Meine Webseite wurde gehackt? Was kann ich tun?

Sollten Sie feststellen, dass Ihre Webseite gehackt wurde, sollten Sie sofort Maßnahmen einleiten, um sich vor weiteren Schäden zu schützen.

Webseite sperren lassen
Haben Sie keinen genauen Überblick, über das Ausmaß des Angriffs, sollten Sie uns umgehend kontaktieren. Wir haben die Möglichkeit, Ihre Website vorübergehend zu sperren, um Sie und Ihre Kunden zu schützen. Diese Sperre können Sie jederzeit persönlich wieder aufheben.

Hinweis
Fällt uns ein Angriff Ihrer Webseite auf, sperren wir Ihre Webseite selbst, um Sie und Ihre Kunden zu schützen.

Schadensanalyse
Als Nächstes ist eine Schadensanalyse durch Sie/Ihren Technischen Ansprechpartner (Werbeagentur) erforderlich.

Dabei sind Folgende Fragen relevant:

- Wann fand der Angriff statt?
- Wie fand der Angriff statt?
- Was wurde auf dem System verändert?
- Gibt es Möglichkeiten zur Rückverfolgung des Täters?

Hat man diese Fragen klären können, sollte unbedingt als erstes die Sicherheitslücke geschlossen werden.

Schwachstelle schließen
Zusätzlich ist es unerlässlich, die Schwachstelle innerhalb Ihres Systems auszumachen und diese durch Konfigurationen oder Sicherheitspatches zu schließen. Ansonsten besteht das Risiko, dass der Angreifer Ihre Webseite wieder über den gleichen Weg kapern kann. Stellen Sie sich folgende Fragen bei der

Analyse.

- Um was für eine Art Angriff handelt es sich?
- Handelt es sich um eine bekannte Sicherheitslücke?
- Gibt es für diese Sicherheitslücke eventuell schon Sicherheitspatches?

Durch diese Informationen kann das weitere Vorgehen geplant werden. Ist der Angriff zum Beispiel erst kurze Zeit her und es wurden große Teile Ihrer Konfiguration o.Ä. geändert, ergibt das einspielen einer kompletten Datensicherung der letzten Tage unter Umständen Sinn. Kann man mit absoluter Sicherheit sagen, dass nur minimale Änderungen gemacht wurden, können die Veränderungen einzeln Rückgängig gemacht werden.

1. Zusätzlich ist es notwendig, die Schwachstelle innerhalb Ihres Systems auszumachen und diese durch Konfigurationen oder Sicherheitspatches zu schließen.

Hilfestellung können hier folgende Fragen bieten:

- Wann fand der Angriff statt?
- Wie fand der Angriff statt?
- Was wurde auf dem System verändert?[/ht_message]