toscom
WEBSERVER EXPERTS

We speak Linux. WEBSITE-CHECK

Mehr Performance für Ihre Website. Durch toscom.

Sicherheit

Oft sagt der zweite Blick mehr als der erste über die Sicherheit einer Website aus - wir schauen mit einem technischen Auge auf ihr Web-Angebot und untersuchen es bei unserem toscom Website-Check auf gravierende Schwächen:

- Betriebssysteme oder Services, die auf Ihrem Server laufen, können angreifbar sein, ohne dass Sie es wissen. Auch veraltete Versionen Ihrer Applikationen können Probleme verursachen
- Veraltete SSL-Zertifikate und falsche Zertifikatsketten sind ein besonderes Sicherheitsrisiko
- Auffällige Dateien können auf Sicherheitsprobleme hinweisen - Stichworte dazu sind Cross-site-scripting (xss), Versionierungsinformationen, History-Informationen
- Konfigurationsprobleme (zB. cookie without secure flag) bleiben oft unbemerkt
- Falsche Mailkonfigurationen können eine Ursache für Probleme sein.
- Ist die Mailingliste durch Spamming auf einer Blacklist gelandet, behindert das die tägliche Arbeit enorm
- Lange Ladezeiten schrecken potenzielle Kunden ab

Inklusivleistungen:

Website-Check

€ 390,-
pauschal

- Analyse einer Website
- Besprechung der Ergebnisse im Detail **optional** gerne nach Aufwand
- gilt für eine Website
- Durchlaufzeit nach Bestellung: zirka eine Woche
- Arbeitszeit € 160,- pro Stunde für Besprechungen oder erweiterte Tests

Weitere Informationen: 0720/11 66 06 | office@toscom.at | www.toscom.at

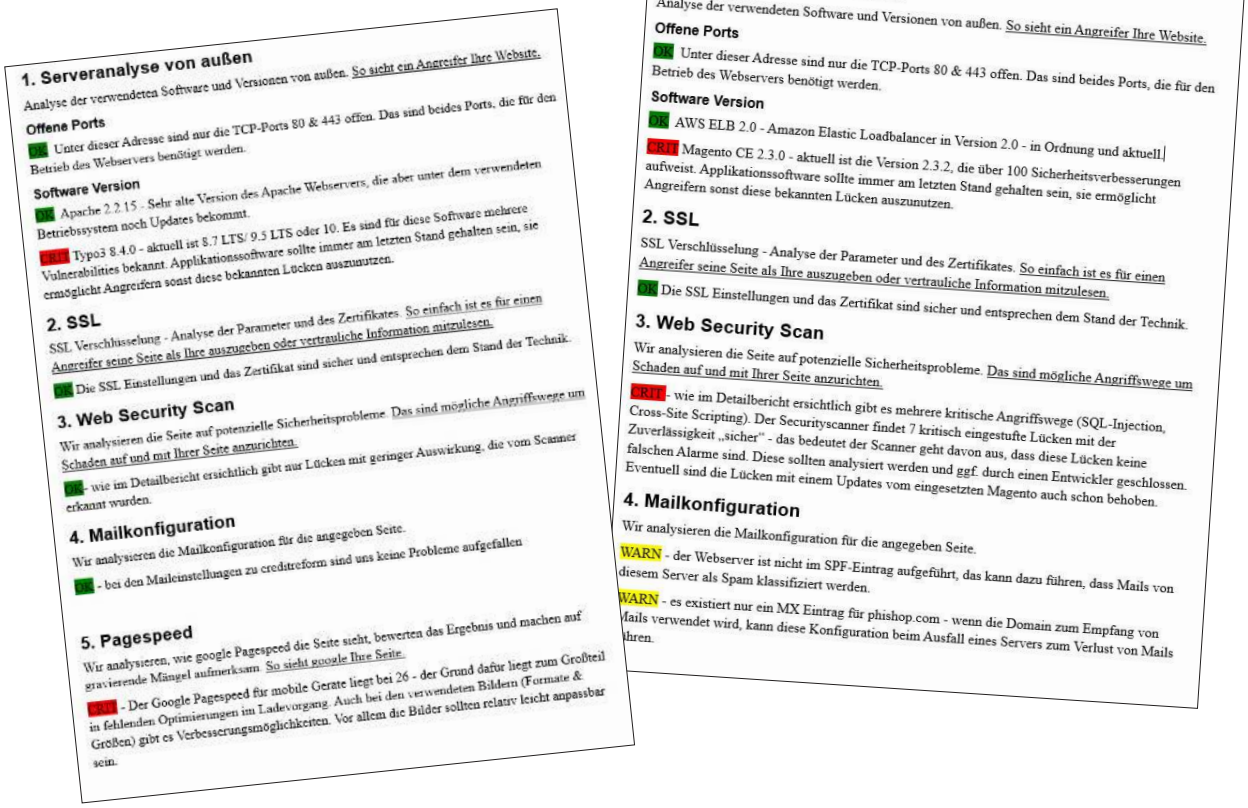
toscom
WEBSERVER EXPERTS

Die detaillierte **Analyse**

Unsere detaillierte Analyse umfasst folgende Schritte:

1. Wir untersuchen den **SERVER VON AUSSEN** - welche Version läuft, welche Services wären angreifbar, wie ist das Betriebssystem zu bewerten, sind die Applikationen veraltet?
2. Wir analysieren die **SSL-VERSCHLÜSSELUNG** - ist die Konfiguration korrekt und aktuell, stimmt die Zertifikatskette?
3. Beim **WEB-SECURITY-SCAN** suchen wir auf der Seite nach möglichen Sicherheitproblemen - wir beschäftigen uns mit Cross-site-scripting (xss), auffälligen Dateien, SQL-Injections, Konfigurationsproblemen, Cross-domain-referer-Leakages etc.
4. Auch die **MAILKONFIGURATION** nehmen wir unter die Lupe - stimmen die DNS-Konfiguration, die MX-Einträge, sind SPF, DKIM und Co. konfiguriert oder ist der Server auf einer Blacklist?
5. Wir analysieren auch, wie Google **PAGESPEED** die Seite sieht und bewerten das Ergebnis

Es handelt sich dabei nicht um einen individualisierten Penetration Test, sondern um einen Überblick darüber, wie ein Angreifer die Seite sieht.
Wir arbeiten gewissenhaft und mit aktuellen Tools, aber dennoch kann es sein, dass nicht alle Probleme entdeckt werden.



1. Serveranalyse von außen

Analyse der verwendeten Software und Versionen von außen. So sieht ein Angreifer Ihre Website.

Offene Ports

OK Unter dieser Adresse sind nur die TCP-Ports 80 & 443 offen. Das sind beides Ports, die für den Betrieb des Webservers benötigt werden.

Software Version

OK AWS ELB 2.0 - Amazon Elastic Loadbalancer in Version 2.0 - in Ordnung und aktuell

CRIT Magento CE 2.3.0 - aktuell ist die Version 2.3.2, die über 100 Sicherheitsverbesserungen aufweist. Applikationssoftware sollte immer am letzten Stand gehalten sein, sie ermöglicht Angreifern sonst diese bekannten Lücken auszunutzen.

2. SSL

SSL Verschlüsselung - Analyse der Parameter und des Zertifikates. So einfach ist es für einen Angreifer seine Seite als Ihre auszugeben oder vertrauliche Information mitzulesen.

OK Die SSL Einstellungen und das Zertifikat sind sicher und entsprechen dem Stand der Technik.

3. Web Security Scan

Wir analysieren die Seite auf potenzielle Sicherheitsprobleme. Das sind mögliche Angriffswege um Schaden auf und mit Ihrer Seite anzurichten.

CRIT - wie im Detailbericht ersichtlich gibt es mehrere kritische Angriffswege (SQL-Injection, Cross-Site Scripting). Der Securityscanner findet 7 kritisch eingestufte Lücken mit der Zuverlässigkeit „sicher" - das bedeutet der Scanner geht davon aus, dass diese Lücken keine falschen Alarme sind. Diese sollten analysiert werden und ggf. durch einen Entwickler geschlossen. Eventuell sind die Lücken mit einem Updates vom eingesetzten Magento auch schon behoben.

4. Mailkonfiguration

Wir analysieren die Mailkonfiguration für die angegeben Seite.

WARN - der Webserver ist nicht im SPF-Eintrag aufgeführt, das kann dazu führen, dass Mails von diesem Server als Spam klassifiziert werden.

WARN - es existiert nur ein MX Eintrag für phishop.com - wenn die Domain zum Empfang von Mails verwendet wird, kann diese Konfiguration beim Ausfall eines Servers zum Verlust von Mails führen.

Herausgeber: toscom, Philipp Kobel, Breiteneckergasse 32, 1230 Wien, 0720/11 66 06, office@toscom.at, Wirtschaftskammer Wien UBIT, UID: ATU57385145, Landesgericht Wien