Internet Security: Massnahmen für sichere Websites

Die Kriminalität verlagert sich vermehrt in den digitalen Bereich (Cyberraum). In früheren Zeiten waren es Piraten, welche Schiffe überfielen, oder Wegelager und Verbrecher, welche Leute beraubten; heutzutage sind es vermehrt Hacker und Cyberkriminelle, welche im Internet ihr Unwesen treiben. Um enorme Schäden zu vermeiden, müssen heutzutage Unternehmen teilweise erhebliche Summen für die Cybersicherheit aufwenden.

Inhaltsverzeichnis

Einleitung

Dieser Beitrag zeigt einige wichtige Massnahmen auf, welche helfen, dass die eigene Website besser gegen Cyberangriffe geschützt ist.

Da mittlerweile WordPress weltweit einen Marktanteil von 43% aller Websites erreicht hat, Tendenz steigend, werden WordPress-Websites vermehrt zu Angriffszielen von Hackern und Internetkriminellen. Dieser Beitrag behandelt vor allem Schutzmassnahmen für WordPress-Websites, doch können diese Massnahmen auch bei anderen Content Management Systemen (CMS, z.B. Joomla, Contao, Typo 3 und Drupal) angewendet werden.

Mit Hilfe von CMS- aber auch Baukasten-Systemen, wie z.B. Jimdo, Wix, usw., ist es heutzutage möglich, dass auch Laien ohne grossen Programmieraufwand eine eigene Homepage veröffentlichen können. Dies stellt aber oft auch ein erhebliches Sicherheitsrisiko dar, wenn man sich nur um den Inhalt der Website kümmert und dabei sicherheitstechnische Massnahmen ausser Acht lässt. Hacker nutzen diese Schwachpunkte gnadenlos aus.

Zudem erlegen die Datenschutzgesetze (DSGVO, DSG) dem Website-Betreiber eine Sorgfaltspflicht auf. Besonders im Umgang mit sensiblen Personendaten gibt es strenge Regeln, deren Nichteinhaltung von Gesetzes wegen gebüsst werden können.

Website Sicherheits-Tests

Es macht Sinn, eine bestehende Website regelmässig auf Schwachstellen und Malware zu überprüfen.

Ein einfache Methode ist, wenn man dazu einen Online-Scanner wie z.B. Sucuri SiteCheck verwendet.
Es gibt aber auch Security-Plugins (wie z.B. Sucuri Security oder All-In-One Security), welche ständig und direkt auf der Website nach Schwachstellen sowie Malware suchen und diese auch entfernen können.

Technische Vorkehrungen

Wahl eines sicheren Webhosters

Es lohnt sich, nicht den billigsten Webhoster auszuwählen, denn dieseein solcher investiert nicht immer in die sichersten Server. Renommierte Webhoster legen viel Wert auf Serversicherheit und scannen die gehosteten Websites auf Malware. Bei Bedarf können diese auch durch sog. Patches eventuell infizierte Codeteile isolieren und so die Sicherheitslücken schliessen, wie dies mein bevorzugter Webhoster Cyon anbietet.
Mehr Informationen siehe:
https://www.cyon.ch/support/a/automatisches-schliessen-von-sicherheitslucken.

Verwendung von renommierten Themes und Plugins

Bei der Auswahl und Verwendung von WordPress-Themes und -Plugins ist aus

Sicherheitsgründen ebenfalls Vorsicht geboten. Es gibt etwa 60’000 kostenlose WordPress-Plugins, doch sollte bei der Auswahl einige Punkte wie Kompatibilität mit der aktuellen WordPress-Version, Aktualität, Anzahl Installationen, Bewertungen, usw. beachtet werden.
Mehr dazu in folgendem Blog-Beitrag:
https://www.smart-webdesign.ch/webdesign-mit-wordpress-cms/#plugins

https und SSL-Zertifikat

Der Datenaustausch sensibler Daten, z.B. beim Übermitteln der Kontaktformulardaten, sollte verschlüsselt erfolgen, damit Hacker die übertragenen Daten nicht ohne weiteres mitlesen können. Dies erfolgt durch die Einrichtung eines SSL-Zertifikats (Secure-Socket-Layer-Zertifikat), welches die Webhoster teilweise kostenlos anbieten. Eine verschlüsselte Verbindung erkennt man am Eintrag von «http**s**://» in der Adresszeile des Browsers und am Schloss-Symbol in der Browserzeile.

Unverschlüsselte Websites werden heutzutage von den meisten Internet Browser als ‚Nicht sicher‘ (Google Chrome, Edge) oder durch ein rot durchgestrichenes Schlosssymbol (Firefox) in der Browserzeile angezeigt.

Login- und Zugangsdaten

Um eine WordPress-Website bearbeiten zu können, muss man sich zuerst in das sog. WordPress-Backend einloggen. Damit überhaupt das Login-Formular erscheint, muss die Adresse (url) der Login-Seite bekannt sein. Im Login-Formular können dann der gültige Benutzername und das korrekte Passwort eingegeben werden, damit ein Login ins WordPress-Backend erfolgreich ist.

Hacker und Internetkriminelle versuchen ständig, sich durch Hacken der Zugangsdaten sich Zugriff zum Backend einer Website zu verschaffen. Deshalb ist es wichtig, dass sichere Benutzernamen und Passwörter gewählt werden.

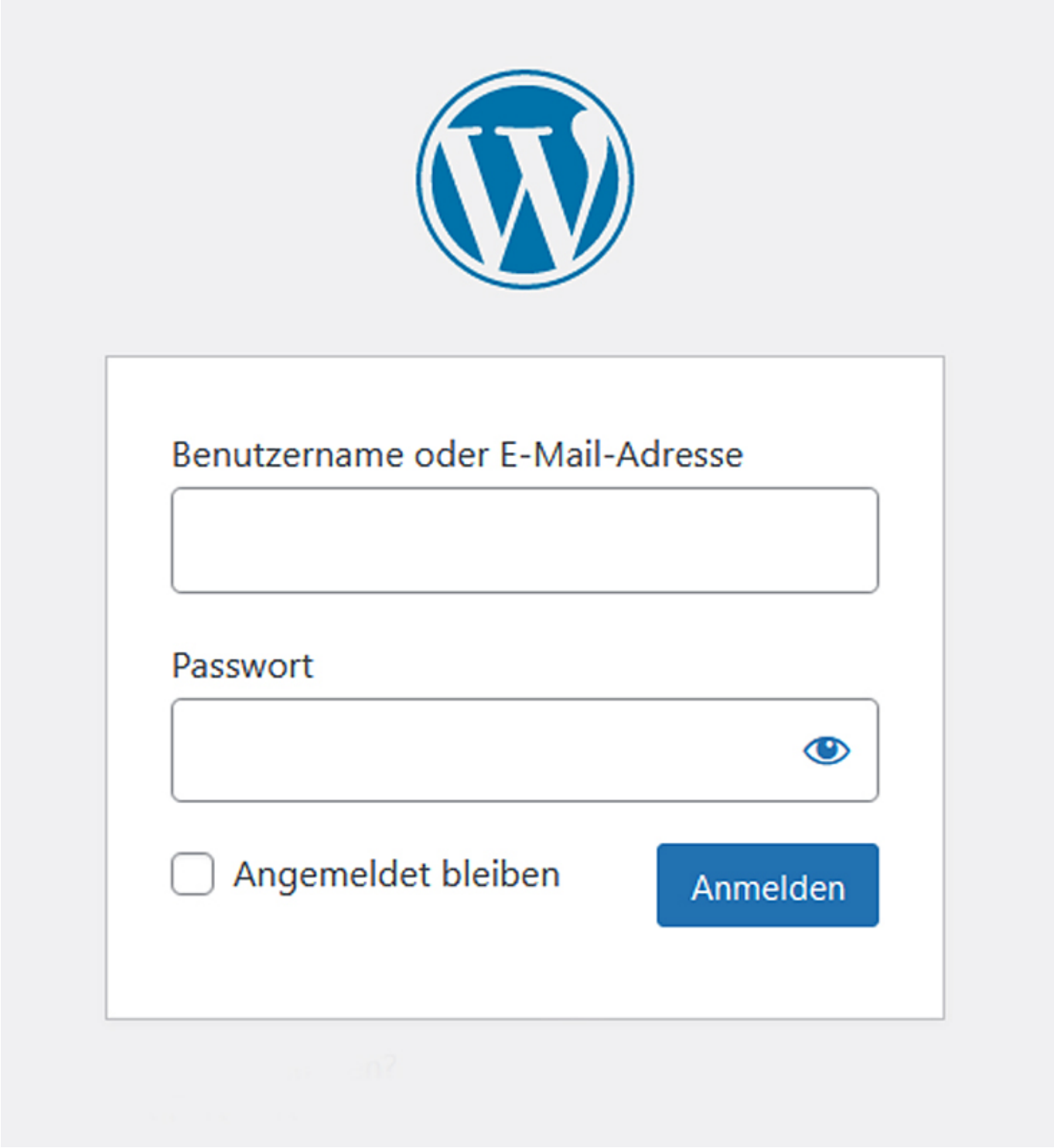


Abbildung WordPress Login

Adresse der Login-Seite (Anmelde-URL)

Bei WordPress ist die Adresse der Login-Seite standardmässig auf **/wp-admin** hinter der Website-Adresse eingestellt, z.B. www.deinesite.ch/**wp-admin**. Dies macht es Hackern einfach, auf die Login-Seite zu gelangen und sich auf das Hacken der Zugangsdaten zu konzentrieren.

Es ist daher Sinnvoll, wenn man die Login-Seite umbenennt, indem die Anmelde-URL geändert wird. So wird der Zugang zu wp-login.php und dem Verzeichnis wp-admin verhindert. Dies kann z.B. mit dem Plugin WPS Hide Login bewerkstelligt

werden.

Benutzername

Die Login-Daten bestehen immer aus dem Benutzernamen (user) und einem Passwort.
Die Wahl eines, nicht einfach zu erratenden, Benutzernamens ist aus Sicherheitsgründen sehr wichtig. Viele WordPress-Anwender übernehmen den vorgeschlagenen Benutzernamen ‚Admin'. Da dies sehr häufig vorkommt, haben es Hacker einfacher, sich Zugang zum WordPress-Backend zu verschaffen. Sie müssen sich nur noch auf das Herausfinden des Passwortes konzentrieren.

Wählen Sie daher immer einen nicht einfach zu erratenen Benutzernamen.

Passwörter

Die Wahl eines sicheren Passwortes ist von entscheidender Bedeutung. Ein solches Passwort sollte eine bestimmte Länge (Minimum 12 Zeichen) und eine Mischung aus Zahlen, Sonderzeichen und Buchstaben in Gross- und Kleinschreibung aufweisen, welche zufällig gewählt sind.

Am besten verwendet man einen Passwortgenerator, welcher die Zeichen und Zahlen zufällig zusammenstellt, z.B. mit folgendem Online-Tool:
https://www.lastpass.com/de/features/password-generator#generatorTool

Auf keinen Fall sollten einfach zu knackende Passwörter verwendet werden, denn die Hacker verfügen über leistungsstarke Password-Cracking-Tools, welche durch Ausprobieren und durch spezielle Algorithmen diese innert Sekunden erraten können.

Wie sicher ein Passwort ist, kann mit folgenden Online-Tools ermittelt werden:
https://www.passwortcheck.ch oder https://checkdeinpasswort.de

So sollte man es nicht machen!
Nachstehend die am häufigsten im Jahr 2023 in Deutschland verwendeten Passwörter:
123456789, 12345678, hallo, 1234567890, 1234567, password, password1, target123, iloveyou, ….

Verhinderung von Brute-Force Attacken

Durch sog. Brute-Force-Angriffe (brute force bedeutet ‚rohe Gewalt'), versuchen Internetkriminelle und Hacker die Zugangsdaten zum Admin-Bereich der Website zu hacken. Brute-Force-Attacken beinhalten Angriffsmethoden, welche mit Hilfe automatisierter Tools und leistungsstarker Hardware innert kurzer Zeit verschiedene Benutzer-Passwort-Varianten ausprobieren und so unsichere Zugangsdaten (siehe oben) innert kurzer Zeit erraten können. Brute-Force-Angriffe gehören seit Jahren zu den Standardmethoden von Cyberkriminellen und Hackern, um sich Zugang zum Admin-Bereich von Websites zu verschaffen.

Da bei sichern Passwörtern solche Angriffe Stunden, Tage oder Monate dauern können, besteht die Gefahr, dass der Webserver abstürzen kann oder dass die Website stark ausgebremst wird.

Es gibt verschiedene Methoden, um Brute-Force-Attacken zu verhindern. Nachstehend eine Auflistung einiger davon:

- Begrenzung der Anmeldeversuche, z.B. mit dem Plugin Limit Login Attempts Reloaded
- Umbenennung der Login-Seite (siehe oben bei ‚Adresse der Login-Seite (Anmelde-URL)‘
- Anmeldung mittels 2-Faktor-Authentifizierung zum Admin-Bereich
- Verwendung von sicheren Passwörtern (siehe oben)
- Änderung der Passwörter in regelmässigen Abständen

Verhinderung von DDoS-Attacken

Mit DoS (*denial of service*) ist eine Nichtverfügbarkeit eines Internetdienstes gemeint. DDoS ist die Abkürzung von *distributed denial of service*, zu Deutsch ‚verteilte Verweigerung eines Dienstes‘. Durch eine sog. DDoS-Attacke werden eine Vielzahl von gezielten Anfragen von einer grossen Anzahl von Rechnern auf eine Website ausgeführt, mit dem Ziel, den Webserver zum Absturz zu bringen oder zu verlangsamen. DDoS-Angriffe dienen nicht wie Brute-Frorce-Attacken dazu, eine Website zu hacken, sondern die entsprechende Website lahmzulegen oder zu verlangsamen.

Schutzmassnahmen vor DDoS-Attacken:

- Verwendung eines Web Application Firewall (WAF). Ein WAF schützt Websites vor einer Vielzahl von Angriffen im Internet.
- Deaktivierung von xmlrpc.php mittels eines Plugins (z.B. Disable XML-RPC-API) oder durch folgenden manuellen Eintrag in der .htaccess-Datei:

```
<Files xmlrpc.php>
    Order Deny,Allow
    Deny from all
</Files>
```

Aktualität der Website

Einer der wichtigsten Sicherheitsmassnahmen besteht darin, dass eine Website stets auf dem neusten Stand gehalten wird, indem neue verfügbare Updates des WordPress-Core sowie der verwendeten Themes und Plugins zeitnah eingespielt werden.

Internetkriminelle und Hacker sind ständig auf der Suche nach Sicherheitslücken in den WordPress-Applikationen. Glücklicherweise findet dies jeweils die Internet-Community rasch heraus und reagiert schnell mit entsprechenden Sicherheits-Updates. Diese sollten umgehend installiert werden, um die Sicherheitslücken zu schliessen.

Mehr zu diesem Thema siehe mein Blogbeitrag WordPress-Updates

Wartung der Website:
Überlassen Sie diese Aufgaben Ihrem Webmaster. Er weiss worauf es ankommt. Für die Websites meiner Kunden biete ich einen umfassenden WordPress-Wartungsservice an.

Updates des WordPress-Core

Es gibt zweierlei WordPress Update-Arten:

- **Minor-Updates**: dies sind Wartungs- und Sicherheitsupdates, welche **umgehend** installiert werden sollten. Minor-Updates erkennt man an den dreistelligen WordPress-Versionsnummern, z.B. 6.4.2.
- **Major-Updates**: diese Updates enthalten Funktionsänderungen und allgemeine Verbesserungen des WordPress Core; diese erkennt man an den zweistelligen WordPress-Versionsnummern, z.B. 6.2.

Seit der WordPress-Version 5.6 lässt sich das Installieren von WordPress-Updates automatisieren.
Ich empfehle aber nur die Automatisierung der Minor-Updates.
Vor dem Installieren eines Major-Updates, ist es meiner Meinung nach besser, wenn diese zuerst in einer sog. Staging-Umgebung (geklonte Website, welche nicht online verfügbar ist) durchgeführt wird und danach die Funktion der Website getestet wird.

Updates von Themes und Plugins

Auch Themes und Plugins sollten regelmässig aktualisiert werden, da auch hier immer wieder Sicherheitslücken geschlossen werden müssen, welche von Hackern entdeckt wurden.

Seit der WordPress-Version 5.5 ist es möglich, dass Updates von Themes und Plugins automatisch installiert werden können. Da aber bei diesen Updates meistens nebst der Fehlerkorrektur auch der Funktionsumfang der Themes und Plugins verändert wird, empfehle ich wie bei den WordPress Major-Updates, die Aktualisierung nicht zu automatisieren, sondern die Updates zuerst in einer Staging-Umgebung zu testen.

Regelmässige Backups

Trotz guten Sicherheitsmassnahmen könnte es dennoch vorkommen, dass eine Website gehackt wird und sog. Malware eingeschleust wird. Manchmal ist es dann notwendig, eine verseuchte Website komplett zu löschen. Aus diesem Grund ist es sehr wichtig, dass man regelmässig Backups von der Website erstellt, um eine gehackte Website wieder herstellen zu können.

Es kann aber auch immer wieder Mal passieren, dass beim Einspielen von Updates (siehe oben) eine Website abstürzen kann, dies falls die Updates unbeabsichtigte Codefehler enthalten. Auch hier könnte man dann problemlos auf vorhandene Backups zurückgreifen, um die Website wieder herzustellen.

In der Regel ist bei renommierten Webhostern ein Backup-Service inbegriffen, bei dem man die Website in einem eigens bestimmten Rhythmus automatisch sichern kann. Diese Backups werden auf dem eigenen Server gespeichert. Es macht daher Sinn, zusätzliche Backups extern (auf der Festplatte eines Computers oder in einer Cloud) abzulegen. Für diesen Zweck gibt es Backup-Plugins.

Bei Websites, welche wenig geändert werden, verwende ich das Plugin Duplicator. Dieses Plugin eignet sich auch sehr gut, wenn man eine Website auf einen anderen Webserver migrieren möchte.

Bei Internetauftritten, welche täglich geändert werden, eignet sich das Plugin Updraft Plus.

Phishing

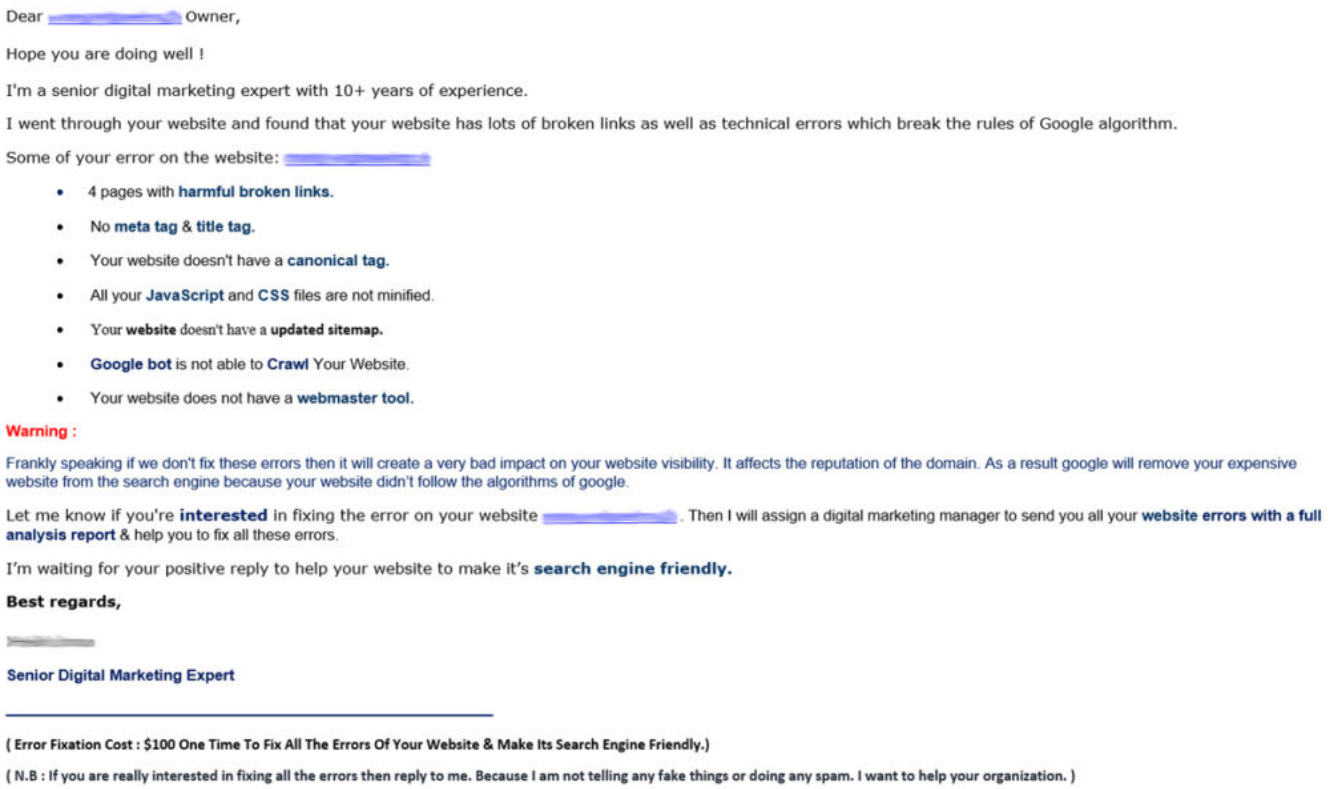
Einer der grössten Sicherheitslücken ist aber immer noch der Internet-Benutzer selbst, indem er auf Phishing hineinfällt und so Internetkriminellen und Hackern geheime Daten (z.B. Login- oder Kreditkartendaten) preisgibt.

Definition des Begriffs ‚Phishing' gemäss Wikipedia:
„Unter dem Begriff Phishing (Neologismus von „fishing", engl. für ‚Angeln') versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es, z. B. an persönliche Daten eines Internet-Benutzers zu gelangen, etwa ihn zur Ausführung einer schädlichen Aktion wie das Einloggen in einen gefälschten / nachgebauten Webauftritt zu bewegen, um die Zugangsdaten wie das Passwort und den Benutzernamen und gegebenenfalls auch einen 2. Faktor für die 2-Faktor-Identifizierung zu erschleichen."

In letzter Zeit häufen sich gefälschte E-Mails von Internetbetrügern und Hackern, welche sich als vermeintliche Webhosting-Dienste ausgeben. Es wird immer mit der Angst geschürt, dass z.B. ein Account gesperrt wurde, dass die Domain abläuft usw. Hier einige nützliche Informationen von meinem Webhoster Cyon über Pishing.

Lassen Sie sich nicht unter Druck setzen und erkunden Sie sich allenfalls beim Webhoster über zurzeit kursierende Phishing-Mails.

In den letzten Jahren haben einige meiner Kunden, aber auch ich selber, immer wieder die gleiche untenstehende E-Mail von unterschiedlichen Adressaten erhalten (zum Vergrössern anklicken). In dieser E-Mail wird angekündigt, dass aufgrund von mehreren angeblichen SEO-Fehlern Google die Website aus den Suchresultaten löschen werde, falls diese nicht korrigiert würden. Auch hier wird bewirkt, dass die angeschriebenen Website-Betreiber verunsichert werden und zu einer schädlichen Aktion gezwungen werden. Jeder der jeweils aufgelisteten SEO-Fehler ist nur erfunden und entspricht nicht den Tatsachen.



Dear [redacted] Owner,

Hope you are doing well !

I'm a senior digital marketing expert with 10+ years of experience.

I went through your website and found that your website has lots of broken links as well as technical errors which break the rules of Google algorithm.

Some of your error on the website: [redacted]

- 4 pages with **harmful broken links.**
- No **meta tag** & **title tag.**
- Your website doesn't have a **canonical tag.**
- All your **JavaScript** and **CSS** files are not minified.
- Your **website** doesn't have a **updated sitemap.**
- **Google bot** is not able to **Crawl** Your Website.
- Your website does not have a **webmaster tool.**

Warning :

Frankly speaking if we don't fix these errors then it will create a very bad impact on your website visibility. It affects the reputation of the domain. As a result google will remove your expensive website from the search engine because your website didn't follow the algorithms of google.

Let me know if you're **interested** in fixing the error on your website [redacted]. Then I will assign a digital marketing manager to send you all your **website errors with a full analysis report** & help you to fix all these errors.

I'm waiting for your positive reply to help your website to make it's **search engine friendly.**

Best regards,

[redacted]

Senior Digital Marketing Expert

(Error Fixation Cost : $100 One Time To Fix All The Errors Of Your Website & Make Its Search Engine Friendly.)

(N.B : If you are really interested in fixing all the errors then reply to me. Because I am not telling any fake things or doing any spam. I want to help your organization.)

Fazit

In der heutigen Zeit ist es dank Web-Baukasten- und Content Management Systemen (CMS) sehr einfach, dass auch Laien ansehnliche Websites erzeugen können. Doch ohne tieferes Wissen über die oben beschriebenen Sicherheitsmassnahmen, kann sehr schnell eine solche Website von Internetkriminellen und Hackern gehackt werden. Vielleicht sagen Sie sich, meine Website ist ja gar nicht so wichtig. Doch für Hacker spielt es keine Rolle, ob eine renommierte oder unbekannte Website gehackt wird, denn jede eroberte Website kann im Hacker-Netzwerk für kriminelle Zwecke eingesetzt werden.
Ziehen Sie deshalb einen Fachmann zu, der sich mit dieser Materie auskennt. Wenn die oben genannten Massnahmen umgesetzt werden, haben Sie wenig zu befürchten, dass Ihre Website gehackt werden sollte.

In eigener Sache:
Bei jeder meiner entwickelten Websites werden die oben erwähnten Massnahmen bezüglich Internet Security umgesetzt. Mehr Informationen zur Entwicklung von Homepages siehe: Produktübersicht Entwicklung Websites / Kosten.

Beitrag von Jean-Pierre Wicht
Webdesigner / Webentwickler