühelos in bereits vorhandene Sicherheitsstrukturen einbinden.

In der heutigen komplexen und sich schnell entwickelnden Bedrohungslandschaft ist die Web Application and API Protection (WAAP-) Plattform von Link11 eine umfassende Lösung, die Ihre wertvollsten Web-Assets schützt. Durch die Integration von Web Application Firewall, Web DDoS Protection, robustem Bot Management und API Protection bietet Link11 einen beispiellosen Schutz mit einer optimierten Benutzererfahrung. Unsere speziell entwickelte Cloud-Infrastruktur, die durch eine 100-prozentige Betriebszeit-SLA und DSGVO-Konformität gestützt wird, garantiert, dass Ihr Unternehmen widerstandsfähig, konform und für legitime Benutzer immer zugänglich bleibt.

BUILT TO DEFEND. ALWAYS AT YOUR SIDE.

LINK11

Link11 GmbH | Lindleystr. 12 | 60314 Frankfurt | www.link11.com