

Schutz Ihrer WordPress Seite

Warum ist das Thema Websicherheit auch für KMUs wichtig?

Websicherheit ist lange nicht mehr nur für Grosskonzerne wichtig. Die verbreitete Meinung, man sei nicht interessant für Hacker ist gefährlich. Hackerangriffe sind meist nicht gegen ein bestimmtes Ziel gerichtet, sondern werden mithilfe von automatisierten Methoden möglichst breit gestreut. Jede Webseite ist somit ein potentielles Ziel, sei dies die Webseite eines Konzerns, eines KMU oder eines Sportclubs. Die Folgen können gravierend sein:



Ihre Webseite kann zur Verbreitung von Schadsoftware missbraucht werden.

Gehackte Webseiten schrecken Benutzer ab. Die Folgen reichen von Reputationsschäden bis zu Umsatzverlusten.



In gewissen Fällen ist es möglich, dass der Webseitenbetreiber für Schäden im Zusammenhang mit der gehackten Webseite haftet.

Durch Schadsoftware können Geschäftsprozesse gestört und die Effizienz beeinträchtigt werden.



Haben Kriminelle Zugang zu Ihrer Webseite erlangt, können sensitive Informationen von Kunden aber auch vom Unternehmen entwendet werden.

Angreifer können Ihre Webseite lahmlegen und somit können Webseitenbetreiber Kundenverluste erleiden.



Kosten für die Bereinigung einer gehackten Webseite fallen deutlich höher aus als Ausgaben für präventiv getroffene Sicherheitsmassnahmen.



Präventive Sicherheitsmassnahmen



Rund 40% aller Webseiten verlassen sich auf WordPress um Webinhalte zu erstellen und zu verwalten. Cyberkriminellen ist dies nicht entgangen und so machen sie sich die fehlende IT-Affinität der Unternehmen zunutze und dringen auf vermeidbare Art und Weise in Ihre Webseite ein. Dank den Sicherheitspaketen der KastGroup (WordPress Security Pakete) können Schwachstellen frühzeitig detektiert, analysiert und fachgerecht behoben werden.

«Mit Malware infizierte Websites sind neben Spam-E-Mails der dominierende Verbreitungskanal für Viren, Trojaner und andere Bösartigkeiten. Folglich müssen Domainhalter als Eigentümer von Websites dazu beitragen, dass ihre Website sicher bleibt.»

- switch.ch

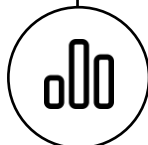


Wir wappnen Ihre Webseite gegen Angriffe!



1. Schritt – Kostenloses & unverbindliches Scanning

Wir bieten Ihnen eine kostenlose Schwachstellenüberprüfung Ihrer Wordpress Webseiten an, um nicht nur Sicherheitslücken, sondern auch Konfigurationsfehler zu detektieren.



2. Schritt – Kostenlose & unverbindliche Aufbereitung der Resultate

Die gefundenen Fehlkonfigurationen und Schwachstellen werden von uns zusammengefasst und übersichtlich dargestellt.



3. Schritt – Beheben von Sicherheitslücken

Anschliessend erstellen wir Ihnen gerne ein Angebot um Ihre Webseite von den gefundenen Sicherheitslücken zu befreien um Sie und Ihre Kunden gegen zukünftige Angriffe zu wappnen.



Unsere Angebote zur Prävention

Express WordPress Protection Paket CHF 399.- (Fixpreis)	Business WordPress Protection Paket CHF 699.- (Fixpreis)
<ul style="list-style-type: none">✓ Upgrade WordPress & Plugins	<ul style="list-style-type: none">✓ Upgrade WordPress & Plugins
<ul style="list-style-type: none">✓ Deaktivieren der XML-RPC Funktion	<ul style="list-style-type: none">✓ Deaktivieren der XML-RPC Funktion
<ul style="list-style-type: none">✓ Deaktivieren des Directory Indexing	<ul style="list-style-type: none">✓ Deaktivieren des Directory Indexing
<ul style="list-style-type: none">✓ Deaktivieren der direkten Datei-Bearbeitung	<ul style="list-style-type: none">✓ Deaktivieren der direkten Datei-Bearbeitung
<ul style="list-style-type: none">✓ Umbenennen des standard Administrator Benutzers	<ul style="list-style-type: none">✓ Umbenennen des standard Administrator Benutzers
<ul style="list-style-type: none">✓ Installieren von Sicherheitsplugins	<ul style="list-style-type: none">✓ Installieren von Sicherheitsplugins
	<ul style="list-style-type: none">✓ Deaktivieren der PHP-Ausführung im Upload Verzeichnis
	<ul style="list-style-type: none">✓ Passwortschutz für den Administrator Login Bereich
	<ul style="list-style-type: none">✓ Ändern des Datenbank Prefixes
	<ul style="list-style-type: none">✓ Aktivieren der Auto-Logout Funktion für inaktive Benutzer
<p><i>Geeignet für Homepages</i></p>	<p><i>Geeignet für Kundenportale und Online Shops</i></p>
<p>Protection wählen</p>	<p>Protection wählen</p>

Mehr Informationen unter <https://security.kastgroup.com/de/kmusecurity/>

