HTProtect

Joomla Security – always up to date.

JOOMLA SECURITY

Dokumentation

HTProtect – deine Joomla-Website einfach absichern. Übersicht, Backend-Schutz, Schutzschild, Site-Scan, Sicherungen & Updates und Hilfe – kurz und anfängerfreundlich erklärt.

htprotect.org · Stand: Juli 2026

Dokumentation

HTProtect – Dokumentation

HTProtect ist kein starres Schloss, sondern ein mitdenkender Schutz für deine Joomla-Website: mehrschichtig, immer aktuell – und er sperrt dich nie aus. Diese Anleitung zeigt Kapitel für Kapitel, **was** genau passiert, **wann** es passiert und **warum** dich das schützt.

Was ist HTProtect?

HTProtect ist ein „Server-Schild" für Joomla, das an mehreren Stellen gleichzeitig aufpasst. Drei Dinge heben es ab:

- **Eine Mini-Firewall, die sich live aktualisiert.** Wird eine neue Angriffsmethode oder eine frische Lücke in einer verbreiteten Erweiterung bekannt, blockiert HTProtect den Angriffsweg automatisch – du musst nicht erst auf ein Update des Herstellers warten. Fachleute nennen das *virtuelles Patchen*.
- **Es hält sich selbst aktuell.** HTProtect spielt eigene Updates automatisch ein, in der Regel binnen etwa drei Stunden – ganz ohne dein Zutun ist der Schutz immer auf dem neuesten Stand.
- **Es sperrt dich nie aus.** Jede Schutzregel wird nach dem Schreiben am echten Server getestet und notfalls automatisch wieder zurückgenommen.

Dazu kommen die Server-Härtung, ein zusätzliches Passwort vor dem Backend, ein Malware-Scanner und automatische Updates mit Backup. Seine Schutzdaten frischt HTProtect auf wie ein Virenscanner seine Virendefinitionen: Es lädt regelmäßig öffentliche, signierte Daten *herunter* – site- oder personenbezogene Daten sendet es dabei nicht ungefragt nach außen.

Für die meisten reicht ein Klick

Der Normalfall ist ein einziger Klick auf **„Jetzt absichern"** in der Übersicht – alles andere passiert automatisch. Und keine Sorge: HTProtect macht nichts kaputt. Vor jeder Änderung wird gesichert, alles wird selbst geprüft und bei Problemen automatisch wieder zurückgenommen.

HTProtect herunterladen

Übersicht

Die Übersicht ist dein Cockpit. Eine **Sicherheits-Ampel** zeigt auf einen Blick, wo du stehst: Grün heißt alles gut, Orange ist ein Hinweis, Rot bedeutet Handlungsbedarf. Orange oder rote Punkte kannst du anklicken – sie führen dich direkt zur passenden Lösung. Der große Knopf **„Jetzt absichern"** erledigt das Wichtigste in einem einzigen Klick.

Damit die Ampel stimmt, arbeitet im Hintergrund **der Wächter**. Er läuft bei *jedem* Seitenaufruf als Allererstes – praktisch ohne spürbare Ladezeit –, hält die Mini-Firewall aktuell und wacht darüber, dass der

Schutzschild unversehrt bleibt. Nur lesend erkennt er außerdem eingeschleusten Code in den Kern- und den aktiven Template-Dateien und meldet ihn.

Auch Verdächtiges an deinen Konten fällt ihm auf – ein neuer Super-User, ein heimlich geändertes Passwort. Gemeldet wird per E-Mail, gebündelt und in der Sprache deines Backends, und nur, wenn wirklich etwas ist. Also kein Spam.

Was wann passiert

Der Schutz folgt einem festen Rhythmus – das meiste davon, ohne dass du je etwas tust:

1. **Bei der Installation**
   HTProtect richtet sich ein, sichert aber noch nichts scharf. Du entscheidest, wann es losgeht.
2. **Ein Klick „Jetzt absichern"**
   Der Schild wird geschrieben, die Upload-Ordner werden abgeriegelt, alles am echten Server getestet und deine sicheren Downloads automatisch freigegeben.
3. **Bei jedem Seitenaufruf**
   Der Wächter prüft Firewall und Unversehrtheit – unmerklich schnell.
4. **Regelmäßig im Hintergrund (etwa alle 6 Stunden)**
   HTProtect holt den signierten Feed und hält Mini-Firewall und Verwundbarkeits-Wissen aktuell. Sicherheitskritisches greift sofort.
5. **Etwa alle 3 Stunden**
   HTProtect prüft auf eigene Updates und spielt sie automatisch ein.
6. **Zur eingestellten Zeit**
   Optionale Auto-Updates deiner Erweiterungen – mit Backup, Gesundheitscheck und automatischem Rückfall.

Backend-Passwortschutz

Vor die Joomla-Anmeldung schaltet HTProtect eine **zweite Passwort-Abfrage** – direkt vor die Backend-Adresse (die mit `/administrator` endet). Angreifer und Bots landen so gar nicht erst auf der Login-Seite. Das ist eine zusätzliche Hürde und schützt sogar vor Lücken im Login selbst, die noch niemand kennt.

1. **Benutzername und Passwort festlegen**
2. **Schutz aktivieren – fertig**

Und die berechtigte Sorge „Was, wenn ich mich selbst aussperre?" nimmt dir HTProtect ab: Es testet die Sperre am echten Server und schaltet automatisch zurück, falls etwas nicht passt. Einen schon vorhandenen Passwortschutz übernimmt es einfach.

Passwort vergessen? Kein Problem: Lösche per FTP die Datei `administrator/.htaccess` – damit ist die Extra-Abfrage weg und du kommst wieder ins Backend.

Schutzschild

Der Schutzschild ist die Server-Ebene deiner Absicherung: eine gehärtete `.htaccess` nach dem Grundsatz „alles verboten außer dem Nötigen". Ein Klick auf **„Jetzt absichern"** genügt – die empfohlenen Einstellungen sind schon gesetzt. Alles Weitere liegt eingeklappt unter **„Erweiterte Einstellungen"** (für Profis; im Zweifel einfach so lassen).

Dahinter greifen mehrere Schichten ineinander:

- **Upload-Ordner dicht.** In Ordnern, in die man Dateien hochladen kann (Uploads, Medien, Cache, tmp), wird die Ausführung von PHP komplett unterbunden. Die häufigste Einbruchsstelle – eine hochgeladene Web-Shell – läuft damit ins Leere (403).
- **Sensible Dateien versteckt.** Der direkte Zugriff auf `configuration.php`, Backups, Logdateien und Ähnliches wird blockiert.
- **Schutz-Header & HTTPS.** Sicherheits-Header werden gesetzt; läuft deine Seite über HTTPS, leitet HTProtect unverschlüsselte Aufrufe automatisch auf die sichere Verbindung um (abschaltbar).
- **Web Application Firewall.** Bekannte Angriffsmuster fängt HTProtect schon *vor* Joomla ab – der Angriff erreicht deine Seite gar nicht erst.

Die Mini-Firewall: Schutz, der nicht altert

Das Besondere: Diese Muster sind nicht in Stein gemeißelt. HTProtect gleicht sich regelmäßig – etwa alle 6 Stunden – mit einem **signierten Feed** ab, ganz wie ein Virenscanner seine Virendefinitionen auffrischt. Wird eine neue Angriffsmethode oder eine frische Lücke in einer verbreiteten Erweiterung bekannt, kommt die passende Blockregel automatisch dazu – der Angriffsweg ist dicht, **bevor** es überhaupt ein offizielles Update der verwundbaren Erweiterung gibt. Sicherheitskritische Einträge greifen sofort, nicht erst beim nächsten Abgleich.

Damit diesen Kanal niemand missbraucht, wird die Signatur des Feeds direkt auf deiner Seite geprüft – nur unverfälschte Daten werden übernommen.

HTProtect sperrt dich nie aus

Neue Schutzregeln bergen theoretisch ein Risiko: Was, wenn eine davon *dich* aussperrt? Genau hier hat HTProtect mitgedacht. Jede Regel wird nach dem Schreiben **am echten Server getestet** (ob Apache, LiteSpeed oder nginx, erkennt es selbst). Würde sie dich aussperren, nimmt HTProtect sie automatisch zurück. Scharf wird der Schild nur, wenn er nachweislich funktioniert.

> **Deine eigenen Downloads bleiben heil**
> Nach dem Absichern ruft HTProtect deine Seite selbst auf und gibt legitime, verlinkte Downloads und Formulare **automatisch** wieder frei. Absichern macht deine eigenen Downloads also nie kaputt. Nur wirklich Riskantes – etwa eine PHP-Programmdatei im Bilder-Ordner – meldet es dir mit Namen, damit du bewusst entscheiden kannst.

Nach Serverumzug oder Domainwechsel? Klemmt danach etwas, lösche die Haupt-`.htaccess` im Joomla-Hauptverzeichnis per FTP und lass sie mit **„Jetzt absichern"** neu schreiben – das entfernt alte, nicht mehr passende Regeln.

Häufiges Problem: eigene Datei wird geblockt (403)

Der Schild lässt nur Bekanntes durch und weist den Rest mit **403 (verboten)** ab – genau das schützt dich. Bindest du aber selbst etwas ein (eigenes Skript, Forum, Shop), kennt er es noch nicht → 403. Kein Defekt: Ein 403 auf eine Datei, die **du** bewusst eingebunden hast, heißt nur „bitte einmal freigeben".

So findest du die blockierte Datei – direkt im Browser, ohne Server-Zugang (30 Sekunden, kaputt machen kannst du nichts):

1. **Öffne die Seite oder Funktion, die nicht funktioniert.**
2. **Drücke die Taste** `F12`
   Das öffnet die in jedem Browser eingebauten Entwicklerwerkzeuge. Klick oben auf den Reiter **Netzwerk**.
3. **Löse die Aktion erneut aus**
   Seite neu laden oder Formular abschicken, dann den **roten Eintrag „403"** anklicken – dort steht der Pfad der blockierten Datei (z. B. `custom-form.php`). Den merkst du dir.

Name	Status
index.php	200
custom-form.php	403

Reiter „Netzwerk": der rote **403** ist die blockierte Datei.

So gibst du sie frei – unter `HTProtect › Schutzschild › Erweiterte Einstellungen`, danach immer `Speichern + .htaccess schreiben` (erst dann wirkt es):

- **Einzelne Datei:** Feld „Einzeldateien direkt freigeben" – eine pro Zeile, z. B. `custom-form.php` (im Unterordner: `tools/sondertool.php`).
- **Ordner mit eigener Software** (Forum, Shop …, führt PHP aus): Feld „Ordner komplett freigeben, inklusive PHP-Ausführung" – z. B. `forum`.
- **Ordner nur mit Dateien zum Herunterladen** (PDFs, Bilder – kein PHP): Feld „Ordner für alle Dateitypen freigeben, ohne PHP" – z. B. `downloads`. Die sicherere Wahl, wenn kein PHP nötig ist.
- **Ganzer, exotischer Dateityp:** Feld „Freigegebene Datei-Endungen (kommagetrennt)" – für ungewöhnliche Endungen, die noch nicht freigegeben sind, z. B. 3D-/CAD-Dateien (`stl, dwg, step`).
- **Notfall, wenn nichts reicht:** Feld „Vertrauenswürdige Pfade (überall durchlassen)" – hebt für diese Pfade auch Verzeichnis-Sperren und Exploit-Signaturen auf. **Nur für selbst geprüfte, harmlose Pfade**, nie pauschal.

Faustregel: so eng wie möglich freigeben – lieber die eine Datei als den ganzen Ordner, lieber „ohne PHP". Ist der 403 im Netzwerk-Tab verschwunden, ist es gelöst.

Seite lässt sich nicht per iframe einbetten

Problem: Eine Seite lässt sich nicht mehr per `<iframe>` auf einer anderen Domain einbinden (z. B. ein auf Seite B gehostetes Kontaktformular, eingebunden auf Seite A). Die Browser-Konsole meldet: `Refused to display … X-Frame-Options: SAMEORIGIN`.

Ursache: Der Clickjacking-Schutz „Einbettung in fremde Seiten verbieten (X-Frame-Options)" auf der **eingebetteten** Seite B verbietet die Fremd-Einbettung.

Lösung (auf Seite B, nicht auf A!): unter `HTProtect › Schutzschild › Erweiterte Einstellungen` den Schalter „Einbettung in fremde Seiten verbieten" ausschalten → `Speichern + .htaccess schreiben`. Für öffentliche Formulare unbedenklich.

Site-Scan

Sollte doch einmal etwas durchgerutscht sein, spürt der Site-Scan es auf. Er durchsucht deine ganze Website nach Schadcode, eingeschleusten Dateien und versteckten Hintertüren (sogenannten Web-Shells) – und kann Funde direkt entfernen. Gestartet wird er **nur von dir**, nie von allein; deinen Server belastet er nicht dauerhaft.

Sehr große Seiten scannt er in Häppchen, damit kein Zeitlimit den Vorgang abbricht; ein erneuter Lauf prüft dann nur noch, was sich geändert hat. Zusätzlich kann er testen, ob deine verlinkten Dateien und Downloads erreichbar sind.

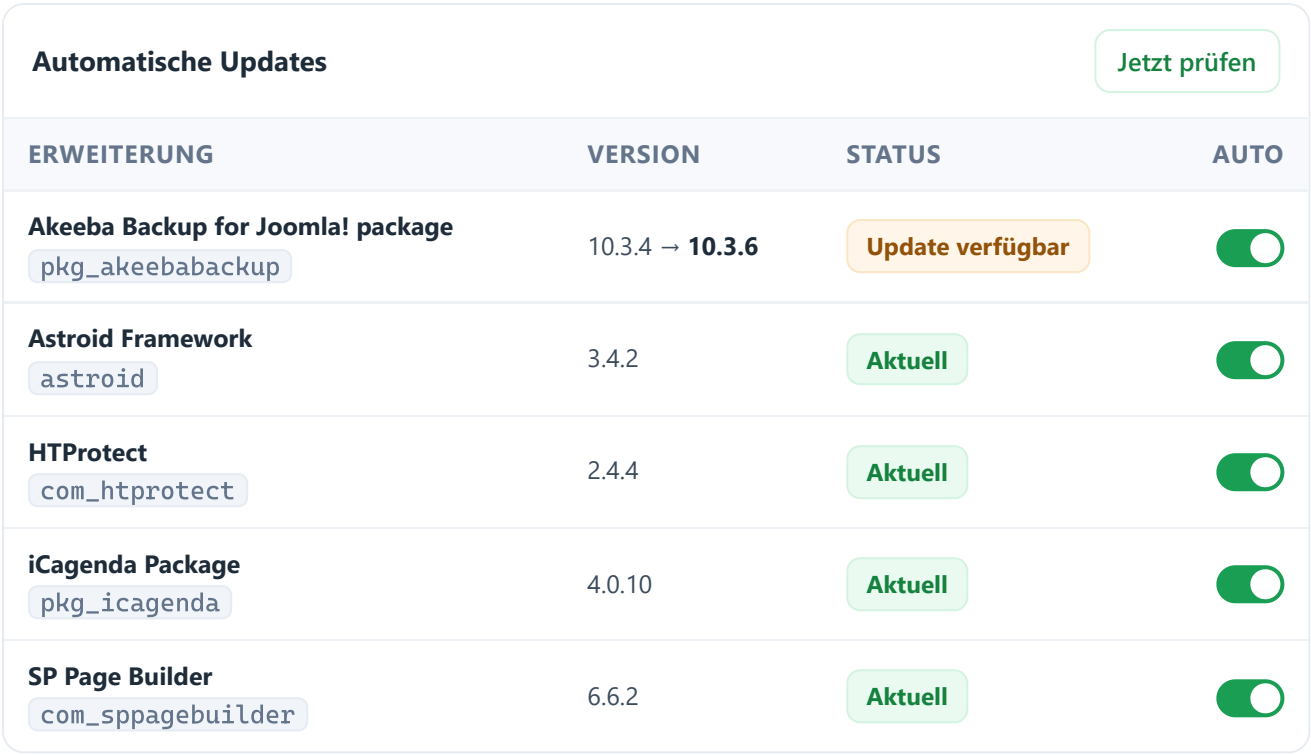
Auch im Kleinen wacht der Scanner mit: **Neu installierte oder aktualisierte Dateien** prüft er auf Schadcode – etwa auf Web-Shells oder eingeschleustes JavaScript. Findet er etwas, kann er es isolieren oder entfernen, und zwar mit strengen Vorkehrungen gegen versehentliche Fehl-Löschungen. Für ein häufiges Muster gibt es eine Spezialbehandlung: in **Helix-Templates** eingeschleustes JavaScript erkennt und entfernt HTProtect gezielt – umkehrbar, mit Backup.

Sicherungen & Updates

Vor **jeder** Änderung an der `.htaccess` legt HTProtect automatisch eine Sicherung an – ein Klick bringt dich jederzeit zum vorherigen Stand zurück. Für Updates gilt dasselbe Prinzip: nie ohne Netz.

Deine Website wartet sich selbst
Automatische Extension-Updates – frei nach deinem Zeitplan.

Auf Wunsch hält HTProtect deine Joomla-Erweiterungen automatisch aktuell. **Vor** jedem Update sichert es Dateien und Datenbank, prüft danach mit einem Gesundheitscheck, ob die Seite noch sauber läuft – und fällt bei Problemen automatisch auf den vorherigen Stand zurück. Standardmäßig werden Sicherheitsupdates bevorzugt, täglich zur eingestellten Zeit.



Die Auto-Update-Übersicht in HTProtect

HTProtect weiß dabei, **was** aktualisiert werden sollte: Es gleicht deine installierten Erweiterungen mit einer Liste bekannter Sicherheitslücken ab und weist gezielt auf verfügbare Updates hin.

Empfehlung: Nicht-Sicherheitsupdates einmal pro Woche laufen lassen, mit 3 Tagen Karenz-Zeit – ein guter Mittelwert.

Das Sicherheitsnetz dahinter:

- **Intervall & Uhrzeit frei wählbar:** wöchentlich, täglich oder „sofort" (im 15-Minuten-Takt).
- **Sicherheits-Updates laufen sofort** – ganz ohne Wartezeit.
- **Karenz-Zeit wählbar:** keine, 1, 3, 7 oder 14 Tage.
- **Malware-Scan beim Update:** bei einem Fund wird sofort zurückgerollt (meist ein Fehlalarm – die Signaturen werden zentral nachgepflegt, ohne site- oder personenbezogene Daten; das Update läuft dann beim nächsten Lauf).
- **Rücksichtsvoll:** Die Update-Quellen werden nie abgeschaltet; fremde Server fragt HTProtect gedrosselt ab, um sie zu schonen.
- **Notbremse:** Entpuppt sich ein Update als hochproblematisch, kann es zentral sofort für alle gesperrt werden.

Hilfe & Support

Hier erreichst du den **Support** (auf Wunsch mit hilfreichen Diagnose-Daten), den **Live-Chat**, diese Dokumentation und die Kaffeekasse.

HTProtect ist darauf ausgelegt, im Zweifel *sanft* nachzugeben statt hart zu versagen. Beschädigt etwa ein übereifriger Server-Virenscanner eine HTProtect-Datei, bleibt deine Seite trotzdem erreichbar: Der betroffene Teil schaltet sich still ab, HTProtect stellt sich über sein Selbst-Update selbst wieder her, und

eine verständliche Hinweisseite erklärt, was los ist. Mit vorhandenen Sicherheits-Tools verträgt es sich (Hands-off-Modus) und hält die Serverlast minimal.

Und willst du HTProtect wieder loswerden? Beim Deinstallieren bietet dir ein Assistent an, die Schutzdateien sauber mitzuentfernen und deine ursprüngliche `.htaccess` wiederherzustellen – spurlos. Ehrlich und umkehrbar, wie alles hier.

Joomla-.htaccess absichern mit HTProtect
Hintergrund-Artikel