

maxcluster

Sicherer Shop, ruhiger Schlaf

Moderne Sicherheitsstrategien
für Magento-Shops

Alfred Maier
maxcluster

GERMANY **DE**
Meet Magento™

22. Oktober 2026



Über mich

Alfred Maier

Senior Technical Sales Consultant | maxcluster GmbH

Ich begleite E-Commerce-Projekte rund um Hosting, Performance, Skalierbarkeit und Sicherheit – mit Fokus auf Magento, Shopware und geschäftskritische Shop-Infrastrukturen.



Seit 2016 bei maxcluster



Fokus: Beratung für E-Commerce-Hosting



Schnittstelle zwischen Technik, Vertrieb und Kunden



Ziel heute: *Security-Themen verständlich einordnen und praxisnah greifbar machen.*



EIN FIKTIVER SHOP

02:17 Uhr

Bestellungen laufen weiter.
Im Checkout liest ein fremdes Skript mit.

*Kann das Monitoring grün sein,
obwohl der Shop kompromittiert ist?*

Verfügbarkeit

Der Shop ist erreichbar. Kunden können bestellen.

Integrität

Code und Inhalte sollen vor unbefugten Änderungen geschützt sein.

Vertraulichkeit

Kundeninformationen sollen nur Berechtigte erreichen.

ABLAUF

Welche Aufgabe übernimmt was?

Ein möglicher Ablauf.
Schutzschichten wirken auch parallel.

- **1. Annäherung**
Unerwünschte Anfragen begrenzen
WAF und Bot Protection prüfen Webverkehr und automatisierten Missbrauch.
- **2. Eindringen**
Angriffswege schließen
Patchen und Zugangsschutz bilden die Basis.
WAF und Shield ergänzen sie.
- **3. Aktivitäten**
Hinweise auf Manipulationen finden
Malware-Scan untersucht Shopinhalte.
EDR betrachtet Aktivitäten am System.
- **4. Vorfall**
Schäden begrenzen und Betrieb zurückbringen
Incident Response koordiniert die Reaktion.
Disaster Recovery plant den Wiederanlauf.

VORBEREITUNG

Das Fundament vor dem Angriff

Hoster, Agentur und Betreiber vereinbaren die Aufgaben vor dem Ernstfall.

Komponenten kennen

Magento, Erweiterungen, Themes und Schnittstellen erfassen.

Software pflegen

Updates bewerten, testen und zügig einspielen.

Zugänge schützen

MFA, passende Rechte und gepflegte Konten.

Schutz aktivieren

Konfiguration und erfolgreiche Aktualisierung prüfen.

Alarme zuordnen

Ansprechpartner und Entscheidungsrechte festlegen.

Wiederaanlauf testen

Sicherungen und vollständige Shopabläufe prüfen.

WAF prüft Webanfragen

Web Application Firewall

Regeln prüfen Anfragen. Passende Treffer können blockiert oder gemeldet werden.

Virtuelles Patching

Eine Regel kann die Ausnutzung einer Lücke erschweren. Der Codepatch bleibt nötig.

Beispiel

Angriff auf eine verwundbare Shopfunktion.

Voraussetzung

Die Anfrage erreicht die WAF. Eine passende Regel ist aktiv.

Betrieb bei maxcluster

Managed WAF als vorgelagerte Schutzschicht. Regeln, Ausnahmen und Shopabläufe gemeinsam prüfen.

Warum Shops eine zusätzliche Schutzschicht brauchen

Angriffsfläche

Shop, Login, Suche, APIs, Plugins und Admin-Bereich sind öffentlich erreichbar.

01

Automatisierung

Bots testen Passwörter, Preise, Warenkörbe und Schwachstellen in hoher Frequenz.

02

Geschäftsfolgen

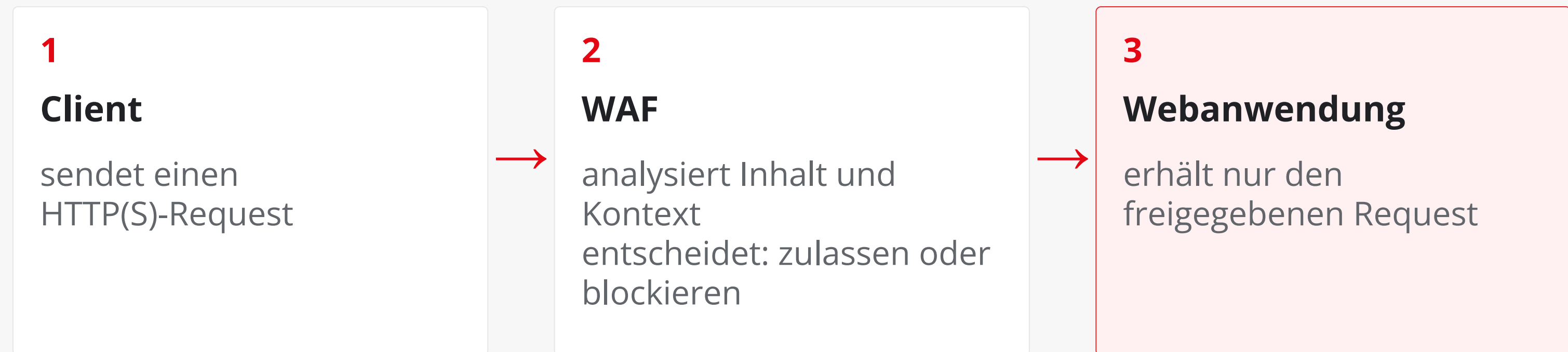
Ausfall, Betrug, Datenabfluss und schlechtere Conversion treffen direkt den Umsatz.

03

Die WAF reduziert die HTTP-Angriffsfläche – sie ersetzt weder sichere Software noch Kapazitätsschutz.

EINFACHE DEFINITION

Eine WAF kontrolliert HTTP(S)-Verkehr



Geprüft werden URL, Methode, Header, Cookies, Parameter und Body – nicht nur IP-Adresse und Port.

Was eine WAF gut kann – und wo sie endet

Gut geeignet

- bekannte Injection- und Exploit-Muster
- Path Traversal, Scanner, Protokollanomalien
- **virtuelles Patchen** bekannter Schwachstellen
- Request-basierte Regeln und Rate Limits

Kein verlässlicher Alleinschutz

- unbekannte Geschäftslogikfehler
- kompromittierte legitime Konten
- große volumetrische DDoS-Angriffe
- Fehler im Code, Rechtekonzept oder Backend

WAF-Betrieb braucht Kontext, Verantwortung und Know-how

Anwendungskontext

Kritische Funktionen, APIs und legitime Sonderfälle müssen bekannt sein.

Kundenmitwirkung

Shopbetreiber liefern Geschäftsprozesse, Ausnahmen und geplante Änderungen.

False Positives

Fehlentscheidungen können Login, Suche, Checkout oder APIs beeinträchtigen.

Regelpflege

Updates, neue Funktionen und neue Angriffe erfordern Tests und Anpassungen.

Ressourcen & Betrieb

Prüfung, Logging und Fehlerfälle beeinflussen Leistung und Verfügbarkeit.

Know-how & Dokumentation

Wissen, Zuständigkeiten und Änderungen müssen im Team verankert sein.

BOT-SCHUTZ

Bot-Protection ist kein Automatikmodus.

- 01 Deklarierte Bots: Googlebot, GPTBot oder ClaudeBot weisen sich über den User-Agent aus – dieser bleibt jedoch fälschbar.

- 02 Verhaltens-Bots: Scraper und Scanner erkennt man erst an Request-Mustern über Zeit.

- 03 Angriffs-Bots: DDoS-Botnetze verteilen Last; lokale Logs zeigen nur den HTTP-Ausschnitt.

Bot-Protection = automatisierte Zugriffe erkennen, bewerten und begrenzen.

Individuelle Bot-Erkennung bindet Daten, Zeit und Fachwissen

Datenbasis

Logs, Real-IP, relevante Felder und ausreichende Beobachtungszeiträume.

Normalverhalten

Crawler, APIs, Kampagnen und Lastspitzen von schädlichen Bots trennen.

Kundenmitwirkung

Erwünschte Bots, Geschäftsprozesse und Ausnahmen gemeinsam bewerten.

Scenario-Entwicklung

Analyse, Schwellenwerte, Umsetzung, Tests und Dokumentation binden Zeit.

Know-how-Transfer

Log-- und Angriffswissen muss in mehreren Teams verfügbar sein.

Dauerhafte Pflege

Simulation, Metriken und Reviews führen zu wiederholtem Nachjustieren.

Bot Protection

Verhalten, Häufigkeit und weitere Signale helfen, schädliche Automation zu erkennen.

Beispiel: Credential Stuffing

Ein Bot probiert gestohlene Login-Kombinationen. Die Funktion selbst arbeitet korrekt.

Mögliche Reaktion

Begrenzen, zusätzlich prüfen oder blockieren.

Erwünschte Bots

Suchmaschinen, APIs und Integrationen berücksichtigen.

Konten bleiben eine eigene Aufgabe

Bot-Schutz ergänzt MFA und Zugangsschutz. Wirkung und Ausnahmen hängen vom eingesetzten Produkt ab.

Schutz direkt in Magento

Eine Magento-spezifische Web Application Firewall als Modul im Shop.

WAF vor Magento

Eine vorgelagerte WAF filtert Webanfragen, bevor sie die Anwendung erreichen.

Shield in Magento

Shield prüft Webanfragen direkt im Magento-Kontext anhand aktiver Regeln.

Magento im Fokus

Vorhandene WAFs können den spezialisierten Schutz ergänzen.

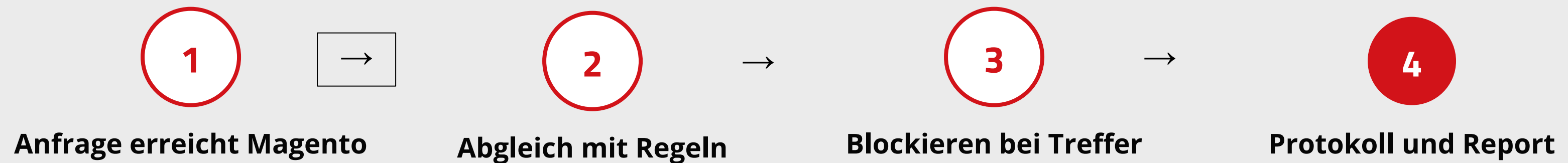
Wirksam betreiben

Aktives Modul, gültige Lizenz, geladene Regeln und klare Verantwortung.

SHIELD

Sansec Shield: Prüfung im Magento

Shield prüft die Anfrage im Magento-Kontext. Eine passende Regel kann den Webangriff blockieren.



Regeln aktualisieren sich über Magento Cron. Erfolgreiche Synchronisation, Modulpflege und Shoptests gehören zum Betrieb.

HERSTELLERBEISPIEL

StyleSmuggler: Zeit für den Patch gewinnen

05.09.2026 00:40

Erster (weltweit) bekannter Fall von StyleSmuggler

05.09.2026 09:15

SansecShield Support verteilt Regelset gegen StyleSmuggler

Ein Zeitgewinn bei diesem Angriff

Eine aktive, passende Regel kann das Patchfenster absichern. Keine garantierte Reaktionszeit für künftige Lücken.

06.09.2026: keine offiziellen Patches verfügbar

CVE-2026-75650. Schutzregel und Codepatch beschreiben unterschiedliche Maßnahmen.

Es herrscht große Verunsicherung bei Shopbetreibern.

07.09.2026: Adobe-Hotfix

Adobe veröffentlicht APSB26-146 und bestätigt aktive Ausnutzung.

Shield mit maxcluster in Betrieb nehmen

Lizenz und Einführung passend zur Magento-Umgebung abstimmen.

1

Passung und Lizenz klären

Magento-Umgebung und benötigten Umfang mit der maxcluster-Beratung besprechen.

2

Modul integrieren und aktivieren

Agentur oder Entwicklung einbinden. Modul, Lizenz und geladene Regeln prüfen.

3

Regelbetrieb und Shopabläufe prüfen

Magento Cron, Synchronisation und Modulpflege kontrollieren. Login, Checkout und APIs testen.

4

Verantwortung für Meldungen festlegen

Ansprechpartner und Reaktionsweg zwischen Betreiber, Agentur und Hoster vereinbaren.

NACH DER ABWEHR

Erkennung bleibt nötig

Ein blockierter Request entfernt keine bestehende Manipulation.

Jetzt fragen wir: Was finden wir im Shop und was sehen wir am System?

Früherer Angriff

Der Shop kann schon vor der Aktivierung von Shield verändert worden sein.

Andere Eintrittswege

Gestohlene Zugänge oder andere Anwendungen benötigen eigenen Schutz.

Bestehende Manipulation

Verdächtige Inhalte und Aktivitäten brauchen eine Untersuchung.

Malware-Scan

Was wurde im Shop verändert?

Ein Scan sucht im festgelegten Prüfbereich nach Schadcode und verdächtigen Mustern.

Beispiele: manipulierte PHP-Dateien oder auffälliges JavaScript in Shopinhalten.

Prüfbereich

Dateien und je nach Lösung auch Datenbankinhalte.

Aussagekraft

Ein Report gilt für Prüfbereich und Prüfzeitpunkt.

ShopSecurity bei maxcluster

Sansec eComscan untersucht Dateien und Datenbank.
Ein Fund braucht Bewertung und Bearbeitung.

Endpoint Detection and Response

Was geschieht auf dem System?

EDR liefert Hinweise zu Aktivitäten am geschützten System und unterstützt Untersuchung und Reaktion.

Beispiel: Ein Webprozess startet unerwartet ein weiteres Programm.

Perspektive

Ereignisse und Aktivitäten am geschützten Endpoint.

Reaktion

Umfang und Eingriffe hängen von Lösung und Freigabe ab.

Abdeckung bewusst bewerten

EDR ersetzt keine gesamte Browser-Sicht und keine personell organisierte Alarmbearbeitung.

Alarm: Wer koordiniert jetzt?

Ein konkreter Hinweis braucht Verantwortliche, technische Entscheidungen und Kommunikation.

1

Koordination übernehmen

Hoster, Agentur und Betreiber verbinden. Zuständige Fachleute nach Bedarf hinzuziehen.

2

Schäden begrenzen und Spuren sichern

Betroffene Zugänge oder Komponenten gezielt eingrenzen. Wichtige Logs und Zustände erhalten.

3

Ursache und Umfang klären

Angriffsweg schließen. Betroffene Schwachstellen und Zugänge entsprechend dem Befund bearbeiten.

4

Geprüften Betrieb freigeben

Sicherheitsprüfung und Shoptests verbinden. Nach dem Wiederanlauf weiter beobachten.

Disaster Recovery bringt den Shop zurück

Backups liefern Datenstände. Der geplante Wiederanlauf verbindet Daten, Systeme und Geschäftsabläufe.

1

Sicherungen schützen

Unveränderliche Sicherungen und räumlich getrennte Kopien stärken die Datenbasis.

2

Geeigneten Zustand auswählen

Ein erfolgreicher Backup-Lauf belegt noch keinen sauberen Shopzustand.

3

Abhängigkeiten wiederherstellen

Code, Daten, Konfiguration, Zugänge, Zahlungen und Schnittstellen berücksichtigen.

4

Den vollständigen Shop testen

Checkout und benötigte Anbindungen prüfen. Ein Restore holt abgeflossene Daten nicht zurück.

ZIELE FÜR DEN WIEDERANLAUF

RPO: Datenstand. RTO: Zeit.

Fiktives Planungsbeispiel. Diese Werte dienen zur Veranschaulichung und sind keine Leistungszusagen.

14:45 Datenstand. 15:00 Unterbrechung. 17:00 Wiederanlauf.

Voraussetzung: Der gewählte Datenstand ist geeignet und der vollständige Wiederanlauf wird geprüft.

RPO: höchstens 15 Minuten zurück

Wie weit darf der nutzbare Datenstand vor dem vereinbarten Bezugspunkt liegen?

RTO: höchstens 2 Stunden

Wie lange darf es bis zum vereinbarten Shopbetrieb dauern?

UNSER FIKTIVER SHOP

Zurück zum geprüften Shop

Um 02:17 Uhr war der Shop erreichbar und sein Checkout manipuliert.

Die Freigabe braucht mehr als ein grünes Verfügbarkeitsmonitoring.

Ursache bearbeitet

Angriffsweg, Umfang und betroffene Zugänge sind geprüft und behandelt.

Shopzustand geprüft

Code, Inhalte und Konfiguration stammen aus einem geeigneten Zustand.

Geschäftsabläufe getestet

Checkout, Zahlungsrückmeldungen und Anbindungen funktionieren. Beobachtung läuft weiter.

maxcluster verbindet die Bausteine

Die Wirkung entsteht aus aktiven Funktionen und vereinbarten Aufgaben mit Agentur und Betreiber.

Managed WAF

Erkannte Webangriffe vor der Anwendung filtern.

Sansec Shield

Magento-spezifische Regeln direkt im Shop.

ShopSecurity

eComscan prüft Dateien und Datenbank auf Schadcode.

Geschützte Backups

Unveränderliche und räumlich getrennte Sicherungen.

Erreichbare Fachleute

Linux-Administratoren und technischer Support.

Vereinbarter Betrieb

Aktivierung, Zuständigkeit und Service-Level abstimmen.

EUER NÄCHSTER SCHRITT

Drei Fragen für euer Team

Jede offene Antwort wird zu einer konkreten Aufgabe mit Verantwortlichem.

Aktiv? Zuständig? Getestet?

Welche Schutzfunktionen sind aktiv?

Konfiguration, geladene Regeln und erfolgreiche Aktualisierung prüfen.

Wer patcht und wer reagiert?

Agentur, Hoster und Betreiber stimmen Aufgaben, Koordination und Vertretung ab.

Wann war der letzte vollständige Restore-Test?

Checkout und benötigte Anbindungen gehören dazu.

Fragen und Diskussion

Welcher Schutzbereich oder Betriebsablauf ist bei euch noch offen?



Euer Ansprechpartner

Alfred Maier



Kontakt

beratung@maxcluster.de

Sprich mit einem Experten

+49 (0) 5251 / 4141 30

Besuch uns online

www.maxcluster.de

15 Minuten für eure Fragen