Browser-Hijacker o.ä. auf Schulhomepage

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 Schreibrechte 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.