Kundeninformation 2016-01 der A.B.C... Promotion vom 1. September 2016

Und Ihre WebSite ist ebenfalls ein Angriffsziel

(Zusammenfassung)

Die Aktivitäten der Hacker im Internet ist in den letzten Monaten dramatisch angestiegen. Es ist Zeit, dass Sie und ich Abwehrmassnahmen auch für Ihre Website ergreifen. Denn es ist absolut nicht witzig, wenn Ihre Besucher plötzlich Virenwarnungen erhalten, gar nicht auf Ihre Site kommen oder Ihr WebServer als SPAM-Schleuder zum Versand von Massenmails missbraucht wird. Bitte nehmen Sie sich die Zeit, die nachfolgenden Detail-Informationen zu lesen.

Was sollten Sie unternehmen?

1. Beauftragen Sie ABC Promotion für die Dienstleistung „Intensiv-Wartung"

Ihre Joomla Installation wird alle zwei Monate auf Aktualität überprüft. Allfällig veraltete Bausteine werden aktualisiert. Das verhindert wirkungsvoll, dass Hacker Ihre WebSite angreifen können.

2. Beauftragen Sie ABC Promotion mit der Installation des Services Safeguarding

Für nur **Euro 9.95** im Monat wird Ihr Server täglich auf Viren und Malware gescannt und falls eine Infektion erfolgt ist, wird die Malware automatisiert entfernt und der Server wird wieder sauber. Zudem haben Sie im Hintergrund den Support von Experten für Server-Sicherheit zur Hand, wenn mal was besonders Schwerwiegendes eintreten sollte.

Warten Sie nicht, bis es zu spät ist!

Und Ihre WebSite ist ebenfalls ein Angriffsziel

So las man es in den Medien:

Cyberattacke auf Schweizer Onlineshops
Zum Kreis der Betroffenen gehörten gleich mehrere Onlineshops der beiden grossen Schweizer Detailhändler. Bei der Migros waren es jene von M-Electronics, Micasa und Do-it-Garden sowie der Online-Supermarkt Leshop.ch. Der grösste Schweizer Onlinehändler Digitec, der mehrheitlich dem Migros-Genossenschaftsbund gehört, war ebenfalls Opfer der Attacke. Bei Coop waren es die Onlineshops von Interdiscount und Microspot. Bei den SBB war laut Sprecher Reto Schärli am Dienstagnachmittag die Website aufgrund der Attacke während rund einer Stunde nur eingeschränkt verfügbar.

Nach Hackerangriff: Sage bestätigt Verlust von Kundendaten
Die Sage Group hat einen Einbruch in seine Computersysteme bestätigt. Der oder die unbekannten Täter hatten Zugriff auf Daten ausschließlich von britischen Kunden. Möglicherweise sind zwischen 200 und 300 Firmen betroffen, die Finanzsoftware von Sage einsetzen.

Sparkasse warnt Website-Nutzer vor Virus
Wer am Montag die Internetseiten von Sparkasse.de besucht hat, könnte sich dabei auf seinem Computer einen Virus eingefangen haben. Die Sparkasse empfiehlt deshalb den Einsatz eines Virenprogrammes.

Diese Firmen haben alle fähige IT-Spezialisten. Und trotzdem...

Hacker haben versucht, den Rüstungsbetrieb Ruag und das Verteidigungsdepartement VBS auszuspionieren.
Unklar ist, welche Schäden die Angreifer anrichteten. Bundesrat Guy Parmelin bestätigte Recherchen der Zeitungen de «Tages-Anzeiger» und «Der Bund». «Die Angriffe dienten der Industriespionage», sagte Parmelin in einem Interview.

CNN: FBI untersucht russischen Hackerangriff auf die «New York Times»
New York - Das FBI untersucht nach CNN-Informationen einen russischen Hackerangriff auf Reporter der «New York Times» und andere US-Medienunternehmen. Der Sender berief sich auf Regierungsinformationen. Die amerikanische Bundespolizei und Sicherheitskreise sähen den russischen Geheimdienst als Urheber der Angriffe in den vergangenen Monaten.

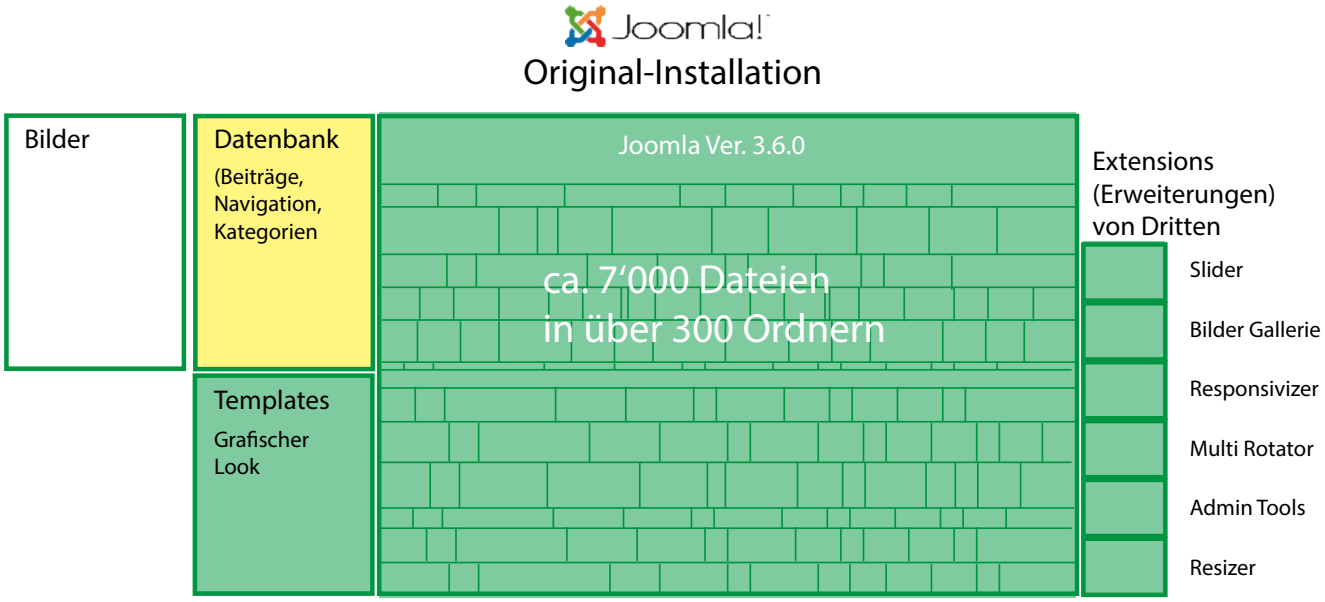
Oder haben sowas erlebt

„Warum sehen die Besucher meine Internet-Seite nicht?“

Sie glauben gar nicht, was zur Zeit im Internet abläuft. Es ist eine Frage der Zeit, bis Ihr Internet-Auftritt „down“ ist.

Wie ist ein Hacker Angriff möglich?

Ihre Website ist mit dem Content Management Tool JOOMLA aufgebaut. Dies ist ein äusserst populäres Werkzeug, welches über 30 Mio. mal installiert ist. Es weist zum Beispiel den Vorteil auf, dass es über einen riesigen Funktionsreichtum verfügt und Sie die Möglichkeit haben, selber Inhalte beizufügen. Weil es über eine so grosse Popularität blicken kann, sind Tausende von Entwicklern motiviert, Erweiterungen (Extensions) zu schreiben und der Joomla Gemeinde entgeltlich oder oft kostenlos zur Verfügung zu stellen. Das gibt wiederum mehr Flexibilität und hohe Funktionalität. Aber: die Kehrseite ist, dass Hacker eben auch um die ungemein grosse Popularität von Joomla wissen. Es ist deshalb für sie oft lohnend, Joomla-Installationen anzugreifen.



Ist eine WebSite mal gestaltet und mit Inhalten gefüllt freut man sich am gelungenen Werk. Aber es ist ein Zustand, der jetzt gut und sicher ist. Das Team von Joomla muss immer wieder erfahren, dass seine äusserst beliebte Software ein Ziel eines Hackerangriffs wurde. In der Regel steht innert wenigen Tagen ein Update zur Verfügung, welches die Sicherheitslücken schliesst. ABC Promotion ist deshalb auch bedacht, schnellstmöglich die neueste Version auf den Server zu laden um Sicherheitsrisiken zu minimieren. Seit Version 3 hat Joomla diese Updates automatisiert. Logt sich der Super User in das Backoffice ein macht Joomla eine Meldung, dass eine neue Version zur Verfügung steht und bietet sie zur Installation an.

Soweit so gut. Das Problem liegt aber vielfach nicht an Joomla selber, sondern an den Extensions von Drittanbietern. Diese updaten sich nicht von selber, haben aber eben auch das Problem, dass sich der Autor einer Sicherheitslücke bewusst wird. Auch er wird zeitnah eine neue Version ohne diese Sicherheitslücke und oft natürlich auch mit weiteren Verbesserungen an den Funktionen herausbringen.

Davon erfährt man als WebSite Betreuer aber leider nichts. Man muss immer wieder systematisch auf die Suche gehen. Eine Extension für eine Bildergalerie ist beispielsweise auf 9 Kundensites installiert. Wenn man nicht einen erheblichen Aufwand betreibt, immer wieder zu kontrollieren ob was Neues zur Installation bereitstünde, geht das schlicht aus den Augen verloren.

Neben dem Joomla Kern und den Extensions gibt es auch auf den Servern immer wieder Weiterentwicklungen. So z.B. für PHP (was die Skriptsprache ist, die Joomla benützt), bei MySQL was die Datenbank ist, auf die sich Joomla stützt und vieles weitere, was an Software auf den Servern installiert ist. Als Kunde merken Sie davon überhaupt nichts und das soll auch so sein. Aber Sicherheitsrisiken entstehen auch dort.

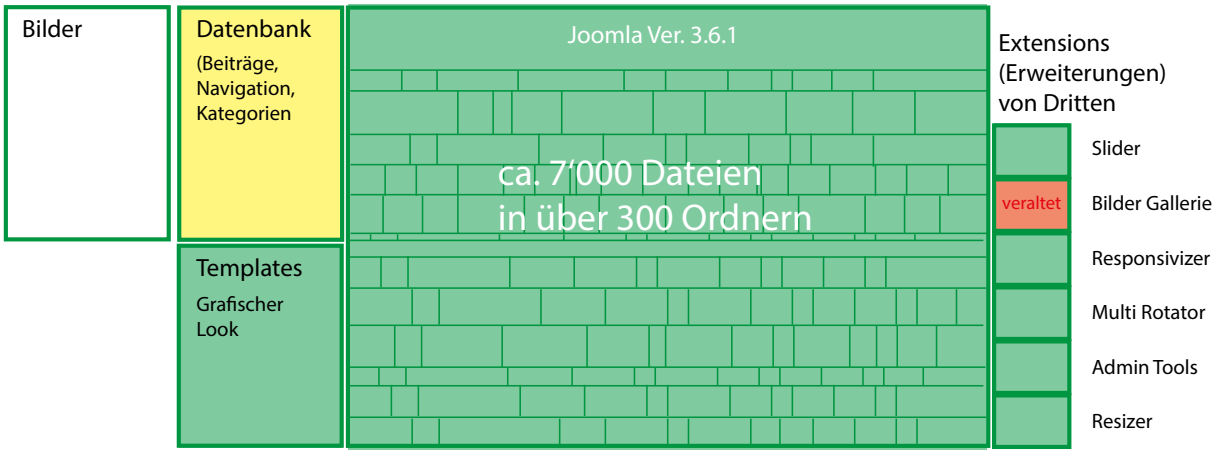
Zusammenfassend ist folgende Erkenntnis wichtig:

Eine WebSite, einmal gestaltet und aufgebaut ist nicht eine Errungenschaft fürs Leben. Die Welt rund herum verändert sich, der technische Zustand einer Site veraltet von Monat zu Monat. Irgendwann kommt der Moment, wo ein Hacker herausfindet, dass sie nicht mehr so frisch ist wie sie aussieht und schlägt zu. Warum die das tun? Weil viel Geld verdient werden kann, wenn es jemandem gelingt, einen WebServer beispielsweise als SPAM-Schleuder zu missbrauchen, indem er pro Nacht ein paar Hunderttausend Mails verschickt.

A.B..C...
Promotion

Joomla!

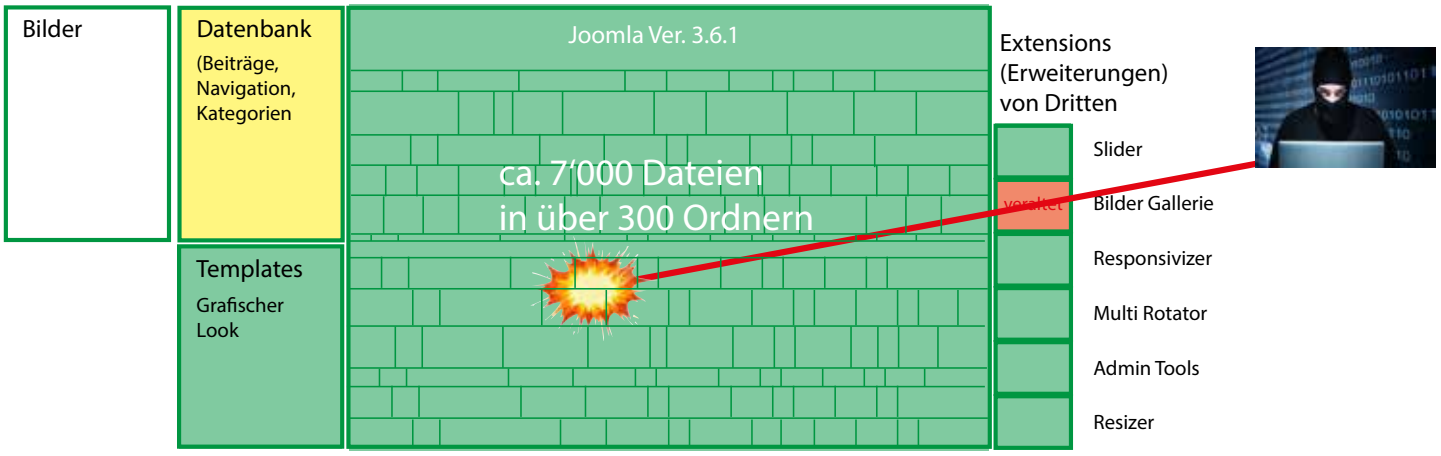
Nach zwei Monaten



Die veraltete Extension stellt ein Sicherheitsrisko dar

Joomla!

Nach drei Monaten...



Ein Hacker nutzt die entstandene Sicherheitslücke aus und schreibt Malware Scripts auf Ihre WebSite.

Das Problem ist, dass man das überhaupt merkt. Je nach Art der Malwareattake ist es ein Skript, das dezent im Hintergrund läuft. Vielleicht schreibt diese Schadsoftware einfach eine Menge Links in irgend ein Directory. Ich hatte kürzlich einen Fall, da hat ein Hacker 1.2 GB Links zu Sportartikeln und Modeartikeln auf einen meiner Server geschrieben. Das war vergleichsweise harmlos, ausser dass er eine Menge Speicher verbraten hat.

Schlimmer ist es, wenn sogenannte SPAM-Bots installiert werden, die Hunderttausende von Mails verschicken. Da ist der ganze Server urplötzlich auf internationalen Blacklists aufgeführt, was im Extremfall dazu führen kann, dass Sie plötzlich selber keine Mails mehr versenden können, weil andere Mailserver annehmen, Sie seien aufgrund des Eintrags ein Spammer.

Die Leute, die hacken sind keine Amateure oder kleine Jungs, die das aus Spass an der Freude machen. Es sind hochintelligente IT-Cracks, die untereinander auch bestens vernetzt sind. Man kann Listen von Servern mit Sicherheitslücken kaufen, man kann gehackte Passwörter zu Millionen erwerben. Auch die Sicherheitslücken werden auf speziellen Internet-Servern, oft im Darknet, gelistet und so weiden Tausende aus, was einer entdeckt hat.

Die Methoden werden von Monat zu Monat dreister, das Know-how der Hacker ist manchmal grösser als das der Sicherheitsfirmen, welche sie zu eliminieren versuchen. Deshalb sind auch Firmen mit einer stattlichen IT-Mannschaft nicht gefeit vor Attacken.

Da sind Sie und Ihr Web-Hoster/-dienstleister ganz kleine Fische, die man ziemlich leicht aufs Kreuz legt, bei aller Vorsorge.

Aber es gibt Abwehrstrategien.

Nun zur Verteidigung.

Massnahme eins.

Nachdem wir nun einige Erkenntnisse über das Gefahrenpotential gewonnen haben ergreifen wir Gegenmassnahmen:

Wichtig ist, dass eine periodische technische Überprüfung Ihrer WebSite sicherstellt, dass keine veralteten Module auf den Joomla-Installationen mehr vorhanden sind. In der Vergangenheit war das nicht so kritisch, es ist selten was passiert. Die Zeiten haben sich aber gründlich geändert. Es ist heute ein Muss, die technische Integrität der Installationen periodisch zu überprüfen.

Intensiv-Wartung

So nennt ABC Promotion ab sofort eine neue Dienstleistung. Sie erteilen uns einen Dauerauftrag, gültig bis auf Widerruf, Ihren Server resp. Ihre Web-Installation periodisch auf Aktualität zu überprüfen. Wir werden ungefähr zweimonatlich alle Extensionen auf Aktualität und Versionenstand der einzelnen Publizierer gegenchecken. Wir führen eine minutiöse Kontrolle darüber, welche Softwarekomponenten bei welchem Kunden eingesetzt werden. Das wird pro Kunde einen Aufwand von einer halben bis anderthalb Stunden mit sich bringen.

Softwarekomponenten von Drittanbietern sind in der Regel kostenpflichtig, wenn auch die Lizenzen bescheiden sind. Oft erhält man Updates während eines Jahres kostenlos, nach Ablauf der Frist muss man die Komponente neu erwerben, manchmal bekommt man einen Discount. Ist es notwendig, die Lizenz erneut zu entrichten, verrechnet ABC Promotion eine Pauschale von CHF 20 pro Modul. Wir können die bezahlte Lizenz ja in der Regel auf mehrere Kunden verteilen.

Diese Intensivwartung ist eine präventive Massnahme, die bereits sehr viel Angriffsmöglichkeiten eliminiert.

Und wenn dennoch gehackt wird?

Bei aller Prävention kann man nicht ausschliessen, dass dennoch ein Angriff eines Fieslings Erfolg hat. Weil die Hackerei heute weltweit eine wahrhafte Landplage im Internet darstellt, haben sich natürlich auch Sicherheitsfirmen mit hervorragend ausgebildeten IT-Spezialisten etabliert, die Hilfe anbieten. Einerseits bieten sie eine Möglichkeit an, WebServer auf Malware (Schadsoftware) zu überprüfen und andere Schwachstellen des Servers wie veraltete PHP Versionen zu entdecken.

Eine Joomla Installation umfasst etwa 7'000 Dateien, die in ca. 300 Ordnern strukturiert gespeichert sind. Bei dieser Zahl ist es praktisch unmöglich, mit menschlicher Arbeit Schadsoftware zu ermitteln und zu beseitigen.

Diese Sicherheitsfirmen bieten extreme Powersoftware an, welche die Server nicht nur Scannen sondern allfällig doch entdeckte Malware automatisch entfernen. Ebenfalls übernehmen sie die Aufgabe, einen Server, der wegen SPAM oder ähnlichem auf eine Blacklist geraten ist, dort wieder auszutragen. Ohne solch starke Abwehrsoftware, die zudem von Experten im Sicherheitsbereich unterstützt wird, ist das beinahe nicht zu schaffen.

Ich habe lange evaluiert, was wir gegen attackierte und infizierte Server unternehmen können, denn ich habe mittlerweilen reiche Erfahrung im Flicken von Servern. Es ist keine wirklich berauschende Arbeit, ich bin lieber kreativ tätig.

Eine kalifornische Unternehmung hat mich überzeugt und ich habe Tests mit einem infizierten Server unternommen. Das Ergebnis war hervorragend. Es wurden 18 Probleme entdeckt. Nachdem ich den Service für die in Frage stehende Domain installiert habe, war nach zwei Stunden der Spuk vorbei und der Server wieder sauber. Ich kann deshalb nur empfehlen, dass Sie mich beauftragen, diese Protektions-Software auch für Ihre Domain zu installieren.

A.B..C...
Promotion

Deshalb: Massnahme zwei.

SiteGuarding.com
Professional Web Security Services

Ich schliesse für Sie bei siteguarding.com ein Abonnement zur automatisierten WebServer Überwachung und automatischer Schadsoftware-Entfernung ab. Die Subskription wird für ein Jahr in Auftrag gegeben.

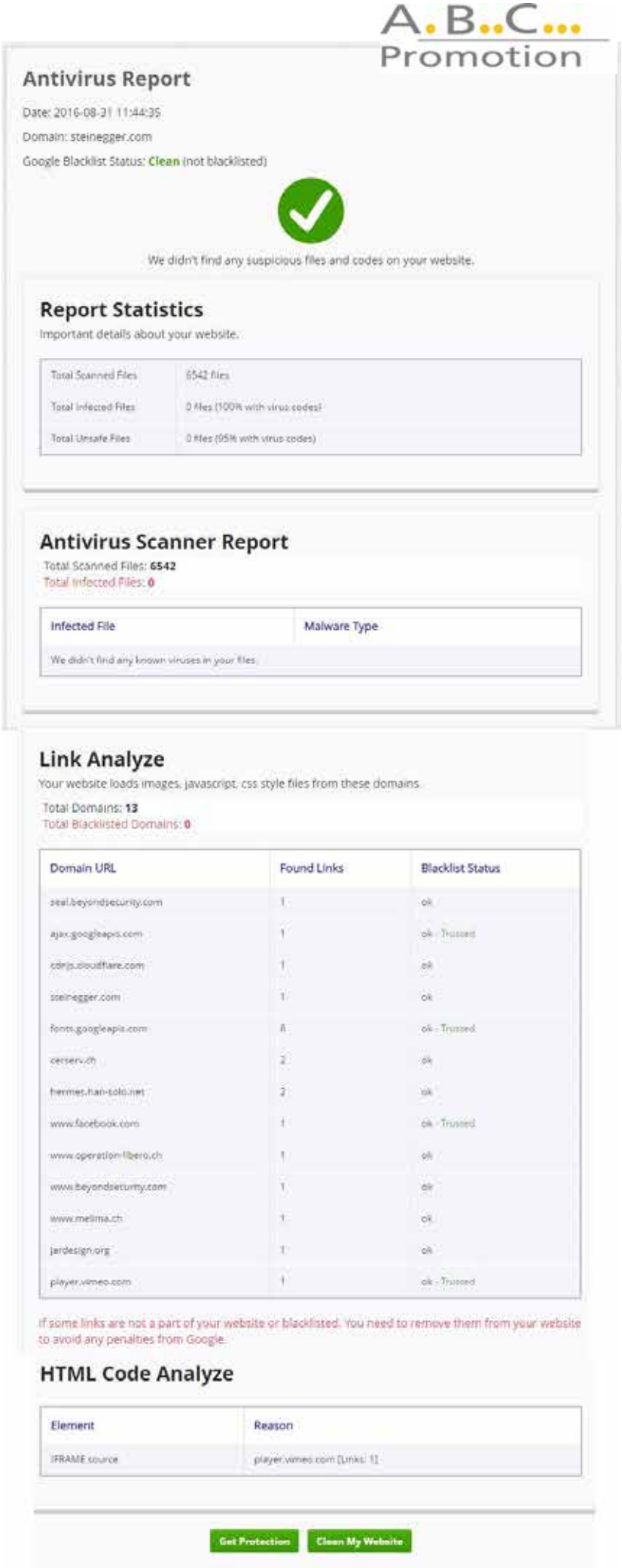
Nach der Anmeldung gibt es einige Installationsschritte und es wird eine Erstüberprüfung vorgenommen. Sollte der Server bereits infiziert sein, wird er automatisch gereinigt, so dass eine positive Rückmeldung per Mail eingeht, dass der Server nun frei von irgendwelcher dubioser Software ist. Das beruhigt ungemein. Denn es ist für niemanden wirklich erfreulich, wenn einer Ihrer Besucher vom Antiviren-Programm die Meldung bekommt, Ihre Site sei infiziert. Es dauert etwa 24 - 48 Stunden, bis die Sicherheitstechniker das ganze Prozedere installiert und durchlaufen haben. Ab dann wird Ihr Server aber täglich gescannt und ein Alarm wird unverzüglich abgesetzt, wenn etwas zur Beunruhigung Anlass geben sollte. Die Einrichtung des Services kostet einmalig CHF 150.

Die Subskription kostet Sie € 9.95/Monat

was etwa 2 Kaffee im Restaurant entspricht.

Dafür bekommen Sie (resp. ich als Ihr WebDienstleister):

- Gratis Installation durch Safeguarding
- Antivirus PRO Standard, Heuristischer Algorithmus zum entdecken unbekannter Viren
- Server basiertes Scannen und Datei-Modifikations-Erkennung
- Max. 25‘000 Dateien
- Viruserkennung (unlimitierte Seiten)
- Angrifferkennung
- Hack/Einspeisungs-Erkennung (SPAM, Porno etc.)
- Analyse von Änderungen auf der Website
- Dateien scannen alle 24 Stunden
- Tägliche Analyse$
- Entfernung von Malware bei bereits gehackten Sites
- Malware Reinigung monatlich
- Server Log Analyse
- Austragung auf Blacklists (Google, Norton, McAfee etc.)
- Voller WebSite Backup
- Warnungen und Benachrichtigungen per E-Mail
- Live Chat Support
- Support per E-Mail
- Kostenlose professionelle Beratung von Sicherheits-Experten und -ingenieuren
- Antwortzeit max. 24 Stunden



Antivirus Report

Date: 2016-08-31 11:44:35

Domain: steinegger.com

Google Blacklist Status: Clean (not blacklisted)

We didn't find any suspicious files and codes on your website.

Report Statistics

Important details about your website.

Total Scanned Files	6542 files
Total Infected Files	0 files (100% with virus codes)
Total Unsafe Files	0 files (05% with virus codes)

Antivirus Scanner Report

Total Scanned Files: 6542

Total Infected Files: 0

Infected File	Malware Type
We didn't find any known viruses in your files.	

Link Analyze

Your website loads images, javascript, css style files from these domains.

Total Domains: 13

Total Blacklisted Domains: 0

Domain URL	Found Links	Blacklist Status
seal.beyondsecurity.com	1	ok
ajax.googleapis.com	1	ok - Trusted
cdnjs.cloudflare.com	1	ok
steinegger.com	1	ok
fonts.googleapis.com	4	ok - Trusted
cerserv.ch	2	ok
hermes.han-solo.net	2	ok
www.facebook.com	1	ok - Trusted
www.operation-libero.ch	1	ok
www.beyondsecurity.com	1	ok
www.melima.ch	1	ok
jardesign.org	1	ok
player.vimeo.com	1	ok - Trusted

If some links are not a part of your website or blacklisted. You need to remove them from your website to avoid any penalties from Google.

HTML Code Analyze

Element	Reason
IFRAME source	player.vimeo.com [Links: 1]

Get Protection | Clean My Website

Beispiel eines Antivirus Rapports

Sie brauchen selber nichts zu unternehmen, das überwache ich für Sie. Wenn etwas auf dem Server nicht in Ordnung ist, bekomme ich von Safeguarding automatisch eine E-Mail und kann die notwendigen Aktionen einleiten.

Ich kann Ihnen versichern, so einen grünen Haken zu empfangen ist ein unwahrscheinlich gutes Gefühl.

Werden Sie jetzt aktiv!

Auf der nächsten Seite finden Sie ein Auftragsformular.

Einerseits für die Auftragserteilung zur Intensiv-Wartung.

Andererseits für die Einrichtung von Safeguarding.

Drucken Sie es aus, ergänzen Sie die Angaben und unterschreiben Sie das Form. Bitte einscannen und per Mail senden an:

abcpromotion5707@gmail.com

(Ich habe keinen Fax mehr.)

Es ist wie ein Wechsel bei der Krankenkasse von Allgemein auf Halbprivat.

Das leisten Sie sich ja auch.

Gönnen Sie das auch Ihrer WebSite.

A.B..C...
Promotion

Budgetübersicht

Eine WebSite ist, wird sie professionell aufgebaut und betreut, ein Budgetposten im Marketing. Dafür haben Sie auch eine Werbeplattform die, anders als Inserate, die sehr kurzlebig sind, 7 x 24 Stunden und 365 Tage im Jahr für Ihre Kunden, Interessenten oder Mitglieder da ist. Folgende Posten sind im Werbebudget zu berücksichtigen.

	einmalig	wiederkehrend
Erstmaliger Aufbau und Gestaltung	nach Aufwand abhängig vom Umfang CHF 150/h	
Hosting bei ABC Promotion		CHF 30/Domain
Unterhalt des Contents (Inhalt), wenn das nicht selber möchten		nach Aufwand abhängig vom Umfang CHF 150/h
„Intensiv-Wartung“		2-monatllich CHF 75 - 225
SiteGuarding	CHF 150 Einrichtung pro Domain	€ 9,95 Standard Paket

Eine veraltete WebSite kann nicht nur ein Sicherheitsrisiko darstellen, sie wird von Ihren Besuchern auch nicht als positiv wahrgenommen.

Auftrag

Ich/wir

Firma: _____

Zuständig: _____

Strasse: _____

PLZ / Ort: _____

E-Mail: _____

wünschen für die Domain: _____
(www.muster.ch)

☐ ab sofort und bis auf Widerruf die Dienstleistung „Intensiv-Wartung“ von ABC Promotion Chris Steinegger, Unterdorfstrasse 2, 5707 Seengen (Büro: Gotthardstrasse 55, 6410 Goldau

☐ ab sofort und bis auf Widerruf die Einrichtung von Siteguarding zum Preis von € 9.95 / Monat
(wird für 12 Monate in Rechnung gestellt. Ohne Kündigung erneuert sich die Subskription um ein weiteres Jahr. Einrichtungspauschale CHF 150.)

Datum: _____ Unterschrift: _____

Bitte dieses Formular nach dem Ausfüllen und Unterschreiben einscannen und mailen an:

abcpromotion5707@gmail.com

Oder per Post senden an: Chris Steinegger, Gotthardstrasse 55, 6410 Goldau.

Die Kommunikationsart „Fax“ wurde bei ABC Promotion wegen Nichtverwendung eingestellt.