Wie wird meine Website und deren Inhalt in 5 Schritten sicherer?

Die Website ist das Schaufenster jedes Unternehmens. Wenn gar das Geschäftsmodell komplett auf dem Internet basiert, wird sie zum wichtigsten Kapital. Doch im Internet lauern überall „Bad Guys", die einzudringen versuchen, Daten stehlen möchten oder gar die Seite blockieren. Heutzutage sind das allerdings weniger ‚böse Buben', sondern oft professionell organisierte Verbrecherbanden.

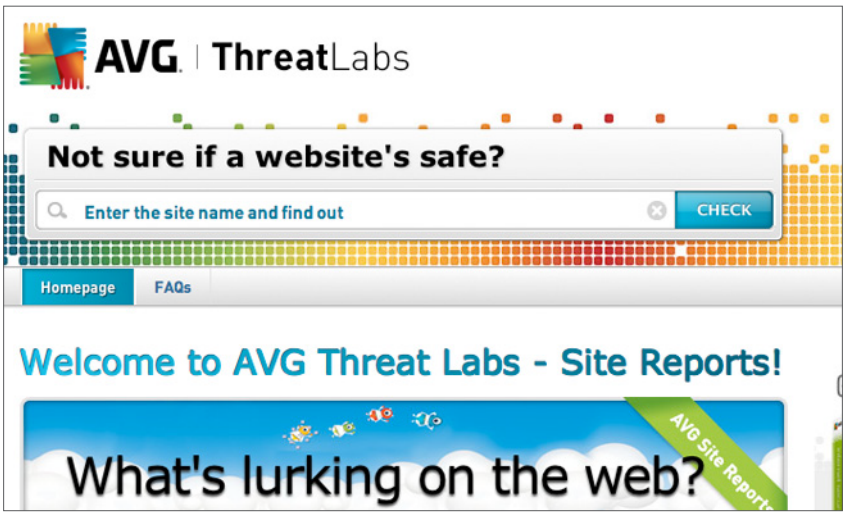
Wer ein Online-Geschäft betreibt, muss ständig auf der Hut sein. Sicherheitsrisiken lauern vor allem bei Transaktionen. Besonders bei Aufträgen mit Bezahlung per Kreditkarte und Warenanlieferung nach Übersee ist höchste Vorsicht angebracht. Bestehen Sie auf PayPal, Banküberweisung oder anderen sicheren Methoden.

Was kann passieren?

- Angreifer ‚kapern' Websites und missbrauchen sie für das Phishing. Das heißt: Ihre Seite wird zur Falle, um Besuchern Daten zu stehlen.
- Angreifer hacken Webseiten und nutzen gezielt Schwachstellen in der Website-Software aus. Damit verschaffen sie sich Zugang zu Kundeninformationen oder führen betrügerische Transaktionen durch.

Ist meine Website sicher?

Mit ‚AVG Threat Labs' können Sie das jetzt ganz einfach selbst prüfen. Unter http://www.avgthreatlabs.com/sitereports erhalten Sie einen Site-Report zum Echtzeit-Status Ihrer Webseite. Für weitere Fragen einfach hier klicken: http://www.avgthreatlabs.com/sitereports/content/faq



AVG

So machen Sie Ihre Firmenwebsite in 5 Schritten sicherer

1. Wer auch immer in Ihrem Unternehmen für den Code, die Installation und die kontinuierliche Pflege der Website verantwortlich ist, sollte die Liste der 25 gefährlichsten Programmierfehler kennen („CWE/SANS Top 25 Most Dangerous Software Errors List"). Achten Sie darauf, dass stets die aktuelle Version dieser Liste genutzt wird. Der Webseiten-Verantwortliche in Ihrer Firma sollte die beschriebenen Probleme verstehen und die in der Liste empfohlenen „Mitigations" umsetzen können. Weitere Informationen zu den Listen finden Sie hier: http://cwe.mitre.org/top25/

2. Sorgen Sie dafür, dass auf dem Web-Server stets die aktuellsten Software-Updates installiert sind und stets die aktuellste Internet Security Software läuft. Das gilt auch für Web-Applikationen von Drittanbietern und für Open Source-Web-Anwendungen. Spielen Sie neue Sicherheits-Patches sofort auf.

3. Setzen Sie diese Sicherheitsmaßnahmen auch auf Ihrem Unternehmensnetz und den dort angeschlossenen Rechnern um.

4. Beziehen Sie auch Passwörter für den Zugriff auf die Web-Hosting-Accounts und den Administratoren-Bereich der Web-Software in Ihre Sicherheitsmaßnahmen mit ein. Verwenden Sie ‚starke' Passwörter.

5. Stellen Sie sicher, dass Sie mit allen relevanten Standards vertraut sind. Dies gilt insbesondere für Compliance-Anforderungen und rechtliche Rahmenbedingungen, inklusive der Anforderungen in Bezug auf Datenschutz und Datensicherheit. Wenn Sie auf Ihrer Website EC- und Kreditkarten akzeptieren, sollten Sie sich an den PCI-Richtlinien orientieren (PCI = Payment Card Industry: Weitere Informationen dazu unter: https://de.pcisecuritystandards.org/minisite/en/

Ihr Fachhändler:

AVG