MM Mustermann
GmbH und Co.KG

Datenschutz und Datensicherheit

Webseiten-Check

http://www.mustermann.de/

Projektdaten

Projektthema	Datenschutz und Datensicherheit **Webseiten-Check**
Auftraggeber	Mustermann GmbH und Co.KG
Ansprechpartner	Herr Michael Mustermann mm@mustermann.de
Durchführung	Dr. Frank H. Thiele GSG GmbH Darmstädter Str. 53 64354 Reinheim Tel/Fax: 06162 1051/1055 www.gsg-edv.de
Ansprechpartner	Dr. Frank H. Thiele f.thiele@gsg-edv.de
Verfasser	Dr. Frank H. Thiele (FT) Kanya Pawlewicz-Rupp (KP)
Abgabe	31.03.2021

Inhaltsverzeichnis

1. Vorwort

1.1 Einführung

Der vorliegende Webseiten-Check der GSG Global Service Group GmbH zeigt auf, ob Ihre Unternehmens-Webseite die relevanten Vorgaben im Datenschutz und in der Datensicherheit rechtskonform und angemessen umsetzt und gibt Hinweise und Tipps zur Behebung von Mängeln und Sicherheitslücken.

Notwendigkeiten

Neben konkreten Pflichten (z.B. Impressum, Datenschutzhinweise etc.) werden auch sinnvolle und erprobte Instrumente (SSL-Verschlüsselung, AGBs, Captcha etc.) überprüft und in die kurzen, übersichtlichen Maßnahmenempfehlungen einbezogen. So wird gewährleistet, dass der geforderte „Stand der Technik" (u.a. Europäische Datenschutzgrundverordnung, IT-Sicherheitsgesetz) in Bezug auf Datenschutz und Datensicherheit ausreichend berücksichtigt wird bzw. durch klare Lösungsvorschläge praxisnah umgesetzt werden kann.

Eine eigene Unternehmenswebseite gehört heutzutage zu den elementaren Informations- und Kommunikationsmitteln. Kaum ein Unternehmen kommt ohne sie aus. Der Internetauftritt dient dazu, das Unternehmen, seine Produkte, Werte, die Professionalität und Seriosität zu repräsentieren und schnelle, einfache Kommunikationswege anzubieten. Entsprechend muss sie korrekt funktionieren und den aktuellen technischen und rechtlichen Anforderungen genügen, um nicht im schlimmsten Fall einen negativen Eindruck vom Unternehmen zu generieren oder kostenpflichtige Abmahnungen durch Dritte (z.B. Wettbewerber, „Abmahnanwälte") auszulösen.

Machenschaften

Webseiten sind ebenfalls beliebte Einfallstore für Cyber-Kriminalität (z.B. mittels SQL-Injection und Cross-Site-Scripting) oder dienen nach einer Kompromittierung unwissentlich als „Spamschleuder" oder Weiterleitung auf dubiose Schad- oder Betrugsseiten. Neben dem Imageschaden sind Umsatzeinbußen realistisch, insbesondere, wenn Kontaktformular und Online-Shop nicht mehr erreichbar sind.

Maßnahmenempfehlungen

Eine regelmäßige Überprüfung der Webseite durch unvoreingenommene und neutrale Experten ist daher insbesondere hinsichtlich der Dynamik und des schnellen Wandels bei Rechtsprechung und technischer Entwicklung äußerst sinnvoll und unter Abwägung der möglichen Konsequenzen bei Datenpannen oder Fehlern eine kluge Präventionsmaßnahme.

Die aus den gewonnenen Erkenntnissen abgeleiteten Maßnahmenempfehlungen stellen konkrete Umsetzungsschritte zur Verbesserung der Sicherheit und der Rechtskonformität Ihrer Webseite dar und sollten möglichst umgesetzt werden. Sofern Sie bei der Umsetzung externe Unterstützung in Anspruch nehmen möchten, stehen Ihnen unsere Experten effizient und zielgerichtet zur Verfügung. Zögern Sie daher nicht, uns dahingehend zu kontaktieren, wir helfen Ihnen gern weiter.

1.2 Haftungsausschluss

Dieses Dokument wurde durch zertifizierte Datenschutz- und Informationssicherheits-beauftragte, welche die gesetzlich geforderte Sachkunde, praktische Eignung und umfassende Erfahrung besitzen, erstellt und geprüft. Es enthält Bewertungen und Empfehlungen, die auf dem Verständnis der Autoren zur angemessenen und korrekten Einhaltung der Rechtsvorschriften und technischer Sicherheitsanforderungen basieren. Die Bewertungen und Empfehlungen werden mit höchster Sorgfalt und nach bestem Wissen vorgenommen.

Rechtsberatung

Eine umfassende Rechtsberatung i.S. des Rechtsdienstleistungsgesetzes kann und will dieser Bericht aber weder leisten noch ersetzen. Es muss zudem berücksichtigt werden, dass verschiedene Rechtsauffassungen und Interpretationsspielräume existieren und fortlaufend materielles Recht durch Rechtsprechung entsteht oder geändert wird. Daher und auch anderweitig wird jegliche Haftung für mögliche Schäden oder Ansprüche ausgeschlossen.

1.3 Verfahrensweise

Im Folgenden wird die Webseite der Mustermann GmbH insbesondere aus dem Blickwinkel einer **Datenschutzaufsichtsbehörde** oder eines spezialisierten **Abmahnanwaltes** betrachtet. Ebenfalls fließen Aspekte der technischen Webseite-Sicherheit ein. Eingesetzt werden verschiedene spezialisierte Tools, die im Vorfeld einer gründlichen Prüfung auf ihre Eignung und Handhabbarkeit hin unterzogen wurden.

Gesamtbild

Ergänzt und verifiziert werden die so erzielten Ergebnisse durch händische Überprüfungen unserer zertifizierten Datenschutz- und Datensicherheitsbeauftragten. Dieses Zusammenspiel von maschinellen und manuellen Methoden und die Einordnung und Zusammenführung der Ergebnisse durch unsere Experten ermöglicht die Erstellung eines differenzierten Gesamtbildes. Neben der Bewertung werden konkrete Maßnahmenempfehlungen zur Behebung von Mängeln und zur Verbesserung des unternehmensindividuellen Datenschutz- und Datensicherheitsniveaus ausgesprochen.

2. Einleitung

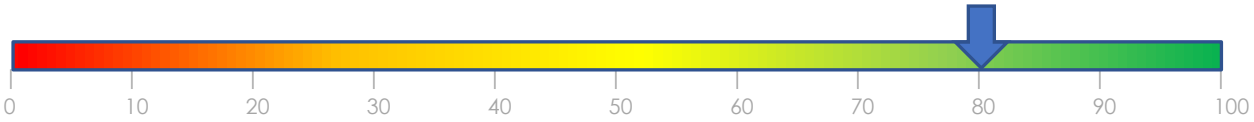
Die zu überprüfende Webseite wurde uns am xx.xx.xxxx durch XXXXX genannt. Sie lautet: www.xxxx.com

Abbildung 1: Hauptseite der Fa. Musterman GmbH

3. Zusammenfassung

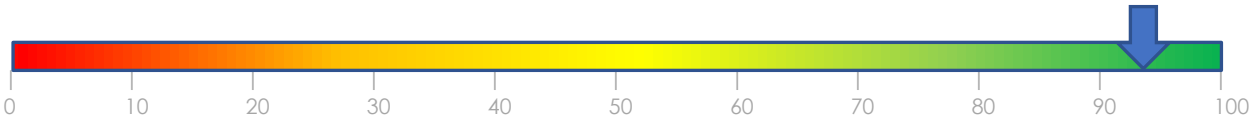
Nachfolgend erhalten Sie einen zusammengefassten Überblick über die in den einzelnen Abschnitten dargestellten Ergebnisse:

Verschlüsselung ((https, SSL, Zertifikat) -> 4.1



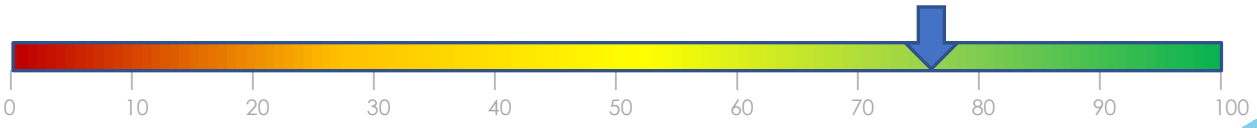
Nach dem gesetzlich vorgeschriebenen „Stand der Technik“ (u.a. DSGVO) müssen Webseiten über ein SSL-Zertifikat verfügen.

Impressum (Link, Inhalt) -> 4.2



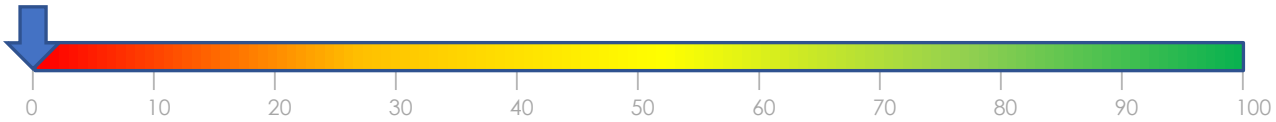
Jede Webseite muss ein Impressum mit bestimmten Pflicht-Inhalten aufweisen. Dieses Impressum muss von jeder Stelle innerhalb der Webseite aufrufbar sein.

Datenschutzerklärung (Link, Inhalt) -> 4.3



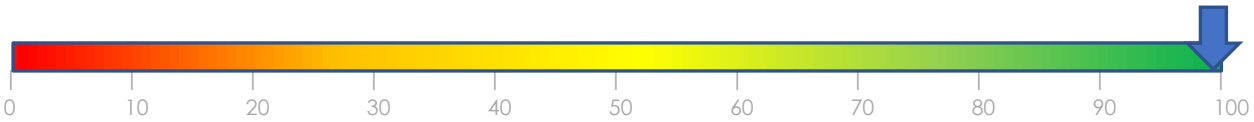
Jede Webseite muss eine Datenschutzerklärung mit bestimmten Pflicht- Inhalten aufweisen. Diese Erklärung muss von jeder Stelle innerhalb der Webseite aufrufbar sein.

AGB -> 4.4



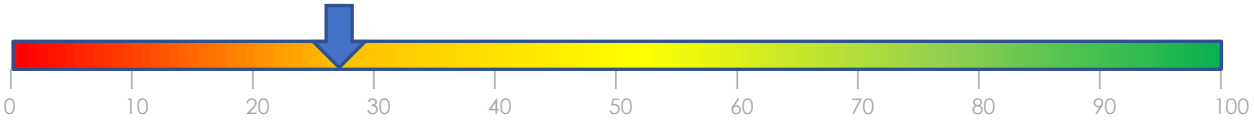
AGB selbst sind nicht gesetzlich vorgeschrieben, zur Regelung von gesetzlichen Anforderungen bei vielen ähnlichen Verträgen mit Privatkunden aber oft sinnvoll.

Widerrufsbelehrung -> 4.5



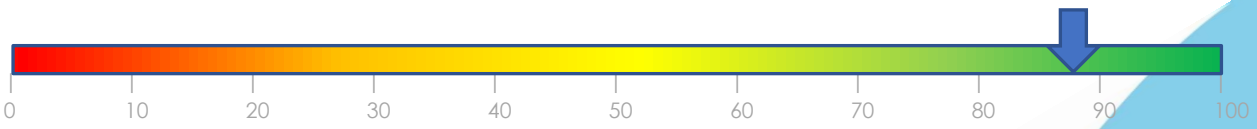
Bei Fernabsatzverträgen mit Privatkunden (z.B. per Online-Shop, Telefon, Katalog) muss eine Widerrufsbelehrung auf der Webseite enthalten sein.

Cookies (Consent-Manager, Parameter) -> 4.6



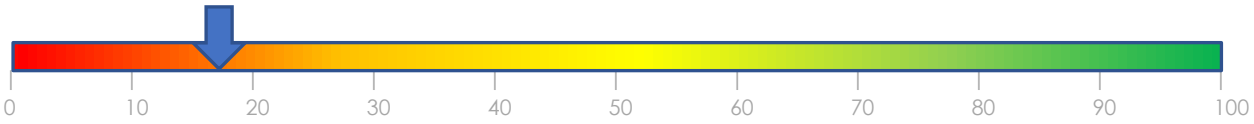
Für Cookies, die technisch nicht notwendig sind (z.B. Statistik-Cookies, Marketing-Cookies) ist im Vorfeld der Datenübertragung eine Einwilligung einzuholen.

Formulare (Captcha, Datenschutzrelevanz) -> 4.7



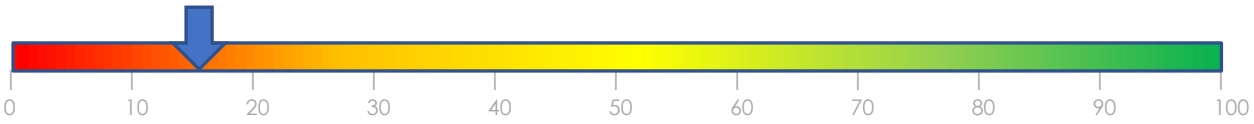
Captchas können einen Beitrag zur Sicherheit der Webseite leisten.

Zusätzliche Inhalte (ext. Einbindungen, soziale Kanäle, iFrames) -> 4.8



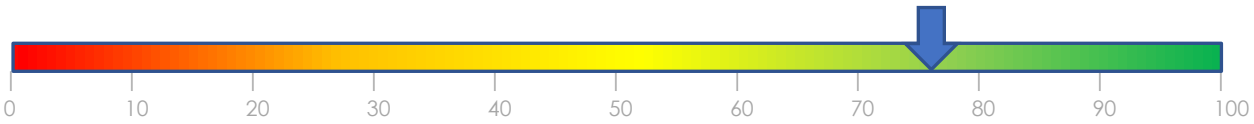
Bei der Einbindung zusätzlicher, fremder Inhalte auf der eigenen Webseite sind technische und/ oder rechtliche Aspekte zu beachten.

Security (Malware, Sicherheitslücken, DNS) -> 4.9



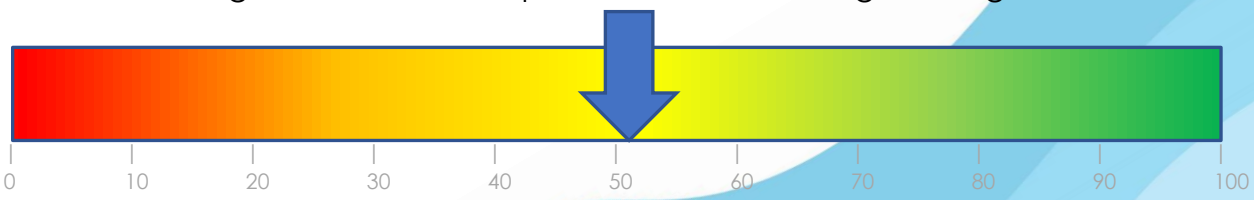
Der Missbrauch unverdächtiger Unternehmenswebseiten ist für Hacker ein einfacher und beliebter Weg, um Schadprogramme weiterzuverbreiten.

SEO Verhalten -> 4.10



Sicherheitsmaßnahmen auf der Webseite können sich positiv auf das Ranking in Suchmaschinen auswirken.

In die Gesamtbetrachtung fallen alle Einzelergebnisse ungewichtet entsprechend der Darstellung durch die grünen Felder auf eine Gesamtpunktzahl von 51%. Hierin sind die Felder mit „ohne Prüfung“ unberücksichtigt geblieben. Ebenso unberücksichtigt wurde der Einzelpunkt 4.10, der sein eigenes Ergebnis darstellt.



4. Überprüfung

4.1 Verschlüsselung (https, SSL, Zertifikat)

Die Homepage – also die Startseite des Webauftritts der Mustermann GmbH – ist unter http://www.xxx.de aufrufbar. Bereits der Beginn der URL mit „http“ zeigt an, dass kein SSL-Zertifikat verwendet wird. An dieser Stelle eine kurze Erläuterung zum notwendigen Einsatz einer SSL-Verschlüsselung:

> *Die Abkürzung SSL steht für Secure Socket Layer. Hierbei handelt es sich um ein Verschlüsselungsprotokoll, damit Daten, wie z.B. Kreditkarten- und Personendaten, sowie Passwörter abgesichert bzw. sicher zwischen Webserver und Webbrowser übertragen werden. SSL verhindert somit, dass ein Dritter sensiblen Daten unerlaubt und ohne weiteres mitlesen bzw. manipulieren und missbrauchen kann.*
>
> *Zur Verschlüsselung von übertragenden Daten wird heute das HTTPS-Protokoll eingesetzt. HTTPS dient der abhörsicheren Datenübertragung und der Authentifizierung. Mittels eines SSL-Zertifikats, welches immer einer bestimmten Domain zugeordnet wird, authentifiziert sich der Webserver gegenüber dem Webbrowser. Der Webbrowser wiederrum kann die Gültigkeit und die Signatur des Zertifikats überprüfen und stellt damit fest, ob es sich um eine echte und vertrauenswürdige Webseite handelt.*

Der Anteil der SSL-verschlüsselten Webseiten steigt erfreulicherweise weltweit stark an. In Deutschland sind inzwischen über 70% der Webauftritte durch ein SSL-Zertifikat geschützt, so dass diese Verschlüsselung bereits zum „aktuellen Stand der Technik“ gezählt wird.

Frage	Antwort
Kann die Webseite verschlüsselt aufgerufen werden (https)?	nein
Wird das Zertifikat von allen gängigen Webbrowsern als vertrauenswürdig eingestuft und somit alle richtigen Zwischenzertifikate installiert?	nein
Ist der Hostname (s.o.) im Zertifikat korrekt aufgeführt?	nein
Kann die Webseite ausschließlich verschlüsselt aufgerufen werden (HSTS) und werden auch Aufrufe über http:// entsprechend umgeleitet?	nein