M0111

AntiSpam-Master

Gambio-Spamschutz für Kontaktformular, Rückrufservice, Preisanfrage und Produktempfehlung - plus Bot-Schutz für die Kontenanlage. Mit unsichtbarem Formularwächter statt Rätselbild, gewichtetem Punktesystem gegen Fehlblockaden und Protokollansicht im Backe

Aktuellstes Release: 2,31
Kompatibel zu den Versionen: 4.6 bis 26.10

published
07.10.2026 21:03 Uhr

Allgemeine Hinweise zu unseren Modulen

Beachten Sie bei geplanten Shop-Updates, dass auch das Modulframework und auch die eingebauten Module zur jeweiligen Shopversion kompatibel sein müssen und stellen Sie ggf. sicher, dass entsprechende Updates für das Modul-Framework und auch für alle genutzten Module zur Verfügung stehen bevor Sie mit der Aktualisierung des Shops beginnen oder diese beauftragen. Wenn Sie die Aktualisierung Ihres Shops durch uns durchführen lassen, aktualisieren wir auch immer vorhandene Xycons-Module und das Modul-Framework, wenn diese für die neue Shop-Version verfügbar sind.

Auf dem Server muss die Servererweiterung IonCube verfügbar sein!
Kontaktieren Sie bitte Ihren Hoster. falls Sie nach der Installation einen Hinweis erhalten, dass IonCube nicht zur Verfügung steht.
Weiterführende Hinweise finden Sie auf unserer Homepage www.xycons.de

Zur Selbstinstallation beachten Sie die beigefügte Installationsanleitung.

Bitte beachten Sie: mit der Installation des Modul-Frameworks werden die beigefügten Lizenzbestimmungen und Haftungsregelungen ausdrücklich zur Kenntnis genommen und anerkannt!
Das Framework und unsere Module dürfen nicht installiert und nicht betrieben werden, wenn Sie diese Regeln nicht in vollem Umfang anerkennen!

Inhaltsverzeichnis

- M0111 AntiSpam-Master für Gambio

- Inhalt
- 1. WAS DAS MODUL LEISTET
- 2. WO SIE DAS MODUL FINDEN
- 3. IN SECHS SCHRITTEN EINGERICHTET
- 4. DAS SETUP IM EINZELNEN
- 4.1 Grundeinstellungen und Zähler
- 4.2 Der Formularschutz
- 4.3 Das Punktesystem
- 4.4 Der Formularwächter
- 4.5 Fremde Zeichensätze
- 4.6 Der Kontenanlageschutz
- 4.7 Die IP-Sperre
- 4.8 Betrieb und Aufbewahrung
- 5. DIE ERKENNUNGSWÖRTER PFLEGEN
- 5.1 Wörter ergänzen und entfernen
- 5.2 Warum "nur ganze Wörter" wichtig ist
- 5.3 Bekannte Kunden ausnehmen
- 6. DER FORMULARWÄCHTER IN DER PRAXIS
- 6.1 Nach dem Einschalten: einmal den Cache aufbauen lassen
- 7. DAS PROTOKOLL: WAS WURDE ABGEWEHRT?
- 7.1 Die häufigsten Gründe - Ihr wichtigstes Werkzeug
- 7.2 Die Vorgangsliste
- 7.3 Der Bereich Kontenanlage
- 7.4 Aufbewahrung und Datenschutz
- 8. WAS TUN, WENN ...
- 8.1 ... trotzdem Spam ankommt
- 8.2 ... ein echter Kunde geblockt wird
- 8.3 ... gar nichts mehr blockiert wird
- 9. WAS DAS MODUL NICHT LEISTEN KANN
- 10. SHOPUPDATE UND MODULPFLEGE
- 11. MODULTEXTE ÄNDERN

M0111 AntiSpam-Master für Gambio

Handbuch

Stand: 2026-10 (Modulversion 2.31) · (c) Xycons GmbH & Co. KG - www.xycons.de

---

Inhalt

1. 1. WAS DAS MODUL LEISTET
2. 2. WO SIE DAS MODUL FINDEN
3. 3. IN SECHS SCHRITTEN EINGERICHTET
4. 4. DAS SETUP IM EINZELNEN
5. 4.1 Grundeinstellungen und Zähler
6. 4.2 Der Formularschutz
7. 4.3 Das Punktesystem
8. 4.4 Der Formularwächter
9. 4.5 Fremde Zeichensätze
10. 4.6 Der Kontenanlageschutz
11. 4.7 Die IP-Sperre
12. 4.8 Betrieb und Aufbewahrung
13. 5. DIE ERKENNUNGSWÖRTER PFLEGEN
14. 5.1 Wörter ergänzen und entfernen
15. 5.2 Warum "nur ganze Wörter" wichtig ist
16. 5.3 Bekannte Kunden ausnehmen
17. 6. DER FORMULARWÄCHTER IN DER PRAXIS
18. 6.1 Nach dem Einschalten: einmal den Cache aufbauen lassen

19. 7. DAS PROTOKOLL: WAS WURDE ABGEWEHRT?
20. 7.1 Die häufigsten Gründe - Ihr wichtigstes Werkzeug
21. 7.2 Die Vorgangsliste
22. 7.3 Der Bereich Kontenanlage
23. 7.4 Aufbewahrung und Datenschutz
24. 8. WAS TUN, WENN ...
25. 8.1 ... trotzdem Spam ankommt
26. 8.2 ... ein echter Kunde geblockt wird
27. 8.3 ... gar nichts mehr blockiert wird
28. 9. WAS DAS MODUL NICHT LEISTEN KANN
29. 10. SHOPUPDATE UND MODULPFLEGE
30. 11. MODULTEXTE ÄNDERN

---

1. WAS DAS MODUL LEISTET

Wer einen Gambio-Shop betreibt, kennt das: Im Postfach und unter KUNDEN > E-MAILS sammeln sich Nachrichten, die niemand geschrieben hat, der etwas kaufen möchte. Werbung für Glücksspiel und Medikamente, Angebote für Suchmaschinenplatzierungen, Linklisten - eingetragen von Programmen, die den ganzen Tag nichts anderes tun, als Formulare auszufüllen. Dazwischen gehen echte Kundenanfragen unter.

Genau hier setzt der AntiSpam-Master an. Er schützt die vier Dialogformulare Ihres Shops:

- das **Kontaktformular**,
- den **Rückrufservice**,
- die Preisanfrage **"Woanders günstiger"**,
- die **Produktempfehlung** an einen Bekannten.

Dazu kommt der Schutz der **Anlage neuer Kundenkonten**. Denn nicht jedes neue Konto ist ein neuer Kunde: Viele werden automatisiert angelegt, um später den Shop für Werbung zu missbrauchen oder Ihre Kundenverwaltung zu fluten.

Das Modul arbeitet auf mehreren Ebenen gleichzeitig:

- Es erkennt einen **Formularroboter daran, wie er tippt** - unsichtbar, ohne dass Ihr Besucher ein Rätselbild lösen muss.
- Es prüft den **Inhalt** gegen eine mitgelieferte, aus echten Spam-Vorgängen gewonnene Erkennungsliste.
- Es prüft **Absenderadresse, Zeichensatz und Domainendung**.
- Es begrenzt, wie oft von **einer Internetadresse** aus Konten angelegt werden können.

Der Besucher bekommt in allen Fällen eine sachliche Meldung angezeigt. Jeder Vorgang wird festgehalten und lässt sich im Administrationsbereich nachlesen - dort sehen Sie nicht nur, was abgewehrt wurde, sondern auch, woran das Modul es erkannt hat. Genau daraus lässt sich ablesen, ob Ihr Shop womöglich zu streng eingestellt ist.

Der wichtigste Grundsatz vorweg: Eine geblockte Nachricht kommt nie an - auch dann nicht, wenn sie von einem echten Kunden stammte. Deshalb ist das Modul so ausgelegt, dass es im Zweifel lieber durchlässt als blockiert, und deshalb gibt es das Protokoll (Kapitel 7). Nehmen Sie sich nach der Einrichtung einmal zehn Minuten dafür - es ist gut investierte Zeit.

2. WO SIE DAS MODUL FINDEN

Das Modul hat zwei Anlaufstellen im Administrationsbereich Ihres Shops:

Wofür	Wo
Einrichten	XYCONS-MODULE > KUNDENKONTO / SETUPS, dort oben der Reiter **AntiSpam-Master**
Auswerten	KUNDEN > ANTISPAM-MASTER PROTOKOLL

Die Einrichtung finden Sie also nicht im Modul-Center des Shops, sondern in der Übersicht Ihrer Xycons-Module. Dort sind alle unsere Module als Reiter nebeneinander aufgeführt.

Der Menüpunkt für das Protokoll erscheint nur für Benutzer, die das Modul auch einrichten dürfen. Arbeiten in Ihrem Shop mehrere Personen mit eigenen Zugängen und soll eine davon das Protokoll einsehen können, geben Sie ihr unter KUNDEN > ROLLEN UND BERECHTIGUNGEN das Leserecht für dieses Modul. Sehen Sie den Menüpunkt nach einem Update gar nicht, hilft ein Leeren der Shop-Caches.

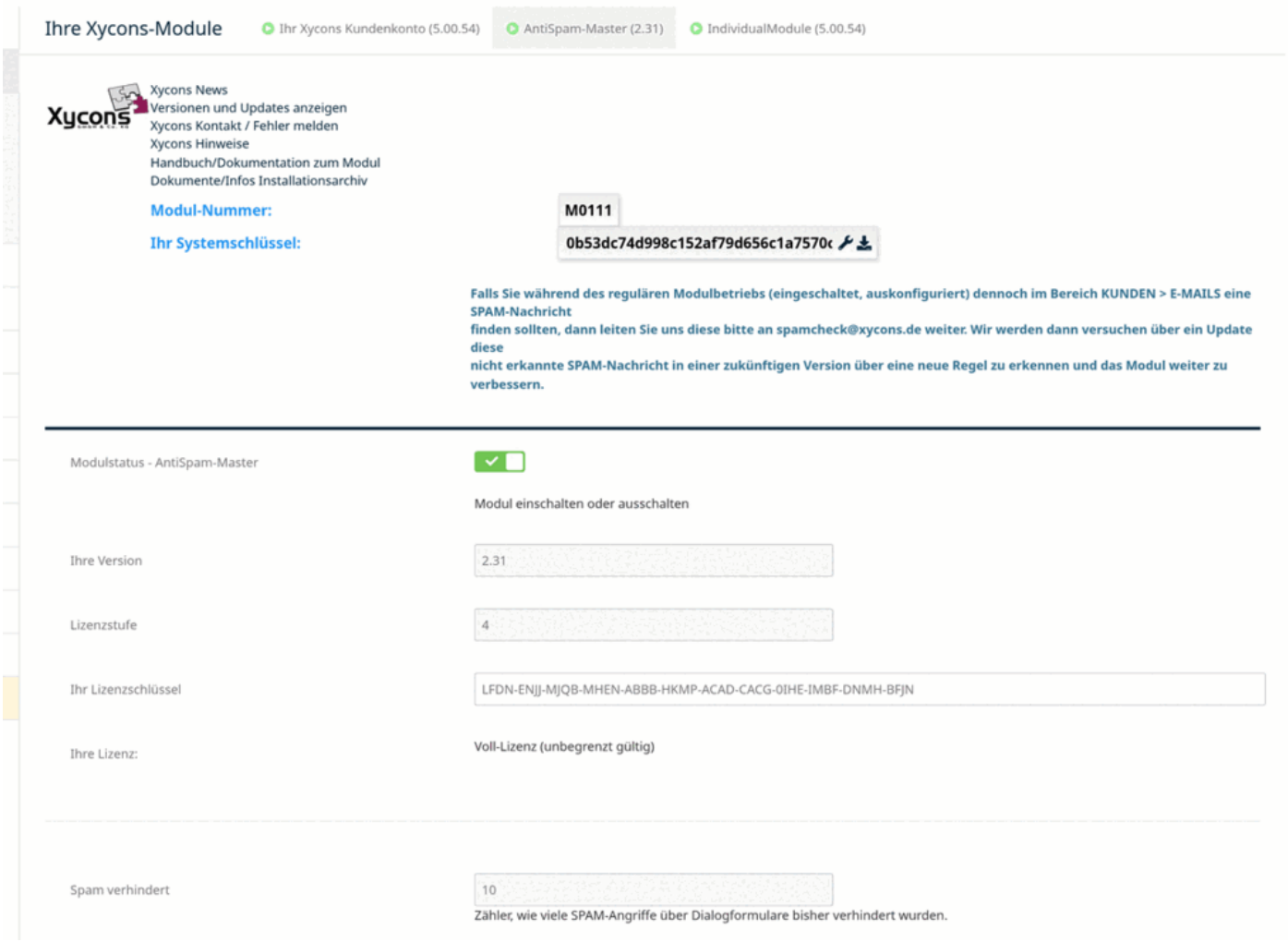

Abbildung 1: Der Kopfbereich des Setups. Oben die Reiter aller installierten Xycons-Module, darunter Modulstatus, Lizenzangaben und der Zähler der verhinderten Spam-Nachrichten.

3. IN SECHS SCHRITTEN EINGERICHTET

Wenn Sie es eilig haben: Diese sechs Schritte genügen für einen wirksamen Schutz. Die Einzelheiten stehen anschließend in Kapitel 4.

- **Schritt 1:** *Modulstatus - AntiSpam-Master* einschalten. Solange der Status auf "Nein" steht, ist jede weitere Einstellung wirkungslos.
- **Schritt 2:** *Formularwächter* einschalten und danach den Themecache neu aufbauen lassen (Kapitel 6). Das ist die wirksamste Einzelmaßnahme überhaupt und trifft echte Besucher nicht.
- **Schritt 3:** *Punktesystem* einschalten und die *Punkteschwelle* auf 3 belassen. Damit scheitert keine seriöse Anfrage mehr an einem einzelnen Reizwort.
- **Schritt 4:** *Kontenanlageschutz* einschalten, wenn Sie Bot-Konten in Ihrer Kundenverwaltung haben.
- **Schritt 5:** Die Erkennungsliste einmal in Ruhe durchsehen (Kapitel 5) und alles streichen, was in Ihrer Branche ein normales Wort ist.
- **Schritt 6:** Nach ein bis zwei Wochen das Protokoll unter KUNDEN > ANTISPAM-MASTER PROTOKOLL öffnen und prüfen, ob etwas zu Unrecht hängen geblieben ist. Erst dann lohnt es sich, an den Feinheiten zu drehen.

Bitte nicht überspringen: Schalten Sie das Modul nicht ein und vergessen Sie es dann. Ein Spamschutz, den niemand kontrolliert, blockiert irgendwann auch Bestellanfragen - und Sie erfahren es nicht, weil eine geblockte Nachricht eben nicht ankommt. Der eine Blick ins Protokoll nach zwei Wochen ersetzt jede Sorge.

4. DAS SETUP IM EINZELNEN

Hier ist jede Einstellung des Setups beschrieben - in der Reihenfolge, in der sie auf der Seite steht. Die Beschriftungen entsprechen genau denen im Shop, damit Sie jede Zeile wiederfinden.

4.1 Grundeinstellungen und Zähler

Einstellung	Bedeutung
Modulstatus - AntiSpam-Master	Der Hauptschalter. Steht er auf "Nein", findet *keine* Prüfung statt - unabhängig davon, was Sie sonst eingestellt haben. Auch die Protokollansicht zeichnet dann nichts mehr auf. *(Standard: Nein)* **Empfehlung:** nach dem Einrichten auf "Ja".
Ihre Lizenz:	Reine Anzeige, welcher Lizenztyp für Ihren Shop erkannt wurde. Hier ist nichts einzustellen.
Spam verhindert	Zähler: wie viele Spam-Nachrichten über die Dialogformulare bisher verhindert wurden. Der Zähler läuft über die gesamte Laufzeit weiter, auch wenn Sie das Protokoll leeren. *(Standard: 0)*
BOT-Konten verhindert	Derselbe Zähler für die Kontenanlage: wie viele automatisiert angelegte Konten abgewiesen wurden. *(Standard: 0)*

Die beiden Zähler beantworten die Frage, ob sich der Schutz lohnt, mit einer einzigen Zahl. Notieren Sie sich den Stand nach der Einrichtung - der Zuwachs nach vier Wochen ist meist überraschend deutlich.

4.2 Der Formularschutz

Diese Einstellungen gelten für die vier Dialogformulare - Kontakt, Rückruf, "Woanders günstiger" und Produktempfehlung.

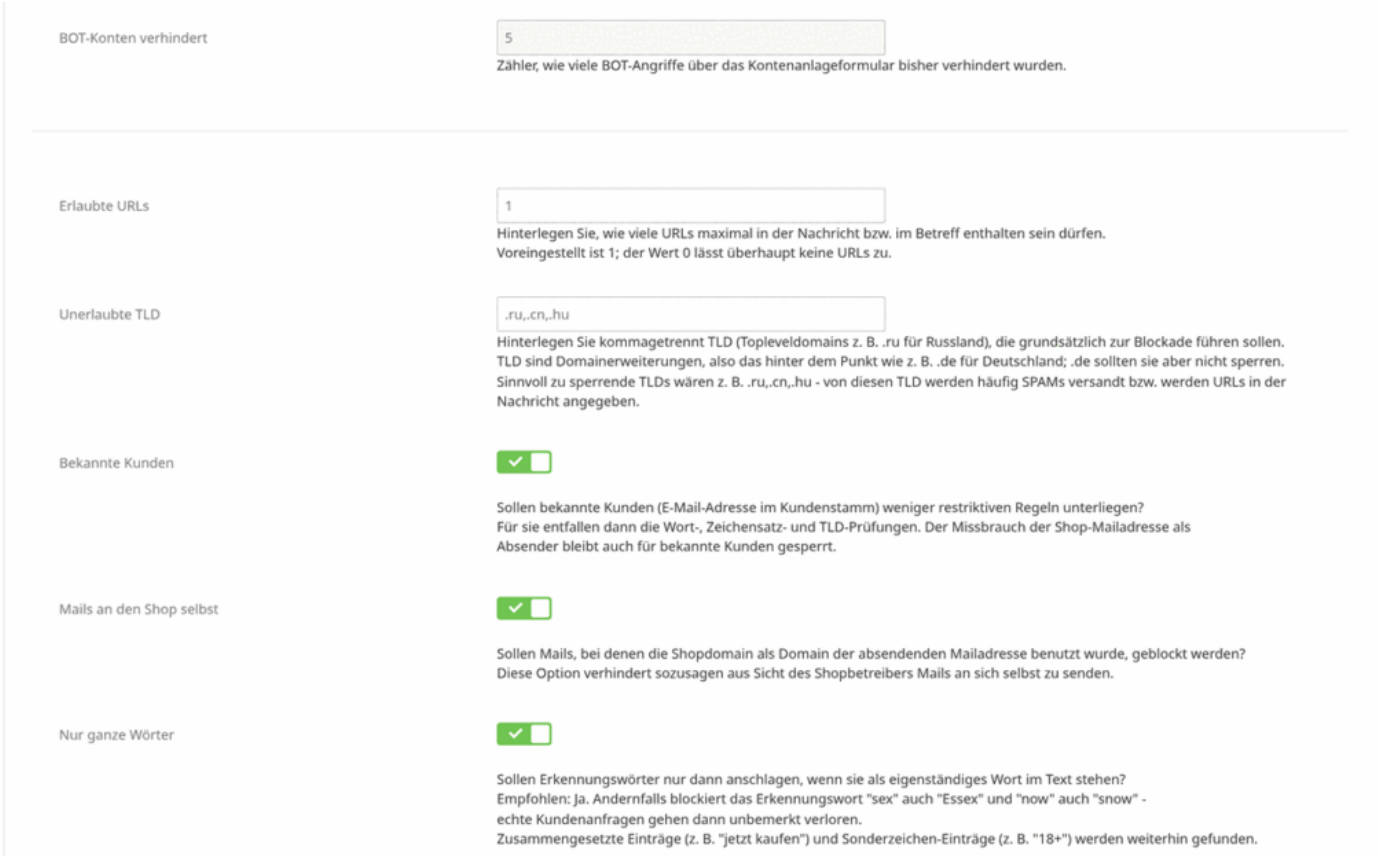

Abbildung 2: Die Einstellungen des Formularschutzes - von den erlaubten Internetadressen bis zur Wortgrenzen-Erkennung.

Einstellung	Bedeutung
Erlaubte URLs	Wie viele Internetadressen eine Nachricht höchstens enthalten darf. Werbenachrichten enthalten oft ganze Linklisten, echte Kundenanfragen selten mehr als eine Adresse. *(Standard: 1)* Der Wert 0 lässt überhaupt keine Adressen zu - das ist für die meisten Shops zu scharf, weil Kunden gern auf ein Produkt bei einem Mitbewerber verweisen.
Unerlaubte TLD	Kommagetrennte Liste von Domainendungen, die zur Blockade führen, wenn sie in der Nachricht, im Betreff, im Namen oder in der Absenderadresse vorkommen. *(Standard: .ru,.cn,.hu)* **Wichtig:** Sperren Sie hier keine Endung, aus deren Land Sie Kunden haben. Ein Shop, der nach Österreich und in die Schweiz liefert, darf *.at* und *.ch* niemals eintragen.

Bekannte Kunden	Sollen Absender, deren E-Mail-Adresse bereits in Ihrem Kundenstamm steht, milder behandelt werden? Bei "Ja" entfallen für sie die Wort-, Zeichensatz- und Endungsprüfungen. *(Standard: Ja)* **Empfehlung:** Ja. Ein bestehender Kunde soll Ihnen schreiben können, auch wenn er zufällig ein Reizwort verwendet. Der Missbrauch der Shop-Adresse als Absender bleibt auch für bekannte Kunden gesperrt.
Mails an den Shop selbst	Blockiert Nachrichten, bei denen die Absenderadresse die Adresse Ihres eigenen Shops ist. *(Standard: Ja)* Ein beliebter Trick: Der Absender trägt Ihre eigene Shop-Adresse ein, damit die Nachricht wie eine interne Mail aussieht und an Filtern vorbeikommt. Es gibt keinen legitimen Grund dafür - diese Prüfung blockiert immer, unabhängig von allen anderen Einstellungen.
Nur ganze Wörter	Sollen Erkennungswörter nur anschlagen, wenn sie als eigenständiges Wort im Text stehen? *(Standard: Ja)* **Empfehlung: unbedingt Ja.** Warum das so wichtig ist, steht in Abschnitt 5.2.
Blockierende Wörter (Formulare)	Die Erkennungsliste, kommagetrennt. Geprüft werden Nachricht, Betreff, Zusatzangaben und Name. *(Standard: die mitgelieferte Liste)* Wird das Feld leer gespeichert, stellt das Modul die mitgelieferte Liste wieder her - Sie können also nichts unwiederbringlich kaputt machen. Zur Pflege siehe Kapitel 5.

4.3 Das Punktesystem

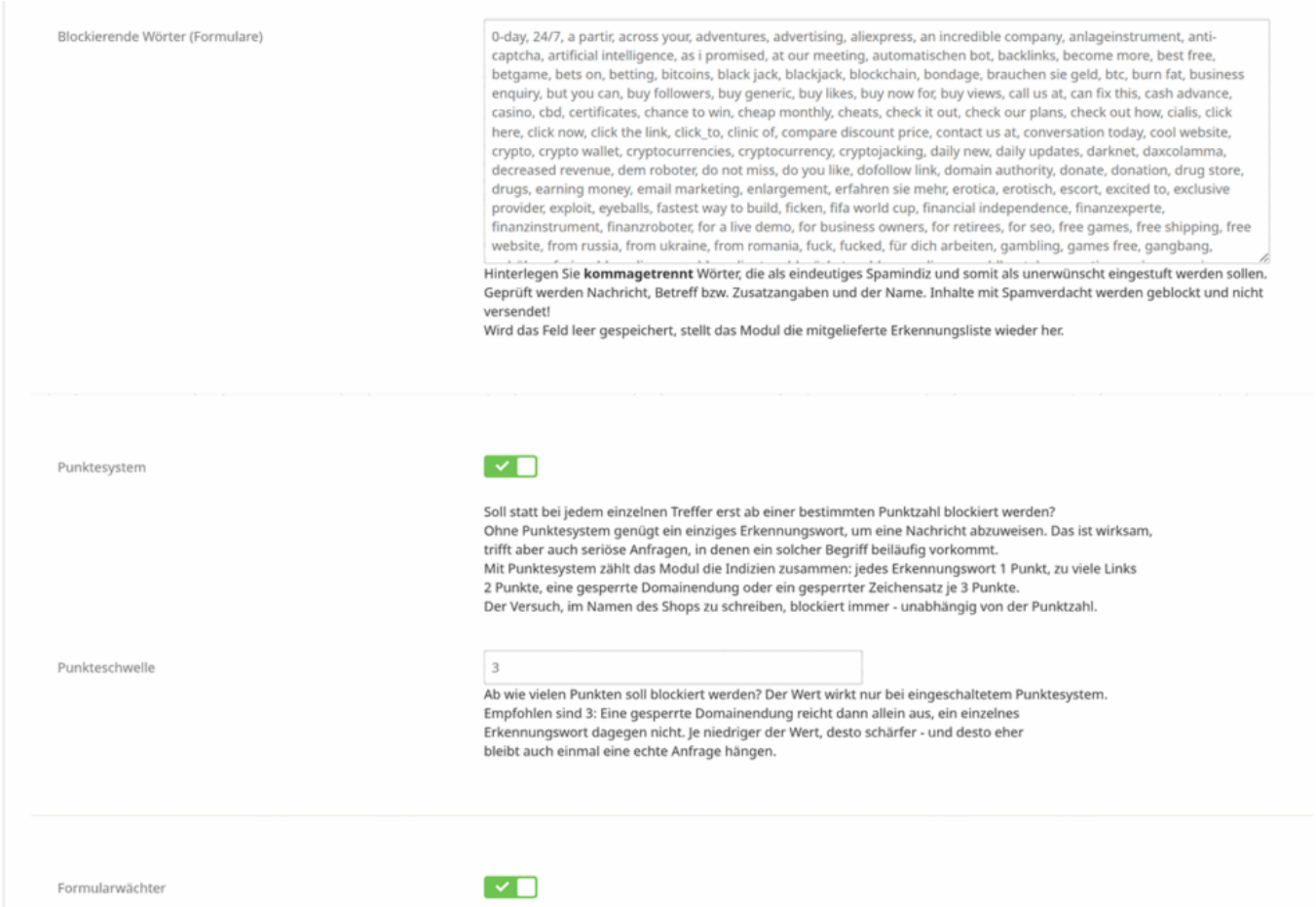

Abbildung 3: Die mitgelieferte Erkennungsliste, darunter Punktesystem, Punkteschwelle und der Formularwächter.

Einstellung	Bedeutung
Punktesystem	Soll erst ab einer bestimmten Punktzahl blockiert werden statt bei jedem einzelnen Treffer? *(Standard: Nein)* Ohne Punktesystem genügt ein einziges Erkennungswort, um eine Nachricht abzuweisen. Das ist wirksam, trifft aber auch die seriöse Anfrage, in der ein solcher Begriff beiläufig vorkommt. Mit Punktesystem zählt das Modul die Indizien zusammen: jedes gefundene Erkennungswort **1 Punkt**, zu viele Links **2 Punkte**, eine gesperrte Domainendung **3 Punkte**, ein gesperrter Zeichensatz **3 Punkte**, ein "Re:" im Betreff einer Erstanfrage **1 Punkt**. **Empfehlung: Ja.** Es ist das wirksamste Mittel gegen Fehlblockaden.

Punkteschwelle	Ab wie vielen Punkten blockiert wird. Wirkt nur bei eingeschaltetem Punktesystem. *(Standard: 3)* Bei 3 blockiert eine gesperrte Domainendung weiterhin allein, ein einzelnes Erkennungswort dagegen nicht mehr - erst drei zusammen, oder ein Erkennungswort plus zu viele Links. Je niedriger der Wert, desto schärfer, und desto eher bleibt auch einmal eine echte Anfrage hängen.

Der Versuch, im Namen des Shops zu schreiben, sowie ein Treffer des Formularwächters blockieren **immer** - unabhängig von Punktesystem und Schwelle. Das sind keine Verdachtsmomente, sondern Beweise.

4.4 Der Formularwächter

Einstellung	Bedeutung
Formularwächter	Soll zusätzlich geprüft werden, ob das Formular überhaupt von einem Menschen ausgefüllt wurde? *(Standard: Nein)* Zwei unsichtbare Prüfungen: ein für Besucher nicht sichtbares Eingabefeld, das nur ein Formularroboter ausfüllt, und ein Zeitstempel - wer ein Formular in Sekundenbruchteilen absendet, hat es nicht gelesen. Beides trifft echte Besucher nicht und funktioniert ohne Rätselbilder. **Empfehlung: Ja** - siehe aber unbedingt Kapitel 6 zum Themecache.
Mindestausfüllzeit (Sek.)	Wie viele Sekunden zwischen dem Aufbau des Formulars und dem Absenden mindestens vergehen müssen. Wirkt nur bei eingeschaltetem Formularwächter. *(Standard: 4)* Empfohlen sind 4 bis 8 Sekunden - so lange braucht auch ein schneller Mensch, um Name, E-Mail-Adresse und eine Nachricht einzugeben. Der Wert 0 schaltet die Zeitprüfung ab; das unsichtbare Feld bleibt dann weiterhin aktiv. Werte über 10 Sekunden sollten Sie meiden: Sie treffen sonst Kunden, die ihren Text aus der Zwischenablage einfügen.
Signaturschlüssel	Wird vom Modul automatisch erzeugt und sichert den Zeitstempel gegen Manipulation ab. Dieser Wert muss nicht geändert werden.

4.5 Fremde Zeichensätze

Fünf gleichartige Schalter, die eine Nachricht abweisen, sobald sie Zeichen des jeweiligen Schriftsystems enthält: **Erkennung Russisch**, **Erkennung Arabisch**, **Erkennung Chinesisch**, **Erkennung Hebräisch** und **Erkennung Armenisch**. *(Standard: jeweils Nein)*

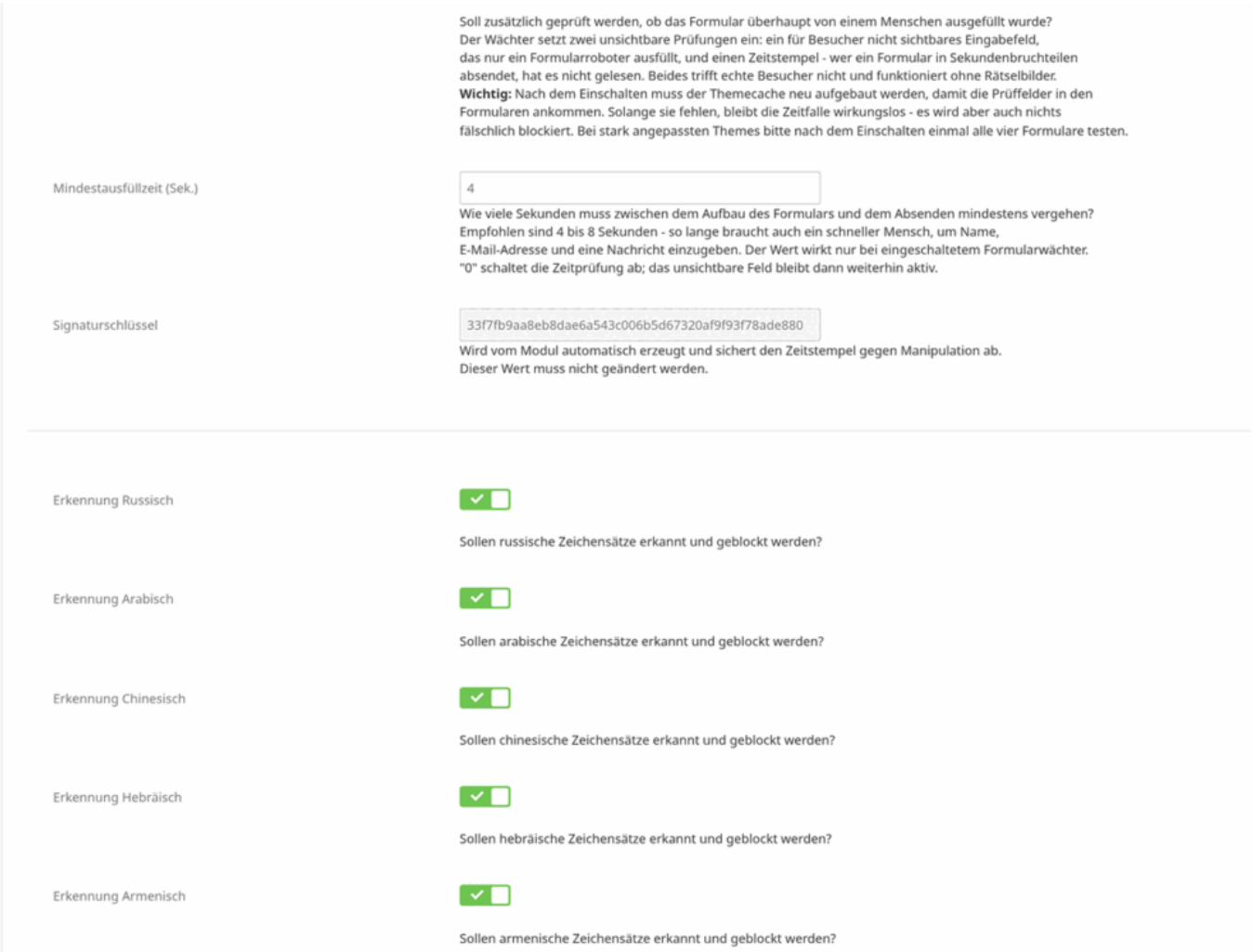

Abbildung 4: Der Abschluss des Formularwächters und die fünf Zeichensatz-Schalter.
Diese Prüfungen sind sehr wirksam, weil ein großer Teil des automatisierten Spams in diesen Schriften verfasst ist. Im Punktesystem zählt ein Treffer 3 Punkte und blockiert damit bei der empfohlenen Schwelle bereits allein.

Schalten Sie nur die Schriftsysteme ein, aus deren Sprachraum Sie **keine** Kunden erwarten. Wer nach Russland liefert oder russischsprachige Kundschaft hat, darf die russische Erkennung nicht aktivieren - sonst kommt keine einzige Anfrage dieser Kunden mehr an, und Sie merken es nicht.

4.6 Der Kontenanlageschutz

Dieser Bereich hat mit den Dialogformularen nichts zu tun: Er prüft die Anlage neuer Kundenkonten.

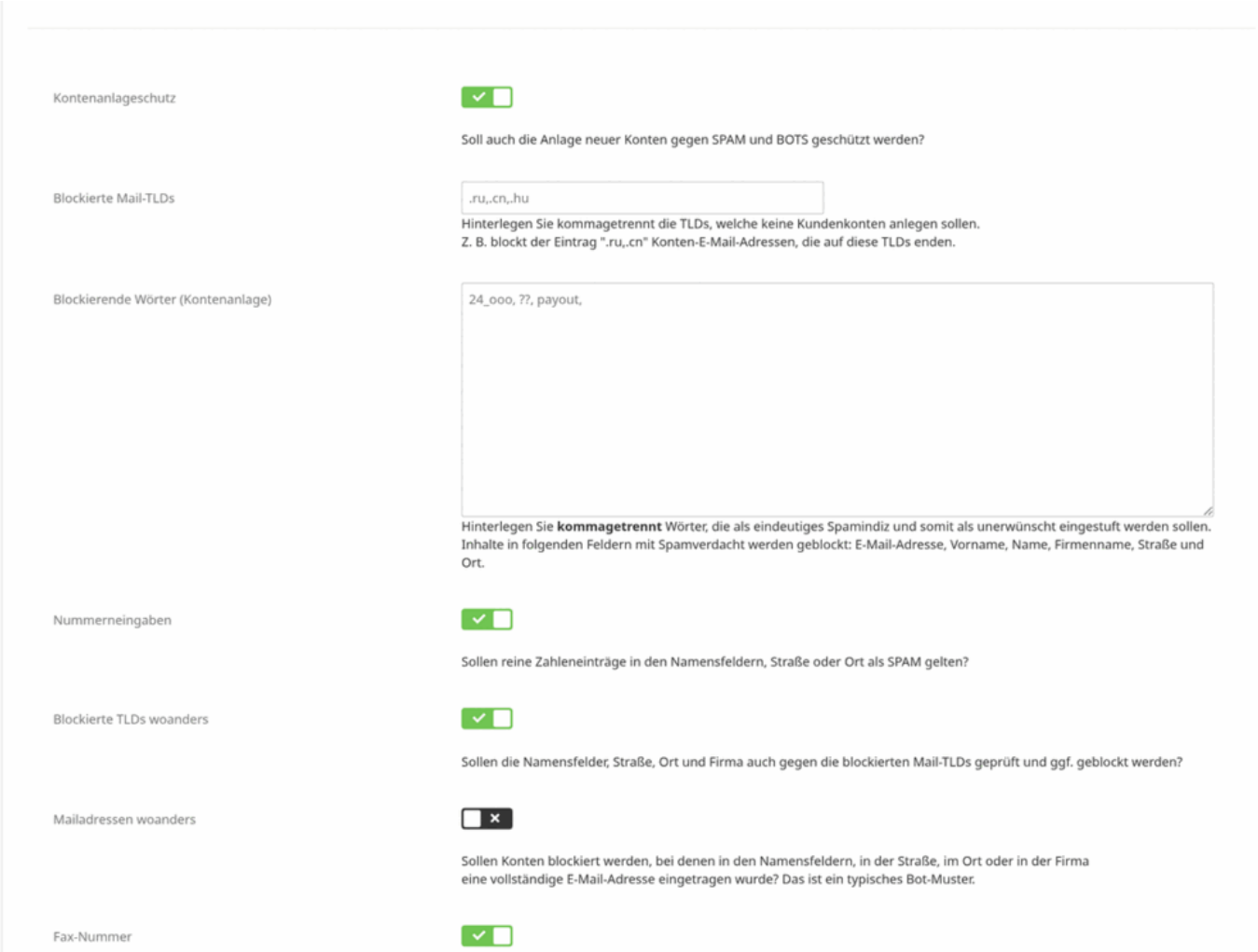

Abbildung 5: Der Kontenanlageschutz mit seiner eigenen Wortliste und den Feldprüfungen.

Einstellung	Bedeutung
Kontenanlageschutz	Hauptschalter für diesen Bereich. Steht er auf "Nein", sind sämtliche folgenden Prüfungen und auch die IP-Sperre wirkungslos. *(Standard: Nein)*
Blockierte Mail-TLDs	Kommagetrennte Domainendungen, mit denen kein Konto angelegt werden darf. Geprüft wird die E-Mail-Adresse. *(Standard: .ru,.cn,.hu)* Diese Liste ist bewusst getrennt von der des Formularschutzes: Bei der Kontenanlage darf man in der Regel strenger sein.
Blockierende Wörter (Kontenanlage)	Eigene Wortliste für die Kontenanlage, kommagetrennt. Geprüft werden E-Mail-Adresse, Vorname, Name, Firmenname, Straße und Ort. *(Standard: eine kurze Grundliste)* Hier gehören Begriffe hinein, die in einer echten Anschrift nie vorkommen - etwa Werbebegriffe im Firmennamen.
Nummerneingaben	Blockiert Konten, deren Straßenfeld ausschließlich aus Ziffern besteht. *(Standard: Nein)* Eine Straße ohne einen einzigen Buchstaben gibt es nicht - eine echte Anschrift enthält immer einen Straßennamen.
Blockierte TLDs woanders	Prüft auch Vorname, Name, Straße, Ort und Firma gegen die oben eingetragenen Domainendungen. *(Standard: Nein)* Automatisch angelegte Konten tragen ihre Werbeadresse gern in einem Namensfeld unter.
Mailadressen woanders	Blockiert Konten, bei denen in einem Namens-, Straßen- oder Firmenfeld eine vollständige E-Mail-Adresse steht. *(Standard: Nein)* Ein typisches Bot-Muster: Das Programm füllt jedes Feld mit demselben Wert.
Fax-Nummer	Blockiert Konten, deren Faxnummer mehr Buchstaben als Ziffern enthält. *(Standard: Nein)* Eine Faxnummer, die überwiegend aus Buchstaben besteht, ist keine.

4.7 Die IP-Sperre

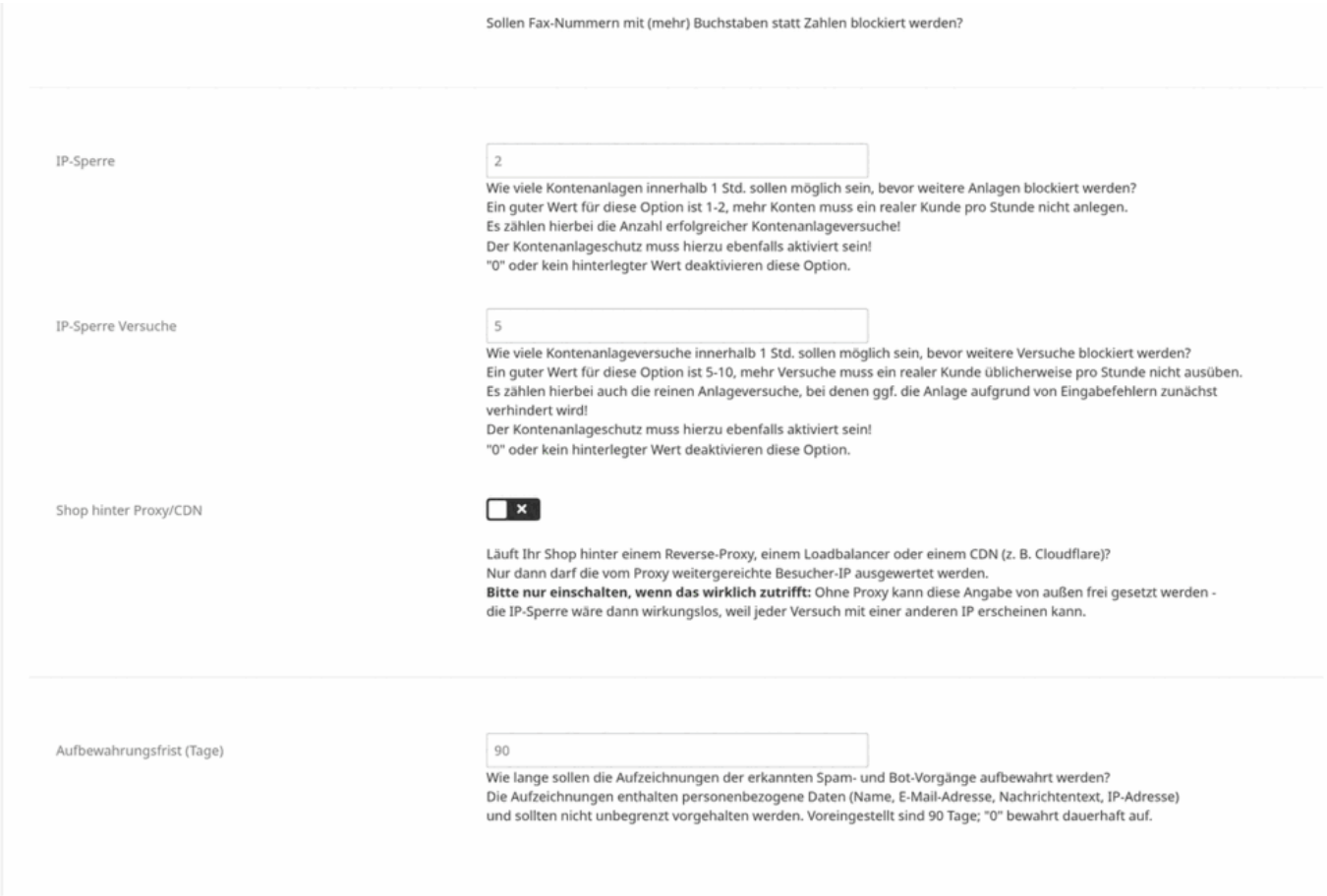

Abbildung 6: Die IP-Sperre, der Proxy-Schalter und die Aufbewahrungsfrist.
Die IP-Sperre wirkt gegen den Fall, dass jemand nicht ein einzelnes Konto anlegt, sondern hundert. Sie zählt, wie oft von derselben Internetadresse aus innerhalb einer Stunde Konten angelegt oder versucht wurden.

Einstellung	Bedeutung
IP-Sperre	Wie viele *erfolgreiche* Kontenanlagen innerhalb einer Stunde von derselben Internetadresse zulässig sind. *(Standard: 2)* Ein guter Wert ist 1 bis 2 - mehr Konten muss ein realer Kunde pro Stunde nicht anlegen. Der Wert 0 schaltet die Prüfung ab.
IP-Sperre Versuche	Wie viele *Versuche* innerhalb einer Stunde zulässig sind - also auch die, die wegen Eingabefehlern gescheitert sind. *(Standard: 5)* Ein guter Wert ist 5 bis 10. Setzen Sie ihn nicht zu niedrig: Ein Kunde, der sich beim Kennwort vertippt, soll nicht ausgesperrt werden. Der Wert 0 schaltet die Prüfung ab.
Shop hinter Proxy/CDN	Läuft Ihr Shop hinter einem Reverse-Proxy, einem Loadbalancer oder einem Verteilnetz wie Cloudflare? *(Standard: Nein)*

Zum Proxy-Schalter: Schalten Sie ihn nur ein, wenn das wirklich zutrifft. Läuft Ihr Shop *nicht* hinter einem Proxy, kann die weitergereichte Besucheradresse von außen frei gesetzt werden - die IP-Sperre wäre dann wirkungslos, weil jeder Versuch mit einer anderen Adresse erscheinen kann. Steht der Schalter umgekehrt auf "Nein", obwohl ein Proxy im Spiel ist, sehen Sie im Protokoll bei allen Vorgängen dieselbe Adresse - die des Proxys.
Beide Werte setzen voraus, dass der **Kontenanlageschutz** eingeschaltet ist.

4.8 Betrieb und Aufbewahrung

Einstellung	Bedeutung
Aufbewahrungsfrist (Tage)	Wie lange die Aufzeichnungen der erkannten Vorgänge aufbewahrt werden. *(Standard: 90)* Die Aufzeichnungen enthalten personenbezogene Daten - Name, E-Mail-Adresse, Nachrichtentext und Internetadresse - und sollten nicht unbegrenzt vorgehalten werden. Der Wert 0 bewahrt dauerhaft auf, was aus Datenschutzsicht nur mit gutem Grund sinnvoll ist. Der Aufräumlauf findet automatisch statt, wenn Sie das Setup des Moduls aufrufen.

5. DIE ERKENNUNGSWÖRTER PFLEGEN

Die Erkennungsliste ist das Herzstück der inhaltlichen Prüfung - und die einzige Einstellung, die wirklich zu Ihrem Shop passen muss. Was für einen Möbelhändler ein sicheres Spam-Kennzeichen ist, kann für einen Spirituosenhändler ein ganz normales Wort sein.

5.1 Wörter ergänzen und entfernen

Die Liste steht im Feld **Blockierende Wörter (Formulare)**, die Einträge sind durch Kommas getrennt. Geprüft werden Nachricht, Betreff, Zusatzangaben und Name. Groß- und Kleinschreibung spielt keine Rolle.

Mehrwortbegriffe sind ausdrücklich erlaubt und oft die bessere Wahl: *jetzt kaufen* trifft genau, *kaufen* allein trifft auch die Frage "Wo kann ich das kaufen?".

Die mitgelieferte Liste stammt aus der Auswertung echter Spam-Vorgänge in Kundenshops. Sie wurde gründlich überarbeitet: Rund 220 Allerweltsbegriffe, die zwar in Werbenachrichten vorkommen, aber genauso in einer seriösen Kundenanfrage - *Angebot*, *Rabatt*, *Kredit*, *Geld*, *sparen*, *bestellen*, *Name*, *buy*, *hello* und viele weitere -, wurden entfernt. Eindeutig spamtypische Einträge sind unverändert enthalten. Eigene Ergänzungen, die Sie vorgenommen haben, bleiben bei Updates erhalten.

So gehen Sie vor:

- **Vor der Inbetriebnahme:** Lesen Sie die Liste einmal durch und streichen Sie alles, was in Ihrer Branche ein normales Wort ist. Ein Weinhändler streicht Begriffe rund um Alkohol, ein Apothekenshop die Medikamentennamen, ein Finanzdienstleister die Geldbegriffe.
- **Im laufenden Betrieb:** Kommt doch eine Werbenachricht durch, suchen Sie darin ein Wort oder eine Wortkombination, die in einer echten Kundenanfrage niemals vorkäme, und ergänzen Sie diese am Ende der Liste.
- **Bei Verdacht auf Fehlblockaden:** Öffnen Sie das Protokoll und sehen Sie sich die häufigsten Gründe an (Abschnitt 7.1). Dort steht schwarz auf weiß, welcher Eintrag wie oft zugeschlagen hat.

Wird das Feld **leer** gespeichert, stellt das Modul beim nächsten Aufruf die mitgelieferte Liste wieder her. Sie können sich also nicht aussperren.
Erreicht Sie trotz eingeschaltetem und eingerichtetem Modul weiterhin Spam über die Shopformulare, leiten Sie diese Nachrichten bitte an **spamcheck@xycons.de** weiter. Wir werten sie aus und arbeiten neue Erkennungsregeln in künftige Updates ein - davon profitieren alle Anwender.

5.2 Warum "nur ganze Wörter" wichtig ist

Steht die Einstellung **Nur ganze Wörter** auf "Nein", sucht das Modul die Erkennungswörter irgendwo im Text - auch mitten in anderen Wörtern. Die Folgen sind erstaunlich weitreichend:

Erkennungswort	trifft dann auch
sex	*Essex*, *Sexta*, *Middlesex*
now	*snow*, *know*, *nowhere*
cash	*Cashmere*
spam	*Spanien* nicht - aber *Spamfilter* in einer Kundenfrage sehr wohl

Eine Kundin aus Essex hätte Ihnen dann nie schreiben können, und Sie hätten es nie erfahren. Mit der Einstellung "Ja" schlägt ein Erkennungswort nur an, wenn es als eigenständiges Wort im Text steht.

Zusammengesetzte Einträge wie *jetzt kaufen* und Einträge mit Sonderzeichen wie *18+* oder *24/7* werden auch bei "Ja" weiterhin zuverlässig gefunden.

5.3 Bekannte Kunden ausnehmen

Steht **Bekannte Kunden** auf "Ja", prüft das Modul bei einem Verdacht zusätzlich, ob die Absenderadresse in Ihrem Kundenstamm hinterlegt ist. Ist sie das, entfallen die inhaltlichen Prüfungen und die Nachricht geht durch.

Das ist eine der wirksamsten Einstellungen gegen verlorene Kundenanfragen: Wer bei Ihnen schon einmal bestellt hat, ist mit hoher Wahrscheinlichkeit kein Werbeversender - selbst wenn seine Nachricht zufällig ein Reizwort enthält.

Nicht ausgenommen bleibt der Missbrauch der Shop-Adresse als Absender und ein Treffer des Formularwächters. Diese gelten auch für bekannte Kunden.

6. DER FORMULARWÄCHTER IN DER PRAXIS

Alle bisher beschriebenen Prüfungen sehen sich an, *was* jemand schreibt. Der Formularwächter fragt etwas anderes: *Wer* hat da eigentlich getippt - ein Mensch oder ein Programm? Das ist die wirksamste Einzelmaßnahme des Moduls, weil sie einen automatisierten Absender erkennt, noch bevor überhaupt ein Wort geprüft wird. Und sie erzeugt praktisch keine Fehlblockaden.

Dahinter stehen zwei Prüfungen, die Ihr Besucher nie zu Gesicht bekommt:

- **Das unsichtbare Feld.** Das Formular enthält ein zusätzliches Eingabefeld, das im Browser nicht dargestellt und auch mit der Tabulatortaste nicht erreicht wird. Ein Mensch kann es gar nicht ausfüllen. Ein Formularroboter liest den Seitenquelltext, findet ein Feld und trägt etwas ein - und verrät sich damit.
- **Die Zeitfalle.** Das Formular merkt sich den Moment, in dem es aufgebaut wurde. Wer Name, E-Mail-Adresse und eine Nachricht in weniger als der eingestellten Mindestzeit einträgt und absendet, hat das Formular nicht gelesen.

Für Ihren Besucher ändert sich dadurch nichts. Das Formular sieht aus wie immer, es gibt kein Rätselbild und nichts abzutippen:

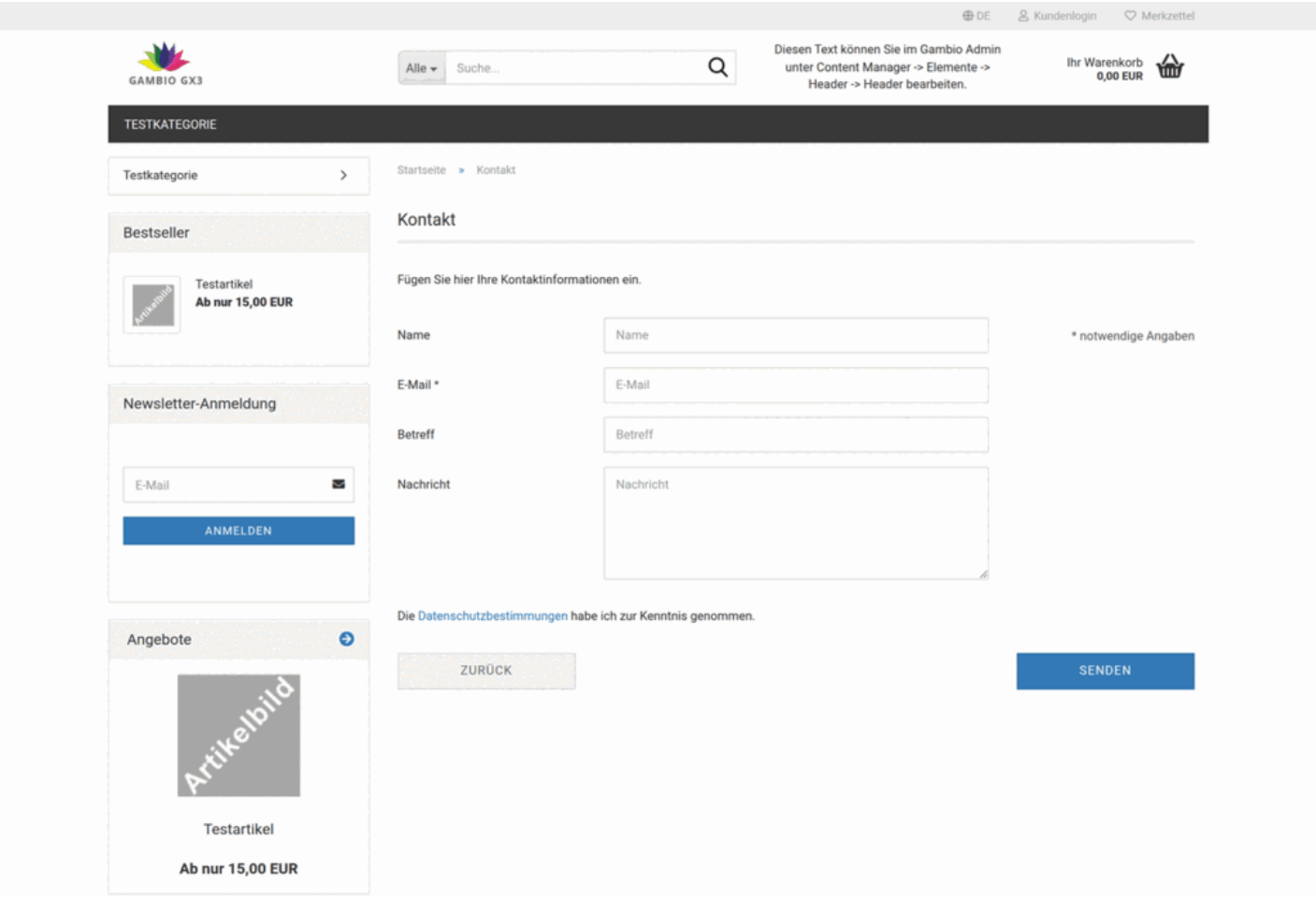

Abbildung 7: Das geschützte Kontaktformular aus Sicht des Besuchers - äußerlich unverändert. Die Prüffelder sind nicht sichtbar.

6.1 Nach dem Einschalten: einmal den Cache aufbauen lassen

Damit die Prüffelder in Ihren Formularen ankommen, muss der Themecache des Shops nach dem Einschalten einmal neu aufgebaut werden. Solange das nicht geschehen ist, bleibt die Zeitfalle wirkungslos - **es wird aber auch nichts fälschlich blockiert**. Das Modul geht hier bewusst auf Nummer sicher: Fehlt das Prüffeld, wird die Nachricht durchgelassen. Ein nicht aktualisiertes Theme kann Ihre Formulare also nie lahmlegen.

Bitte testen Sie nach dem Einschalten trotzdem einmal alle vier Formulare - Kontakt, Rückruf, "Woanders günstiger" und Produktempfehlung -, indem Sie selbst eine Nachricht abschicken. Das gilt besonders für stark angepasste Themes.

Ein Formular, das jemand eine Stunde lang offen liegen lässt, wird übrigens nicht beanstandet - beanstandet wird nur, was zu schnell geht.

7. DAS PROTOKOLL: WAS WURDE ABGEWEHRT?

Ein Spamschutz, den man nicht nachvollziehen kann, ist ein Vertrauensproblem: Man sieht, was *nicht* mehr ankommt - aber nicht, was das Modul dabei sonst noch abgefangen hat. Genau dafür gibt es die Protokollansicht unter **KUNDEN > ANTISPAM-MASTER PROTOKOLL**.

Zwei Reiter trennen die Bereiche: *Formulare* und *Kontenanlage*. Oben stehen die Kennzahlen des gewählten Zeitraums.

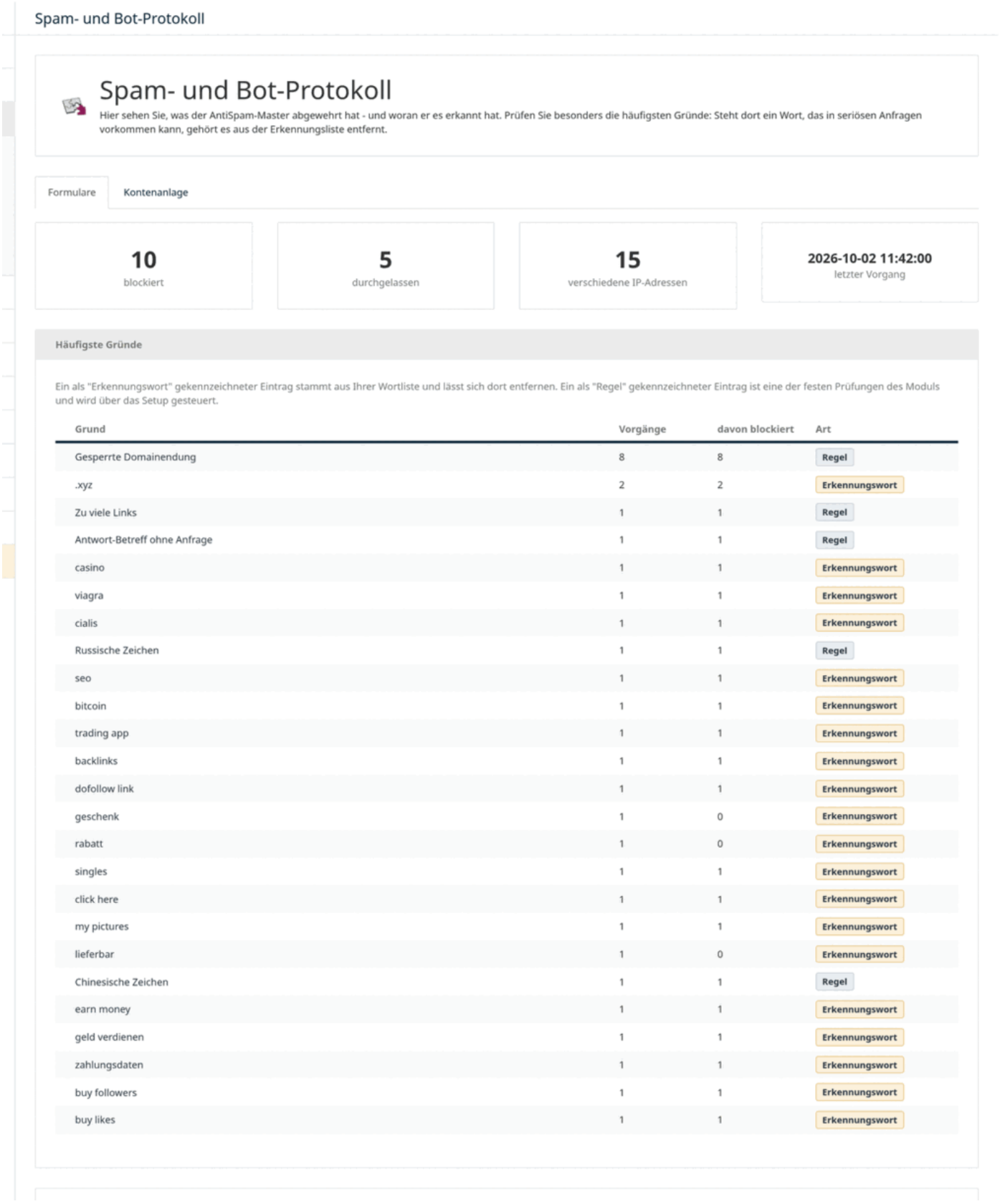

Abbildung 8: Die Kennzahlen des gewählten Zeitraums und die Tabelle der häufigsten Gründe.

7.1 Die häufigsten Gründe - Ihr wichtigstes Werkzeug

Die Tabelle "Häufigste Gründe" ist der Grund, warum sich ein Blick in diese Ansicht wirklich lohnt. Sie zeigt, woran das Modul die Vorgänge erkannt hat - sortiert nach Häufigkeit. Jeder Eintrag ist gekennzeichnet:

- **Erkennungswort** - der Eintrag stammt aus Ihrer Wortliste und lässt sich dort entfernen.
- **Regel** - eine der festen Prüfungen des Moduls (gesperrte Domainendung, Zeichensatz, Formularwächter). Diese steuern Sie über das Setup.

Und so nutzen Sie die Tabelle: Steht ganz oben ein Erkennungswort, das in einer seriösen Anfrage an *Ihren* Shop vorkommen kann, haben Sie einen Kandidaten für die Streichung gefunden. Ein Fahrradhändler, bei dem *Rahmen* ganz oben steht, sollte das Wort entfernen. Ein Möbelhändler, bei dem *casino* ganz oben steht, lässt es stehen. Diese eine Tabelle beantwortet damit die Frage, die man sonst nur raten kann: Wo blockiert mein Shop zu viel?

Die Spalte "davon blockiert" zeigt zusätzlich, wie oft ein Grund tatsächlich zur Blockade geführt hat und wie oft er nur mitgezählt wurde, ohne allein auszureichen.

7.2 Die Vorgangsliste

Darunter steht jeder einzelne Vorgang mit Zeitpunkt und Internetadresse, E-Mail-Adresse, Name und Betreff, einem Auszug des Inhalts, den erkannten Gründen, der Punktzahl und dem Status.

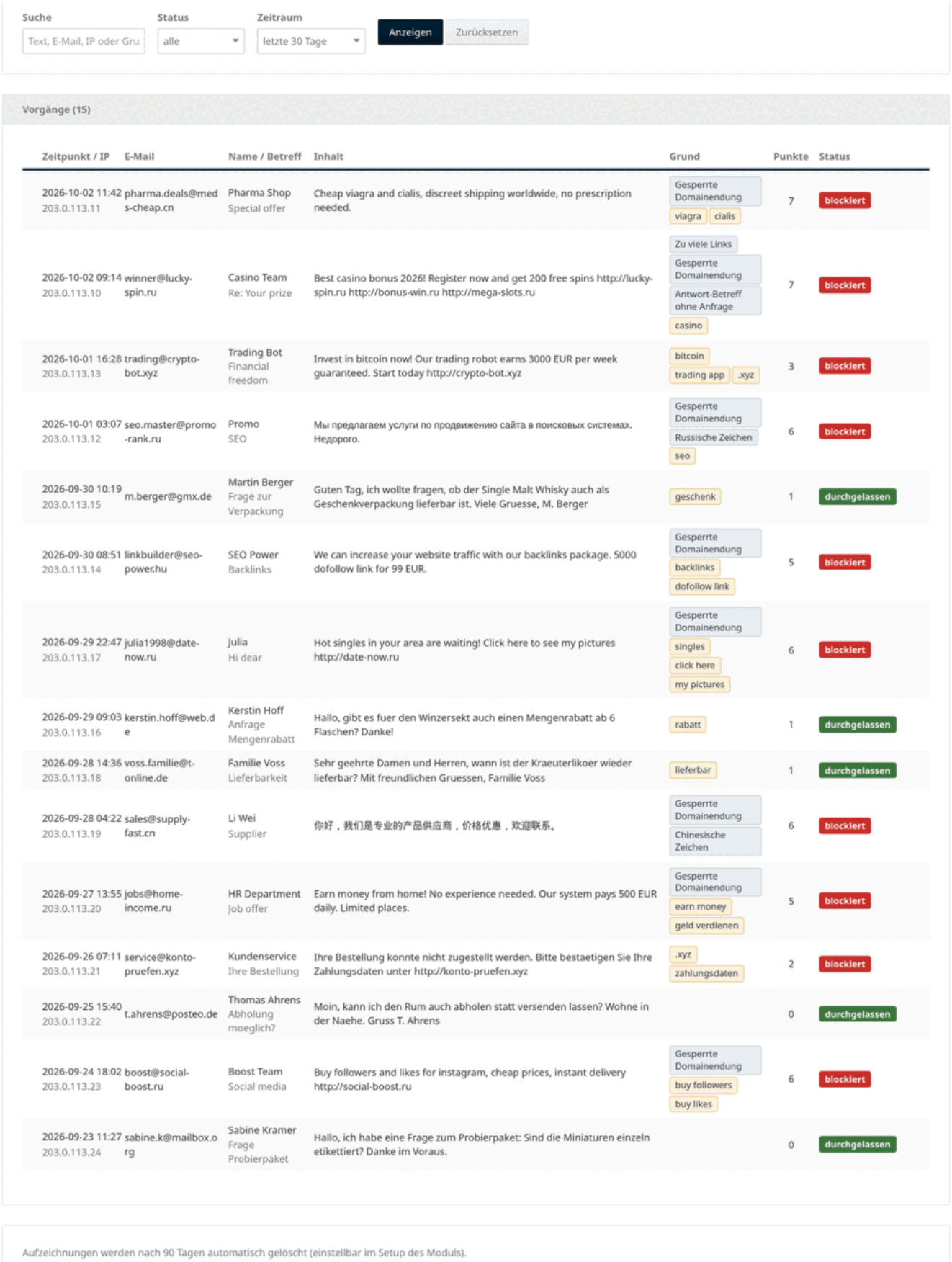

Abbildung 9: Die Filterleiste und die Vorgangsliste. Rechts sehen Sie je Vorgang die erkannten Gründe, die Punktzahl und ob blockiert wurde.

Die Gründe sind farblich unterschieden: **gelb hinterlegte** Einträge sind Erkennungswörter aus Ihrer Wortliste - die können Sie dort streichen. **Blaugrau hinterlegte** Einträge sind feste Prüfungen des Moduls wie "Gesperrte Domainendung" oder "Russische Zeichen" - die steuern Sie über das Setup.

Der Status verdient eine Erklärung. Es gibt zwei:

- **blockiert** - die Nachricht wurde nicht versendet beziehungsweise das Konto nicht angelegt.
- **durchgelassen** - das Modul hat etwas bemerkt, es hat aber nicht zur Blockade gereicht. Diese Vorgänge sind der Sinn des

Punktesystems: Sie sehen, was Sie *fast* verloren hätten.

Damit lässt sich die Punkteschwelle belastbar einstellen, statt sie zu schätzen. Stehen unter "durchgelassen" überwiegend echte Kundenanfragen, ist die Schwelle richtig gewählt. Stehen dort überwiegend Werbenachrichten, senken Sie die Schwelle um einen Punkt.

Auch bei ausgeschaltetem Punktesystem wird die Punktzahl mitgeschrieben. Vorgänge mit nur einem Punkt sind dann die wahrscheinlichsten Fehlblockaden - ein guter Startpunkt für die Durchsicht.

Über die Filterleiste schränken Sie nach Zeitraum, Status und einem Suchbegriff ein. Die Suche geht über Inhalt, E-Mail-Adresse, Internetadresse und Grund - praktisch, wenn ein Kunde anruft und sagt, seine Nachricht sei nicht angekommen: Adresse eingeben, und Sie sehen sofort, ob und woran sie hängen geblieben ist.

7.3 Der Bereich Kontenanlage

Der zweite Reiter zeigt dasselbe für die abgewiesenen Kontenanlagen. Statt Nachricht und Betreff sehen Sie hier die eingegebenen Kontodaten - Vorname, Name, Straße und Firma.

Spam- und Bot-Protokoll

Hier sehen Sie, was der AntiSpam-Master abgewehrt hat - und woran er es erkannt hat. Prüfen Sie besonders die häufigsten Gründe: Steht dort ein Wort, das in seriösen Anfragen vorkommen kann, gehört es aus der Erkennungsliste entfernt.

Formulare | Kontenanlage

5	0	5	2026-10-01 03:14:00
blockiert	durchgelassen	verschiedene IP-Adressen	letzter Vorgang

Häufigste Gründe

Ein als "Erkennungswort" gekennzeichneter Eintrag stammt aus Ihrer Wortliste und lässt sich dort entfernen. Ein als "Regel" gekennzeichneter Eintrag ist eine der festen Prüfungen des Moduls und wird über das Setup gesteuert.

Grund	Vorgänge	davon blockiert	Art
Gesperrte Domainendung	5	5	Regel
Straße nur aus Ziffern	2	2	Regel
Domainendung im Namensfeld	2	2	Regel
seo	1	1	Erkennungswort
E-Mail im falschen Feld	1	1	Regel
casino	1	1	Erkennungswort
viagra	1	1	Erkennungswort

Suche: Text, E-Mail, IP oder Gru | Status: alle | Zeitraum: letzte 30 Tage | Anzeigen | Zurücksetzen

Vorgänge (5)

Zeitpunkt / IP	E-Mail	Inhalt	Grund	Punkte	Status
2026-10-01 03:14 203.0.113.60	bot4711@mail-temp.ru	Ivan / Petrov / 12345 / -	Gesperrte Domainendung Straße nur aus Ziffern	2	blockiert
2026-09-30 09:41 203.0.113.61	seo.robot@rank-up.cn	Li / Chen / seo-service.cn / SEO Agency	Gesperrte Domainendung Domainendung im Namensfeld seo	3	blockiert
2026-09-29 17:08 203.0.113.62	casino.player@spin-win.hu	Max / Muster / info@spin-win.hu / Casino	Gesperrte Domainendung E-Mail im falschen Feld casino	3	blockiert
2026-09-27 05:52 203.0.113.63	xk29fj@throwaway.ru	asdf / qwer / 99999 / -	Gesperrte Domainendung Straße nur aus Ziffern	2	blockiert
2026-09-25 21:19 203.0.113.64	promo.bot@cheap-meds.cn	Anna / Ivanova / viagra-shop.cn / Pharma	Gesperrte Domainendung Domainendung im Namensfeld viagra	3	blockiert

Aufzeichnungen werden nach 90 Tagen automatisch gelöscht (einstellbar im Setup des Moduls).

Protokoll dieses Bereichs leeren

Abbildung 10: Abgewiesene Kontenanlagen mit den eingegebenen Daten und dem jeweiligen Grund.
Diese Ansicht ist besonders aufschlussreich, wenn Sie den Kontenanlageschutz gerade erst eingeschaltet haben: Sie sehen auf einen Blick, nach welchem Muster die automatisierten Konten in Ihrem Shop angelegt wurden, und können die Wortliste und die Feldprüfungen gezielt darauf einstellen.

7.4 Aufbewahrung und Datenschutz

Die Aufzeichnungen enthalten personenbezogene Daten - Name, E-Mail-Adresse, den Nachrichtentext und die Internetadresse des Absenders. Über die **Aufbewahrungsfrist (Tage)** im Setup legen Sie fest, wie lange sie vorgehalten werden; voreingestellt sind 90 Tage.

Unten in der Protokollansicht können Sie das Protokoll des jeweiligen Bereichs außerdem jederzeit vollständig leeren. Die Zähler im Setup bleiben davon unberührt.

Ein Hinweis zur Beruhigung: Die Ansicht stellt die aufgezeichneten Inhalte ausschließlich als Text dar. Auch wenn ein Absender in seine Nachricht Schadcode geschrieben hat, wird dieser im Administrationsbereich nicht ausgeführt.

8. WAS TUN, WENN ...

8.1 ... trotzdem Spam ankommt

Schauen Sie zuerst ins Protokoll: Steht der Vorgang dort mit dem Status "durchgelassen", hat das Modul ihn erkannt, aber die Punkteschwelle war zu hoch - senken Sie sie um einen Punkt. Taucht er dort gar nicht auf, wurde nichts erkannt, und Sie brauchen eine neue Regel.

Prüfen Sie der Reihe nach:

- Ist der **Formularwächter** eingeschaltet und der Themecache danach neu aufgebaut worden? Das fängt den größten Teil ab.
- Enthält die Nachricht ein Wort oder eine Wortkombination, die in einer echten Kundenanfrage niemals vorkäme? Dann ergänzen Sie sie in der Erkennungsliste.
- Ist die Absenderendung eine, die Sie sperren können, ohne echte Kunden zu treffen?
- Ist die Nachricht in einer fremden Schrift verfasst, aus deren Sprachraum Sie keine Kunden haben?
- Enthält die Nachricht mehrere Links? Dann senken Sie *Erlaubte URLs*.

Kommen weiterhin Nachrichten durch, senden Sie uns diese bitte an **spamcheck@xycons.de**. Wir werten sie aus und ergänzen die Erkennung im nächsten Update.

8.2 ... ein echter Kunde geblockt wird

Das ist der unangenehmere Fall, weil er sonst unbemerkt bliebe - genau dafür gibt es das Protokoll. Öffnen Sie es, filtern Sie auf "blockiert" und sehen Sie sich die Tabelle der häufigsten Gründe an. Die häufigste Ursache ist ein zu allgemeines Erkennungswort.

Prüfen Sie außerdem:

- Steht *Nur ganze Wörter* auf "Ja"? Wenn nicht, ist das mit hoher Wahrscheinlichkeit die Ursache.
- Ist das *Punktesystem* eingeschaltet? Es ist das wirksamste Mittel gegen Fehlblockaden.
- Haben Sie eine Domainendung gesperrt, aus deren Land Sie doch Kunden haben?
- Haben Sie einen Zeichensatz gesperrt, aus dessen Sprachraum Sie doch Kunden haben?
- Steht *Bekannte Kunden* auf "Ja"?
- Ist die *Mindestausfüllzeit* zu hoch eingestellt? Werte über 10 Sekunden können Kunden treffen, die Text aus der Zwischenablage einfügen.

8.3 ... gar nichts mehr blockiert wird

- Steht der *Modulstatus - AntiSpam-Master* auf "Ja"? Ohne ihn ist alles andere wirkungslos.
- Ist die Erkennungsliste versehentlich geleert worden? Speichern Sie das Feld leer - das Modul stellt die mitgelieferte Liste wieder her.
- Ist für die Kontenanlage der *Kontenanlageschutz* eingeschaltet? Ohne ihn wirken auch die IP-Sperre und die Feldprüfungen nicht.
- Steht *Bekannte Kunden* auf "Ja" und schreibt Ihnen der Absender aus einer Adresse, die als Kunde hinterlegt ist? Dann ist das so gewollt.

- Ist das *Punktesystem* mit einer sehr hohen Schwelle eingeschaltet? Im Protokoll sehen Sie dann viele Vorgänge mit dem Status "durchgelassen" - senken Sie die Schwelle.

9. WAS DAS MODUL NICHT LEISTEN KANN

Damit keine falschen Erwartungen entstehen - drei Dinge, die außerhalb der Reichweite des Moduls liegen:

- **Es wirkt nur innerhalb des Shops.** Ihre Postfächer erreicht es nicht. Schreibt Ihnen jemand direkt an Ihre E-Mail-Adresse, läuft das an Ihrem Shop vorbei und kann vom Modul weder geprüft noch verhindert werden. Was Sie mit dem Modul erreichen: Die ärgerlichen Spameinträge unter KUNDEN > E-MAILS gehen deutlich zurück, meist auf null.
- **Es ersetzt keinen Serverschutz.** Gegen massenhafte Aufrufe, die Ihren Server in die Knie zwingen sollen, hilft nur eine Abwehr auf Serverebene.
- **Es liest keine Gedanken.** Eine Werbenachricht, die höflich formuliert ist, keine Links enthält, aus einer deutschen Adresse kommt und in ordentlichem Deutsch verfasst ist, sieht für jede Prüfung wie eine echte Anfrage aus. Solche Fälle bleiben - sie sind aber selten, weil sie sich für den Versender nicht lohnen.

10. SHOPUPDATE UND MODULPFLEGE

Bitte beachten Sie vor jedem Update Ihres Shops - also vor einem Service Pack ebenso wie vor einem Masterupdate:

- **Vorher prüfen:** Sehen Sie auf unserer Seite www.xycons.de nach, ob das Modul für die neue Shopversion bereits freigegeben ist. Ein Modul passt sich nicht von selbst an eine neue Shopversion an.
- **Immer mit aktualisieren:** Spielen Sie beim Shopupdate stets die neuesten Versionen des Moduls *und* der Modulumgebung ein - nicht nur den Shop. Wer nur den Shop aktualisiert, hat danach unter Umständen ein Modul, das nicht mehr arbeitet, und sucht die Ursache an der falschen Stelle.

Wenn Sie die Aktualisierung Ihres Shops durch uns durchführen lassen, aktualisieren wir vorhandene Xycons-Module und die Modulumgebung immer mit, sofern sie für die neue Shopversion verfügbar sind.

Nach einem Update des Moduls lohnt sich ein Blick ins Setup: Neue Fassungen bringen gelegentlich neue Einstellungen mit, die zunächst ausgeschaltet vorbelegt sind, damit sich am Verhalten Ihres Shops nichts unbemerkt ändert.

11. MODULTEXTE ÄNDERN

Modultexte können Sie - wie bei allen Modulen von uns - über die Shopfunktion **"Texte ändern"** im Administrationsbereich an eigene Bedürfnisse anpassen.

Für dieses Modul betrifft das vor allem die Meldung, die ein Besucher zu sehen bekommt, wenn seine Nachricht abgewiesen wurde. Sie ist bewusst sachlich und knapp gehalten - wenn Sie einen freundlicheren oder ausführlicheren Ton bevorzugen, etwa mit dem Hinweis auf Ihre Telefonnummer als Ausweichweg, ändern Sie den Text dort einfach ab.

Ein Ausweichweg ist eine gute Idee: Nennen Sie in der Meldung Ihre Telefonnummer oder eine direkte E-Mail-Adresse. Dann kommt auch der seltene Fall einer Fehlblockade nicht als verlorener Kunde bei Ihnen an, sondern als Anruf.

Xycons GmbH & Co. KG

Wir wünschen viel Erfolg beim Einsatz unseres Moduls!