BK Modules

Bedingungen der Bereinigung eines gehackten PrestaShop-Shops

VERSION
1.0

GÜLTIG SEIT
12.11.2026

FÜR WEN
Alle, die auf bkmodules.com die Bereinigung eines gehackten PrestaShop-Shops bestellen

Dies ist der Vertrag der Bereinigung eines gehackten PrestaShop-Shops: was wir in Ihrem Shop und auf seinem Server tun, wie schnell, was wir von Ihnen brauchen, was die Garantie abdeckt und wann Sie Ihr Geld zurückbekommen. Es ist ein Vertrag zwischen Unternehmen, nur für Unternehmer und Freiberufler, die für ihre gewerbliche oder berufliche Tätigkeit abschließen (Abschnitt 1). Lesen Sie ihn vor dem Abschluss: Beim Bezahlen setzen Sie ein Häkchen, mit dem Sie bestätigen, dass Sie ihn akzeptieren. Wir schicken Ihnen mit der Bestellbestätigung eine Kopie als PDF, und Sie finden ihn jederzeit in dieser Bestellung in Ihrem Konto.

Was Sie gebucht haben

In Ihrer persönlichen Kopie (der, die Sie beim Bezahlen öffnen, und der, die in Ihrer Bestellung bleibt) ist angekreuzt, was Sie buchen, und am Ende steht die „Kostenübersicht“ mit dem Preis.

☐ Bereinigung eines gehackten PrestaShop-Shops und seines Servers, in weniger als 24 Stunden und mit 30 Tagen Garantie (Abschnitte 5, 7 und 8).

Der Preis ist ein Festpreis und ändert sich nicht mit den Stunden, die uns die Arbeit kostet. Er steht nicht in diesem Text, weil er von der Währung und den Bedingungen Ihres Kontos abhängt: Es ist der Preis, den Sie beim Bezahlen sehen, bevor Sie die Bestellung bestätigen, und er steht in der „Kostenübersicht“ am Ende Ihrer Kopie dieses Vertrags und in Ihrer Bestellung, mit der Währung, den Steuern und etwaigen Rabatten. Er wird vollständig im Voraus bezahlt, und wir beginnen, sobald die Zahlung bestätigt ist. Wenn Ihr Land Sie verpflichtet, für diesen Kauf eine Steuer zu erklären, ist diese Erklärung Ihre Sache.

1. Wer diesen Vertrag schließt

Auf der einen Seite die BK Modules LLC, die unter dem Handelsnamen BK Modules auftritt: eine im Bundesstaat New Mexico (USA) gegründete Gesellschaft mit beschränkter Haftung mit Sitz in 102 Gold Ave SW, Albuquerque, NM 87102, USA, und der US-amerikanischen Steuernummer (EIN) 35-2838640. E-Mail: bkmodules@bkmodules.com. Telefon: +1 (813) 214-0078. In diesem Vertrag „wir“.

Auf der anderen Seite das Unternehmen oder der Freiberufler, das bzw. der mit seinem Konto auf bkmodules.com abschließt. In diesem Vertrag „Sie“. Wenn Sie im Namen eines Unternehmens oder eines Ihrer Kunden abschließen, bestätigen Sie uns, dass Sie dazu berechtigt sind und dass dieses

Unternehmen oder dieser Kunde an diesen Vertrag gebunden ist.

Nur für Unternehmer und Freiberufler

Dieser Vertrag gilt nur für Unternehmer und Freiberufler, die die Bereinigung für ihre gewerbliche oder berufliche Tätigkeit buchen. Mit dem Abschluss erklären Sie, dass das bei Ihnen der Fall ist. Das Verbraucherschutzrecht findet keine Anwendung, und es gibt kein Widerrufsrecht.

2. Was dieser Vertrag regelt

Die Bereinigung eines gehackten PrestaShop-Shops ist eine Leistung, die Sie einmal bezahlen: Wir bereinigen einen angegriffenen PrestaShop-Shop und seinen Server, schließen die Lücke, durch die die Angreifer hereingekommen sind, und geben Ihnen 30 Tage Garantie. Sie verlängert sich nicht und wird nicht erneut abgerechnet. Für alles, was dieser Vertrag nicht regelt, gelten die Allgemeinen Geschäftsbedingungen von bkmodules.com, und wenn beide zur Bereinigung Unterschiedliches sagen, geht dieser Vertrag vor.

3. Begriffe, die wir verwenden

- **Shop**: die PrestaShop-Installation, die Sie beim Abschluss angeben, mit ihrer Domain. Die Bereinigung gilt für genau einen Shop.
- **Server**: die Maschine, auf der der Shop installiert ist, ob Server, VPS oder Hosting-Paket. Die Bereinigung gilt für genau einen Server.
- **Zugänge**: die Benutzer, Passwörter, Schlüssel und Verbindungsdaten, die Sie uns geben, damit wir im Shop und auf dem Server arbeiten können.
- **Schadcode**: alles, was jemand ohne Ihre Erlaubnis im Shop oder auf dem Server abgelegt hat, um Daten oder Zahlungen zu stehlen, Ihre Besucher umzuleiten, Spam zu versenden oder wieder hereinzukommen. Das kann eine Datei sein, Code, der in eine saubere Datei eingeschleust wurde, Daten in der Datenbank, ein Benutzer, ein Schlüssel oder eine geplante Aufgabe.
- **Einfallstor**: die Schwachstelle, durch die der Angreifer hereingekommen ist. Zum Beispiel ein Modul mit einer bekannten Sicherheitslücke, ein gestohlenes Passwort oder eine vergessene Datei auf dem Server.
- **Bericht**: das Dokument, das wir Ihnen am Ende schicken, mit dem, was wir gefunden und getan haben, und dem, was wir Ihnen empfehlen.
- **Übergabe**: der Zeitpunkt, zu dem wir Ihnen den Bericht schicken und Ihnen sagen, dass die Arbeit erledigt ist.
- **Neuinfektion**: wenn nach der Übergabe wieder Schadcode im Shop oder auf dem Server auftaucht.

4. Was wir für die Arbeit brauchen: Ihre Zugänge

Um anzufangen, brauchen wir zwei Zugänge: SSH zum Server mit dem Benutzer root, also mit voller Kontrolle über den Server, und das PrestaShop-Backoffice mit einem SuperAdmin-Profil. Ohne root fassen wir nichts an: Die Frist beginnt nicht, und bekommen Sie ihn nicht innerhalb von 7 Tagen nach der Zahlung, gilt die Erstattung aus Abschnitt 9.

Sie geben sie uns in Ihrem Konto auf bkmodules.com, in dem Formular, das wir Ihnen mit der

Zahlungsbestätigung verlinken. Liegt Ihr Shop auf einem Shared Hosting, fragen Sie vor der Buchung Ihren Anbieter, ob er Ihnen root gibt.

Was ein Angreifer hinterlässt, liegt meist außerhalb des Shop-Ordners: in geplanten Aufgaben, bei anderen Systembenutzern oder in Dateien, die man mit einem eingeschränkten Zugang weder sehen noch anfassen kann. Mit einem eingeschränkten Zugang wüssten wir nicht, ob der Server sauber ist, deshalb beginnen wir nur mit root. Funktioniert root während der Arbeit nicht mehr, unterbrechen wir, bis er wieder geht.

Die Updates der Module

Außerdem brauchen wir die Updates der Module, die aktualisiert werden müssen, denn ein Modul mit einer Sicherheitslücke bleibt eine offene Tür. Wir sagen Ihnen, welche, sobald wir sie finden. Module anderer Hersteller werden über Ihr Konto auf deren Website oder bei PrestaShop Addons heruntergeladen, weil die Lizenz Ihnen gehört: Sie geben uns die Dateien oder den Zugang zu diesem Konto. Muss für die neue Version eine Lizenz oder ein Support gekauft oder verlängert werden, ist diese Zahlung Ihre Sache.

Braucht eine Arbeit Ihr Hosting-Panel (zum Beispiel Plesk oder cPanel), Ihr Konto in der Google Search Console oder einen anderen Dienst, fragen wir Sie danach, und Sie geben ihn uns über dasselbe Formular.

Wie wir Ihre Zugänge aufbewahren

- Verschlüsselt, in einem Passwortmanager. Niemals in E-Mails, Tickets oder Dokumenten.
- Nur die Personen, die an Ihrem Shop arbeiten und zur Verschwiegenheit verpflichtet sind, verwenden sie, und nur für diesen Vertrag.
- Wir geben sie an niemanden weiter, es sei denn, ein Gesetz oder ein Gericht verpflichtet uns dazu. In diesem Fall informieren wir Sie, sofern es uns erlaubt ist.
- Wir bewahren sie bis zum Ende der Garantie auf, damit wir bei einer Neuinfektion wieder hineinkommen. Bitten Sie uns, sie früher zu löschen, tun wir das, und um danach die Garantie zu nutzen, müssen Sie sie uns erneut geben.
- Wenn der Vertrag endet, löschen wir sie. Haben wir einen eigenen SSH-Schlüssel auf dem Server installiert, entfernen wir ihn, sofern wir noch Zugang haben. Trotzdem empfehlen wir Ihnen, die Passwörter zu ändern, die Sie uns gegeben haben.
- Haben wir den Verdacht, dass jemand unbefugt Kenntnis von Ihren Zugängen erlangt haben könnte, informieren wir Sie unverzüglich, damit Sie sie ändern.

5. Was wir tun

1. Bevor wir irgendetwas anfassen, kopieren wir die Dateien und die Datenbank des Shops so, wie sie sind. Mit der Kopie lässt sich eine Änderung bei Bedarf rückgängig machen, und sie belegt, was vorhanden war.
2. Wir suchen Schadcode in den Dateien des Shops und des Servers, in der Datenbank, bei den Benutzern, in den geplanten Aufgaben und in den Logs des Servers und finden heraus, was das Einfallstor war.
3. Wir entfernen den Schadcode aus den Dateien und der Datenbank, zusammen mit den Benutzern, Schlüsseln und Aufgaben, die der Angreifer hinterlassen hat. Ist eine Datei von PrestaShop oder einem Modul verändert, ersetzen wir sie durch das Original derselben Version.

4. Wir schließen das Einfallstor, damit niemand mehr auf diesem Weg hereinkommt: Je nach Fall aktualisieren oder korrigieren wir das betroffene Modul, entfernen die vergessene Datei oder ändern das gestohlene Passwort. Mit den Dateien, die Sie uns geben (Abschnitt 4), aktualisieren wir auch die anderen Module des Shops, die eine bekannte Sicherheitslücke haben.
5. Wir härten das System in den Grundzügen. Wir ändern die Passwörter und Schlüssel der PrestaShop-Administratoren, der Datenbank und des Servers und geben Ihnen die neuen. Wir entfernen Administratoren und Benutzer, die Sie nicht kennen, den Installationsordner und überflüssige Dateien, setzen die Dateirechte richtig und verhindern, dass in den Ordnern, in die Bilder und Dokumente hochgeladen werden, Code ausgeführt wird.
6. Wir bringen den Server mit allen Änderungen auf den neuesten Stand, die in unserer Hand liegen: Paket-Updates, Sicherheitspatches, Konfiguration und bei Bedarf die PHP-Version, die wir auf die höchste anheben, die Ihr PrestaShop und seine Module unterstützen. Das Einzige, was wir nicht tun, ist, den Server auf eine andere Version des Betriebssystems zu bringen (Abschnitt 6).
7. Warnt Google oder der Browser Ihre Besucher, der Shop sei gefährlich, oder steht Ihre Domain auf einer Spam-Liste und Ihre E-Mails kommen nicht an, bitten wir zum Schluss die Stelle, die die Warnung ausgegeben hat, den Shop erneut zu prüfen. Bei Google tun wir das über die Search Console, mit Ihrem Zugang. Ob die Warnung entfernt wird, entscheiden sie, und das dauert meist zwischen einigen Stunden und einigen Tagen.
8. Wir schicken Ihnen den Bericht mit dem, was wir gefunden haben, wie die Angreifer hereingekommen sind, was wir getan haben und was wir Ihnen empfehlen. Die Empfehlungen, die für die Garantie nötig sind, sind markiert, jede mit ihrer Frist.

Was der Angriff oder unsere Bereinigung im Shop kaputtmacht, reparieren wir im Rahmen dieser Arbeit. Muss der Shop für die Bereinigung eine Zeit lang für Besucher geschlossen werden oder kann sich eine Änderung auf den Verkauf auswirken, erklären wir es Ihnen vorher und warten auf Ihre Zustimmung.

Die Kopie aus dem ersten Punkt bewahren wir bis zum Ende der Garantie auf und löschen sie danach. Wenn Sie den Angriff anzeigen wollen, fordern Sie sie vorher bei uns an, dann geben wir sie Ihnen.

6. Was die Bereinigung nicht umfasst

- Die Aktualisierung von PrestaShop, weder auf eine andere Version noch auf einen Patch derselben Version, auch dann nicht, wenn Ihre Version keine PHP-Version unterstützt, die noch Sicherheitspatches bekommt. Lässt sich das Einfallstor nur durch eine Aktualisierung schließen, sagen wir es Ihnen im Bericht und erstellen Ihnen dafür ein separates Angebot.
- Den Wechsel des Servers auf eine andere Version des Betriebssystems. Ist er nötig, muss der Shop eventuell auf einen anderen Server oder zu einem anderen Hosting umziehen, was wir Ihnen separat anbieten und mit Ihnen abstimmen.
- Die Wartung nach der Übergabe. Den Shop zu überwachen, ihn zu aktualisieren und zu reparieren, was ab dann nicht funktioniert, ist ein anderer Vertrag: die PrestaShop-Wartung.
- Die Wiederherstellung von Daten, die der Angriff gelöscht oder beschädigt hat, etwa Bestellungen, Kunden, Produkte oder Bilder. Haben Sie ein sauberes Backup, sagen wir Ihnen, was sich daraus zurückholen lässt, als separate Arbeit.

- Die Behebung von Fehlern, die nicht vom Angriff kommen, die Entwicklung neuer Funktionen oder Änderungen am Design.
- Den Kauf von Lizenzen oder Verlängerungen für Module anderer Hersteller.
- Besucher oder Google-Positionen zurückzuholen, die Sie durch den Angriff verloren haben. Bei Warnungen von Google, Browsern und Spam-Listen ist das Beantragen der erneuten Prüfung enthalten (Abschnitt 5).
- Andere Websites, Shops oder Konten auf demselben Server sowie E-Mail-Konten. Sehen wir, dass sie ebenfalls infiziert sind, sagen wir es Ihnen.
- Ein Gutachten oder einen Bericht mit Beweiskraft vor Gericht, die Anzeige sowie die Benachrichtigung Ihrer Kunden, Ihrer Bank, Ihres Zahlungsanbieters oder der Datenschutzbehörde.

Was nicht enthalten ist, bewerten wir und bieten es Ihnen separat an, und Sie entscheiden.

7. Wie schnell

Wir übergeben Ihnen den Shop bereinigt in weniger als 24 Stunden, durchgehend gezählt, tagsüber und nachts, an allen Tagen der Woche, auch an Wochenenden und Feiertagen.

- Die 24 Stunden beginnen, wenn wir beide Zugänge aus Abschnitt 4 haben und sie funktionieren: SSH mit root und das Backoffice mit SuperAdmin-Profil. Vorher fangen wir nicht an. Fehlt einer oder funktioniert er nicht, sagen wir es Ihnen, sobald wir es bemerken.
- Die Frist ruht, solange wir auf etwas warten, das nur Sie uns geben können, ab dem Moment, in dem wir Sie darum bitten, bis wir es haben: das Update eines Moduls, einen weiteren Zugang, root, wenn er nicht mehr funktioniert, oder Ihre Zustimmung zu einer Änderung, die sich auf den Verkauf auswirkt.
- Die Frist endet mit der Übergabe.

8. 30 Tage Garantie

Kommt es innerhalb von 30 Tagen nach der Übergabe zu einer Neuinfektion, bereinigen wir den Shop und den Server kostenlos erneut, sofern alle Arbeiten aus Abschnitt 5 durchgeführt werden konnten. Dafür muss all das zutreffen:

- Alle Module, deren Aktualisierung wir von Ihnen verlangt haben, wurden aktualisiert.
- Sie haben die Empfehlungen, die der Bericht als für die Garantie nötig markiert, fristgerecht umgesetzt.
- Ließ sich das Einfallstor nur durch eine Aktualisierung von PrestaShop oder des Betriebssystems schließen, ist diese Aktualisierung erfolgt.
- Niemand hat rückgängig gemacht, was wir getan haben, oder das Einfallstor wieder geöffnet.

Wann es keine Garantie gibt

Die Garantie deckt eine Neuinfektion in diesen Fällen nicht ab:

- Ein Modul, dessen Aktualisierung wir verlangt haben, ist immer noch nicht aktualisiert, oder Sie haben uns seine Dateien nicht gegeben.
- Sie haben die als für die Garantie nötig markierten Empfehlungen nicht umgesetzt.
- Jemand (Sie, Ihr Team, ein anderer Dienstleister oder Ihr Hoster) ändert, was wir getan haben,

installiert neue Module oder Themes oder verändert etwas am Server, und dadurch öffnet sich das Einfallstor wieder oder ein neues.
- Der Angreifer kommt mit einem gültigen Passwort herein, das außerhalb des Shops und des Servers gestohlen wurde: auf Ihrem Computer, aus Ihrem E-Mail-Postfach, aus Ihrem Hosting-Panel oder bei einer Person aus Ihrem Team.
- Der Angriff kommt von anderen Websites oder Konten auf demselben Server, die nicht zur Bereinigung gehören, oder von der Infrastruktur Ihres Hosting-Anbieters.
- Der Angriff nutzt eine Sicherheitslücke aus, die am Tag der Übergabe öffentlich nicht bekannt war.
- Sie melden sich nach Ablauf der 30 Tage.

So nehmen Sie sie in Anspruch

Schreiben Sie uns innerhalb der 30 Tage an bkmodules@bkmodules.com und beschreiben Sie, was Sie sehen. Wir prüfen, ob es sich um eine Neuinfektion handelt und ob die Garantie sie abdeckt, und sagen es Ihnen. Deckt sie sie ab, bereinigen wir sie in weniger als 24 Stunden ab dem Zeitpunkt, an dem wir funktionierende Zugänge haben, root eingeschlossen, nach den Regeln aus Abschnitt 7, und die Garantie läuft ab dieser neuen Übergabe erneut 30 Tage. Deckt sie sie nicht ab, erklären wir Ihnen, warum, und erstellen Ihnen ein Angebot für die Bereinigung.

9. Wann Sie Ihr Geld zurückbekommen

Können wir die Arbeit aus einem Grund nicht erledigen, der bei uns liegt, erstatten wir Ihnen alles, was Sie bezahlt haben.

Kann sie aus einem Grund nicht erledigt werden, der nicht bei uns liegt, erstatten wir Ihnen den gezahlten Betrag abzüglich 99 € Bearbeitungskosten. Sie decken die Zeit, die wir für Ihren Shop reservieren, die Prüfung dessen, was Sie uns geben, und die Abwicklung von Zahlung und Erstattung. Haben Sie in einer anderen Währung bezahlt, ziehen wir den entsprechenden Betrag in dieser Währung ab, der in der „Kostenübersicht“ steht. Das gilt nur in diesen Fällen:

- Sie haben uns innerhalb von 7 Tagen nach der Zahlung die Zugänge aus Abschnitt 4 nicht mit root gegeben, obwohl wir Sie darum gebeten und daran erinnert haben. Da wir ohne root nicht anfangen, erstatten wir Ihnen nach diesen 7 Tagen den Betrag mit diesem Abzug.
- Die Zugänge, die Sie uns geben, funktionieren nicht, oder root funktioniert während der Arbeit nicht mehr, und Sie beheben das nicht innerhalb von 7 Tagen nach unserem Hinweis.
- Ihr Hosting-Anbieter verhindert die Arbeit, weil er keinen root-Zugang gibt, das Konto sperrt oder den Eingriff blockiert, und das wird nicht innerhalb von 7 Tagen gelöst.
- Sie stornieren den Auftrag, bevor wir beginnen, also bevor wir uns zum ersten Mal mit Ihren Zugängen im Shop oder auf dem Server anmelden.
- Was bereinigt werden muss, ist nicht das Gebuchte, weil es kein PrestaShop-Shop ist oder es mehrere Shops oder Server sind, und Sie nehmen das Angebot für das, was über einen Shop und einen Server hinausgeht, nicht an.

Bleibt die Arbeit aus einem dieser Gründe halb fertig, schicken wir Ihnen auch, was wir bis dahin gefunden haben.

Nach der Übergabe gibt es keine Erstattung. Außerhalb der Fälle dieses Abschnitts wird der gezahlte Betrag nicht erstattet.

Wir erstatten den Betrag innerhalb von 14 Tagen, nachdem der Fall eingetreten ist, über dasselbe Zahlungsmittel, mit dem Sie bezahlt haben.

10. Ihre Pflichten

- Uns die Zugänge aus Abschnitt 4 mit root und die Updates der Module zu geben und die Zugänge bis zum Ende der Garantie aktuell zu halten.
- Die nötigen Lizenzen oder Verlängerungen für Module anderer Hersteller zu bezahlen.
- Unsere Fragen so schnell wie möglich zu beantworten. Solange wir auf Ihre Antwort warten, ruht die Frist.
- Während wir arbeiten, nichts im Shop oder auf dem Server zu ändern und es auch niemand anderem zu erlauben. Wenn eine andere Person oder ein anderes Unternehmen ebenfalls daran arbeitet, sagen Sie es uns.
- Die Empfehlungen des Berichts umzusetzen, vor allem die als für die Garantie nötig markierten.
- Berechtigt zu sein, das zu nutzen, was sich im Shop befindet: das Theme, die Module und ihre Lizenzen sowie die Inhalte.
- Die Leistung für rechtmäßige Zwecke zu nutzen, ohne von uns etwas zu verlangen, was gegen das Gesetz oder die Rechte anderer verstößt.

11. Vertraulichkeit und personenbezogene Daten

Alles, was wir bei der Arbeit im Shop und auf dem Server von Ihrem Geschäft sehen (Daten, Umsätze, Konfiguration, Code, Dokumente), ist vertraulich. Wir verwenden es nur für diesen Vertrag und geben es an niemanden weiter, auch nicht nach Vertragsende. Das gilt nicht für das, was bereits öffentlich ist, und nicht für das, was wir aufgrund eines Gesetzes oder einer gerichtlichen Anordnung offenlegen müssen.

Wie wir Ihre Daten verarbeiten, steht in der Datenschutzerklärung.

Bei der Arbeit im Shop verarbeiten wir personenbezogene Daten Ihrer Kunden. Für diese Daten sind Sie der Verantwortliche und wir sind Ihr Auftragsverarbeiter, mit den Verpflichtungen aus dem Abschnitt „Die Daten Ihrer Kunden, wenn wir in Ihrem Shop arbeiten“ der Allgemeinen Geschäftsbedingungen, die Bestandteil dieses Vertrags sind: sie nur für diese Arbeit und nach Ihren Weisungen zu verarbeiten, mit Vertraulichkeit und geeigneten Sicherheitsmaßnahmen; Sie unverzüglich über jede Verletzung zu informieren; keine weiteren Auftragsverarbeiter einzusetzen, ohne Sie vorher zu informieren; Sie bei der Erfüllung der Rechte Ihrer Kunden zu unterstützen und am Ende zu löschen, was wir haben. Da wir in den USA ansässig sind, erfolgt der Zugriff auf diese Daten mit den Garantien, die die Europäische Union für solche Fälle anerkennt und die in der Datenschutzerklärung beschrieben sind.

Wenn der Angriff Daten Ihrer Kunden offengelegt hat

Im Bericht sagen wir Ihnen, welche Daten Ihrer Kunden für den Angreifer erreichbar waren und, falls es sich feststellen lässt, ob er sie mitgenommen hat. Ob die Datenschutzbehörde, Ihre Kunden oder Ihr Zahlungsanbieter benachrichtigt werden müssen, entscheiden Sie als Verantwortlicher, und die Benachrichtigung ist Ihre Sache. In der Europäischen Union muss die Behörde innerhalb von 72 Stunden benachrichtigt werden, nachdem die Verletzung bekannt geworden ist. Wenn Sie glauben, dass das auf Sie zutrifft, fangen Sie also mit der Vorbereitung an, ohne auf den Bericht zu

warten.

12. Haftung

Wir arbeiten an Ihrem Shop mit der Gewissenhaftigkeit und dem Fachwissen eines Profis und verpflichten uns, die Arbeit aus Abschnitt 5 gut und innerhalb der Frist aus Abschnitt 7 zu erledigen und die Garantie aus Abschnitt 8 einzuhalten. Niemand kann zusichern, dass ein Shop nie wieder angegriffen wird, und bei einer Neuinfektion schulden wir Ihnen diese Garantie.

Wir haften nicht für:

- mittelbare Schäden wie entgangenen Gewinn, Verlust von Umsätzen, Kunden oder Daten und Unterbrechungen Ihres Geschäftsbetriebs;
- die Folgen des Angriffs, etwa abgeflossene Daten oder Zahlungen, Bußgelder, Forderungen Ihrer Kunden und Warnungen von Google und Virenscannern;
- das, was Ihr Hosting-Anbieter, Module, Themes und Dienste von Drittanbietern, Änderungen anderer am Shop oder am Server und fehlende Zugänge oder Backups verursachen;
- das, was wir auf Ihre Weisung hin tun.

Unsere Gesamthaftung aus diesem Vertrag übersteigt nicht den Betrag, den Sie uns dafür bezahlt haben. Nichts davon beschränkt unsere Haftung für Vorsatz oder grobe Fahrlässigkeit oder die Haftung, die gesetzlich nicht beschränkt werden darf.

Wir haften auch nicht für Verzögerungen aufgrund von Ereignissen, die wir vernünftigerweise nicht beeinflussen können, etwa allgemeine Ausfälle des Internets oder des Stromnetzes, der Zahlungsdienste oder der Dienste von Drittanbietern, auf die wir angewiesen sind.

13. Wann der Vertrag endet

- Mit dem Ende der Garantie, 30 Tage nach der Übergabe oder nach der letzten Bereinigung im Rahmen der Garantie, oder wenn wir Ihnen Ihr Geld erstatten (Abschnitt 9).
- Wir können die Arbeit abbrechen, wenn Sie etwas Rechtswidriges von uns verlangen oder die Zugänge oder die Leistung nutzen, um anderen zu schaden, nachdem wir Sie darauf hingewiesen haben, es sei denn, die Schwere des Verstoßes erfordert sofortiges Handeln.
- Am Ende löschen wir Ihre Zugänge wie in Abschnitt 4 beschrieben, die Kopie des Zustands, in dem wir den Shop vorgefunden haben, und die Arbeitskopien. Den Bericht behalten Sie.

14. Elektronische Kommunikation

Sie sind damit einverstanden, dass dieser Vertrag, der Bericht und die übrige Kommunikation zur Bereinigung Sie auf elektronischem Weg erreichen: per E-Mail an die Adresse Ihres Kontos und in Ihrem Konto auf bkmodules.com. Um sie zu empfangen, brauchen Sie nur einen Browser, ein E-Mail-Programm und die Möglichkeit, ein PDF zu öffnen. Sie können von uns kostenlos eine Papierkopie jedes dieser Dokumente verlangen. Halten Sie Ihre E-Mail-Adresse aktuell, denn Hinweise, die wir an sie senden, gelten als zugestellt.

15. Änderungen dieses Vertrags

Wir können diesen Vertrag aktualisieren. Jede Version trägt ihre Nummer und das Datum, ab dem sie gilt, und sie gilt für Bereinigungen, die ab diesem Datum gebucht werden. Für Ihre Bereinigung samt Garantie gilt immer die Version, die Sie beim Bezahlen akzeptiert haben.

16. Anwendbares Recht und Gerichtsstand

Dieser Vertrag unterliegt dem Recht des Bundesstaats New Mexico und dem anwendbaren Bundesrecht der Vereinigten Staaten.

Für alle Streitigkeiten sind die einzelstaatlichen oder bundesstaatlichen Gerichte mit Sitz im Bernalillo County (Albuquerque, New Mexico) zuständig.

17. Kontakt

BK Modules LLC · 102 Gold Ave SW, Albuquerque, NM 87102, USA · bkmodules@bkmodules.com · +1 (813) 214-0078