Sicherheit im Internet
Schützen Sie sich vor Bußgeldern

Sicherheit im Internet gewinnt Jahr für Jahr stetig an Bedeutung. Schlagzeilen wie „Yahoo gehackt" und „Ransomware" („Erpressertrojaner") lassen aufhorchen und Themen wie „Datenschutz" und „Datensicherheit" gewinnen immer mehr an Bedeutung. Bei dem einen macht sich Unsicherheit breit und Ängste werden geschürt, andere übergehen diesen Sachverhalt rigoros und leben das Prinzip „Mich betrifft das nicht!". Wir sagen: „Beides ist falsch!"

Nehmen wir an, Sie sind Betreiber eines Onlineshops, Waren gehen bei Ihnen ein und aus und Sie bieten Ihren Kunden verschiedene Zahlungsmodalitäten an. Als Eigentümer eines Webshops sind Sie neben der Funktionalität für den Schutz Ihrer Kundendaten verantwortlich sowie für den einwandfreien Zahlungsvorgang. Sie haften für Ihre Internetpräsenz. Schließen Sie also alle eventuellen Sicherheitslücken. Mit der „simplen" Erstellung eines Onlineauftritts sind Ihre Aufgaben nicht erfüllt. Es ist ein Irrglaube, dass „online" gleichzusetzen ist mit einer einwandfreien automatisierten Funktion Ihres Webshops oder Ihrer Website. Die regelmäßige Wartung ist unerlässlich und wird oft im Aufwand unterschätzt.

Erst vor kurzem (Januar 2017) veröffentlichte der BSI eine Pressemitteilung, aus der hervorging, dass mindestens 1000 deutsche Webshops vom „Online-Skimming" betroffen sind. Dies bedeutet für die Kunden, dass deren Daten inklusive der Kreditkarteninformationen an „Hacker" im Hintergrund übermittelt werden. Eine Liste mit allen bekannten Domains wurde veröffentlicht und ins Internet gestellt. Der Imageschaden für diese Unternehmen dürfte beträchtlich sein.

Die Verantwortung für solche Schäden hat der Websitebetreiber zu übernehmen. Der Gesetzgeber hat ihn klar in die Pflicht genommen und entsprechende Vorgaben für Websites definiert:

„Nach § 13 Absatz 7 TMG sind Betreiber von Online-Shops verpflichtet, ihre Systeme nach dem

Stand der Technik gegen Angriffe zu schützen. Eine grundlegende und wirksame Maßnahme hierzu ist das **regelmäßige** und **rasche Einspielen** von verfügbaren Sicherheitsupdates." BSI Pressemitteilung

Zuwiderhandlungen führen nach § 16 TMG zu Bußgeldern von bis zu 50.000 Euro.

Heutzutage basieren die meisten Websites auf etablierten Shop-Systemen wie etwa Magento oder auf standardisierten Content-Management-Systemen (CMS). Diese Systeme wie zum Beispiel typo3, WordPress, Drupal oder auch Joomla! haben alle eins gemeinsam: Sie benötigen eine regelmäßige Wartung und das Einspielen von Sicherheitsupdates ist zwingend erforderlich.

Es ist ein Fehler anzunehmen, dass der Webhoster für die Sicherheit der Website verantwortlich ist. Häufig ist der Webhoster gerade einmal dazu verpflichtet, für die Sicherheit des bereitgestellten Betriebssystems zu sorgen. Alles Weitere obliegt jedoch der Verantwortung des Websitebetreibers!

Das im Hintergrund laufende System stellt das Fundament Ihres Webshops oder Ihrer Website dar. Dieses entwickelt sich stetig weiter, Ihre Website ohne entsprechende Pflege jedoch nicht.

Mangelnde Betreuung kann zu fehlerhaften Darstellungen Ihrer Inhalte führen, da sich die verwendeten Technologien im Internet stets weiterentwickeln. Dadurch können Texte abgeschnitten oder Bilder falsch platziert werden. Im schlimmsten Fall ist eine Navigation durch die Inhalte der Website nicht mehr möglich.

Auch das inzwischen als Standard vorhandene „Responsive Design", also die Ausspielung der Inhalte ausgerichtet an der Bildschirmgröße des jeweiligen Endgerätes (z.B. Tablet), kann durch mangelhafte Wartung zerstört werden. Mit der Zeit können blockierende Inhalte eine längere Ladezeit Ihrer Website zur Folge haben. Lange Ladezeiten sind eines der K.O.-Kriterien jeder Website über das mobile Endgerät. Stellen Sie sich selbst die Frage: Möchten Sie sich auf einer solchen Website informieren? Nehmen Sie diese Website überhaupt ernst? Um Ihren professionellen Auftritt zu wahren, ist es unumgänglich, Sicherheitslücken zu schließen. Eine absolute Sicherheit gibt es zwar leider nicht, aber man kann zumindest ein stabiles Fundament schaffen, um mit entsprechend kurzen Reaktionszeiten einem Hackerangriff entgegenzuwirken und um das Risiko eines solchen bereits im Vorfeld zu minimieren.

Vielleicht mag der ein oder andere Leser sich denken: „Auf meiner Website befinden sich keine sensiblen Daten, was soll mir da schon passieren?" Aber Ihr Webserver kann auch unbemerkt im Hintergrund im Rahmen eines Botnetzwerks viele Spam-E-Mails versenden. Mit der Zeit könnte hierdurch die IP-Adresse Ihres Servers sowie auch die verwendete Domain auf globalen Blacklists landen. Die Zustellung von sämtlichen E-Mails über Ihre Domain würde dadurch blockiert, was sich beispielsweise im Rahmen einer Newsletter-Versendung negativ auswirken würde. Dieser Imageschaden lässt sich anschließend

nur mit erheblichen Kosten wieder korrigieren.

Ein guter Rat ist daher: Führen Sie regelmäßige Backups durch. Diese Backups sollten jedoch nicht auf dem gleichen Server abgelegt werden. Darum sollten auch „Backup-Plugins" von diversen CMS-Anbietern kritisch betrachtet werden. Speichern Sie deshalb regelmäßig eine Kopie Ihres Webauftritts lokal ab. Dazu gehört neben den Dateien der Website auch ein Backup der Datenbank. Durch diese Maßnahmen könnten im schlimmsten Fall nach einem Angriff diese Daten jederzeit auf einem entsprechend konfigurierten Server wieder zeitnah eingespielt und der Schaden somit in Grenzen gehalten werden.

Die wichtigste Regel aber lautet: Führen Sie Updates durch, egal ob es sich um eine neue Version des Core-Systems, eines Plugins oder eines Themes handelt!

Sobald eine Aktualisierung zur Verfügung steht, sollte diese schnellstmöglich installiert werden. Meist werden alle bis dahin bekannten Sicherheitslücken geschlossen. Beachten Sie aber, dass das Einspielen von Sicherheitsupdates nicht immer reibungslos funktioniert und eine vorherige Backuperstellung daher zwingend notwendig ist.

Natürlich sind die hier bereits aufgeführten Punkte nur die Spitze des Eisbergs. Es gibt noch viele weitere Optimierungsmöglichkeiten, um Ihren Webauftritt sicherer zu gestalten und technisch qualitativ aufzuwerten.

Sollten Sie weder über das Fachwissen verfügen noch die benötigte Zeit zur Verfügung haben, um die Wartung Ihres Webauftritts sicherzustellen, wenden Sie sich mit diesem Thema am besten einfach an die Agentur Ihres Vertrauens.