Browser-Hijacker o.ä. auf Schulhomepage

Beitrag von „Talida“ vom 19. November 2015 20:08

Hatte schonmal jemand einen Browser-Hijacker o.ä. auf der eigenen Schulhomepage? Ist das überhaupt möglich?
Ich kenne das Problem, wenn ich eine befallene Website aufrufe und kann den Übeltäter größtenteils aufspüren und entfernen. Nun scheint es aber so zu sein, dass unsere HP der Verbreiter ist und ich habe keine Ahnung, wo ich suchen muss bzw. wie wir das Teil wieder loswerden.

Beitrag von „Stefan“ vom 19. November 2015 20:14

Welche Software nutzt ihr denn?

Beitrag von „Talida“ vom 19. November 2015 20:18

Die HP wurde mit Contao erstellt, ist kürzlich aber vom Webdesigner zu uns umgezogen, d.h. wir haben die Software noch gar nicht installiert.

Beitrag von „Stefan“ vom 19. November 2015 21:31

Habt ihr denn das coresystem auf den aktuellen Stand?
Mit Contao kenne ich mich leider nicht aus, aber wenn ihr die Homepage schon umgezogen habt, dann nutzt ihr das cms ja schon.

Beitrag von „Talida“ vom 19. November 2015 22:13

Die Website ist lediglich auf uns übertragen worden. Der Provider blieb. Für alles andere hatten wir noch keine Zeit, d.h. wir haben noch nicht daran gearbeitet. Habe nun den ganzen Abend gegoogelt und komme zu dem Schluss, dass der Fehler nicht bei uns liegen kann. Ich sollte also den bisherigen Webdesigner ansprechen, ob sein Contao befallen sein könnte, oder?
Sicherheitshalber setze ich mich morgen mit dem Provider in Verbindung.
Wir wollen die Homepage nämlich grundsätzlich umstricken und dann mit Wordpress arbeiten. Ich habe also keine Lust, mich jetzt 'nur' für diese Aktion in Contao einzuarbeiten ... Ich habe rudimentäre und veraltete HTML-Kenntnisse. Habe einen falschen Link im Quelltext gefunden, komme aber nicht dran, weil ich ja nur Zugriff auf die Daten habe, die ich per FTP-Zugang sehe. Gerne würde ich auch nur die Teile der Homepage vom Netz nehmen, die befallen sind. Aber auch da finde ich den entscheidenden Pfad o.ä. nicht. Werde mich am WE in Ruhe damit beschäftigen. Falls bis dahin jemand noch eine schnelle Lösung hat, wäre ich dankbar. Stoße an meine Grenzen und habe im Moment keine Zeit für aktuellen Input.
Zu befürchten ist allerdings, dass der Rechner in der Schule, mit dem ich heute versucht habe dem Problem auf die Spur zu kommen, den Hijacker bereits gefangen hat. Der Virenschutz, den der Schulträger installiert, ist lächerlich, aber auf mich hört ja keiner ...

Danke für deine Hilfe, Stefan!

Beitrag von „Stefan“ vom 19. November 2015 22:54

Was ich nicht verstehe ist, dass Contao doch ein CMS system ist.
Und als solches musst du (meist) doch nicht im HTML programmieren (es sei denn dies ist bei den Templates notwendig).

Hast du mal versucht in den Admin-Bereich zu gelangen.
Lt. Dokumentation über die Url +/contao

Gerade die CMS Systeme sollten immer möglichst aktuell gehalten werden, da Bugs häufig ein Einfalltor bieten können.

Beitrag von „toastrider“ vom 19. November 2015 22:55

Hallo, es könnte sein, dass irgendjemand Dir ein paar kleine php SKripte untergejubelt hat, die nun auf der Homepage schlaten und walten. Ein Suchen und Eliminieren ist hier sehr schwierig.

SPannenderweise finden manchen Virenscanner die Skripte, d.h. Homepage mal per ftp auf den lokalen Rechner kopieren und einen guten ANtivirus drüberlaufen lassen. Generell würde ich jedoch dazu raten die Seite komplett neu aufzusetzen, vor allem wenn sowieso ein Systemwechsel ansteht, da sonst die Hintertüre nach wie vor offen steht und alles wieder von vorne losgehen kann.

Gruß
toastrider

Beitrag von „Scooby“ vom 20. November 2015 00:16

Wir hatten das Problem auch schon einmal, bei dem ein Massenangriff eine Sicherheitslücke in einer veralteten Joomla-Komponente attackiert hat und so Schreibreche auf die Dateien erhalten hat. Der Virus hat in alle (ca. 500!) html und php-Dateien einen komplexen iframe-Text mit einem verschlüsselten Link eingefügt, sodass Besucher unserer Seite in einem unsichtbaren iframe auf eine osteuropäische Seite weitergeleitet wurden, von der aus dann versucht wurde, über bekannte Sicherheitslücken in gängigen Browsern Schadsoftware auf die Rechner zu installieren.

Meine Schritte waren:

1. Die Seite umgehend deaktivieren und durch eine simple nur-html-Seite mit nur wenigen Zeilen Text ersetzen (Kontaktdaten der Schule, Hinweis auf Wartungsarbeiten), diese Seite mehrmals täglich prüfen, ob sie auch schon verändert wurde.

2. Server-Logs untersuchen, ob du das Einfallstor findest (kann z.B. ein infizierter Rechner sein, über den das FTP-Passwort abgegriffen wurde).

3. Alle Passwörter von einem sicheren Rechner aus (Mac, Live-Linux, o.ä.) verändern: Frontend/Backend-Zugänge, FTP-Passwörter, Zugänge zu irgendwelchen Kundenportalen, etc.

4. Ein Backup aus der Zeit vor dem Virenbefall einspielen.

5. Alle Patches, Updates, etc. einspielen. Nicht benutzte Komponenten deaktivieren.

6. Die Seite wieder online stellen und mehrmals täglich prüfen.

Beitrag von „Talida“ vom 22. November 2015 19:39

Ich danke euch für den Input! Nun habe ich mich doch mit dem cms auseinandergesetzt und gelernt, dass ich sehr wohl Zugriff habe. Manches kann so einfach sein ... Auf Verdacht habe ich das Plugin (oder heißt das in diesem Fall Template?), das die Bildergalerie steuerte deaktiviert und siehe da, der böse Hijacker ist weg! Hoffe jetzt sehr, dass es das auch war. Das System hat länger kein Udate erfahren. Auch das kann ja gefährlich sein. Habe nun alle Passwörter geändert und notdürftig die Bilder eingestellt, die wirklich benötigt werden. Der Rest muss noch ein paar Wochen warten und wird dann weniger kompliziert gestaltet. Bei all den Zusatzaufgaben, die ich bereits habe, hat mir das jetzt noch gefehlt.