SIWECOS
Auf der sicheren Seite

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

SIWECOS KMU Webseitencheck 2019

Für den SIWECOS KMU Webseiten-Check 2019 wurden 1.406 Webseiten kleiner und mittelständischer Unternehmen aus Deutschland mit den Scannern des SIWECOS Projektes auf mögliche Schwachstellen hin untersucht.

Projektpartner

RUHR
UNIVERSITÄT
BOCHUM
RUB

eco
Verband der
Internetwirtschaft e. V.

Unterstützt durch

cms garden

HACKMANIT

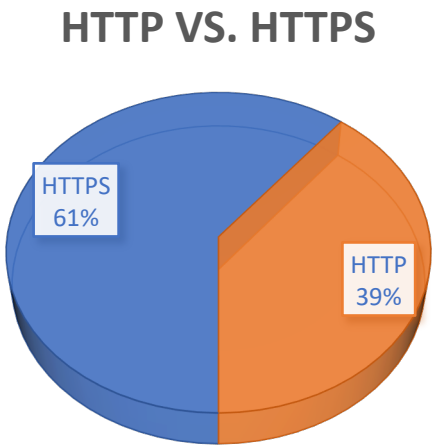
Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

HTTPS Verwendung immer noch nicht bei allen Webseiten eingeführt.

Erstaunlicherweise sind in der untersuchten Schnittmenge nur 61% der Webseiten über HTTPS zu erreichen, die veraltete HTTP Verbindung wird noch von 39% aller Webseiten verwendet, obwohl Browser die Besucher solcher Webseiten eindeutig vor den Gefahren einer unsicheren Verbindung warnen.

HTTPS hat sich als Standard für Webseiten etabliert. Das Protokoll wird zur Herstellung von Vertraulichkeit und Integrität in der Kommunikation zwischen Webserver und Webbrowser (Client) im World Wide Web verwendet.

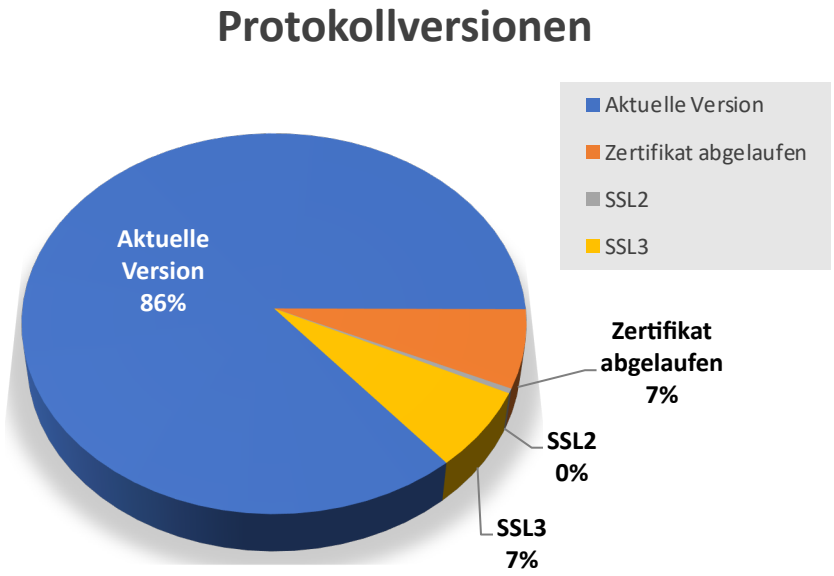
Aktuelle Internetbrowser wie der Google Chrome kennzeichnen inzwischen Internetseiten ohne HTTPS als „nicht sicher“.



Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

7% der überprüften Webseiten wiesen abgelaufene Zertifikate auf.

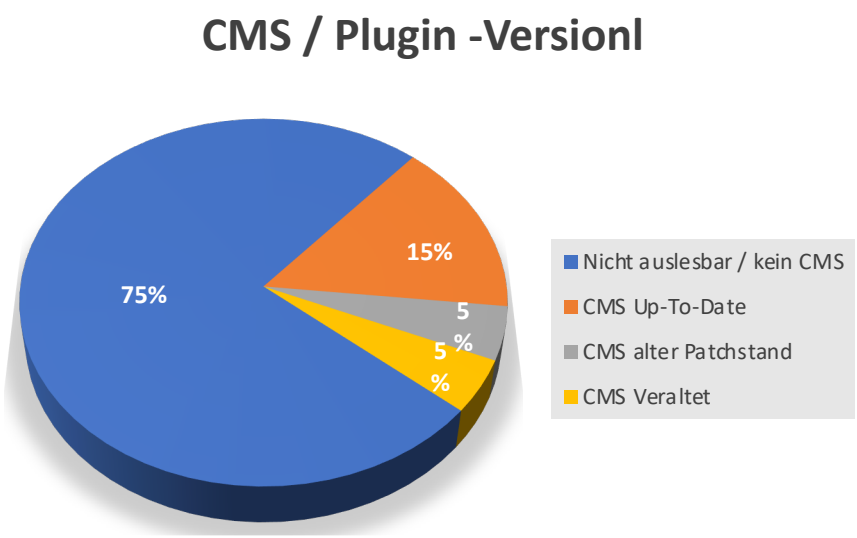
Runde 14% der geprüften Webseiten, die ein Server-Zertifikat einsetzen, tun dies fehlerhaft. Der überwiegende Teil der Zertifikate ist bei der ausstellenden Zertifizierungsstelle abgelaufen oder wurde fehlerhaft implementiert. In beiden Fällen führt dies dazu, dass ein Besucher beim Aufruf der Webseite gewarnt wird.



Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Bei rund 25 % der überprüften Webseiten lässt sich die Version des Content Management Systems oder der verwendeten Plugins auslesen.

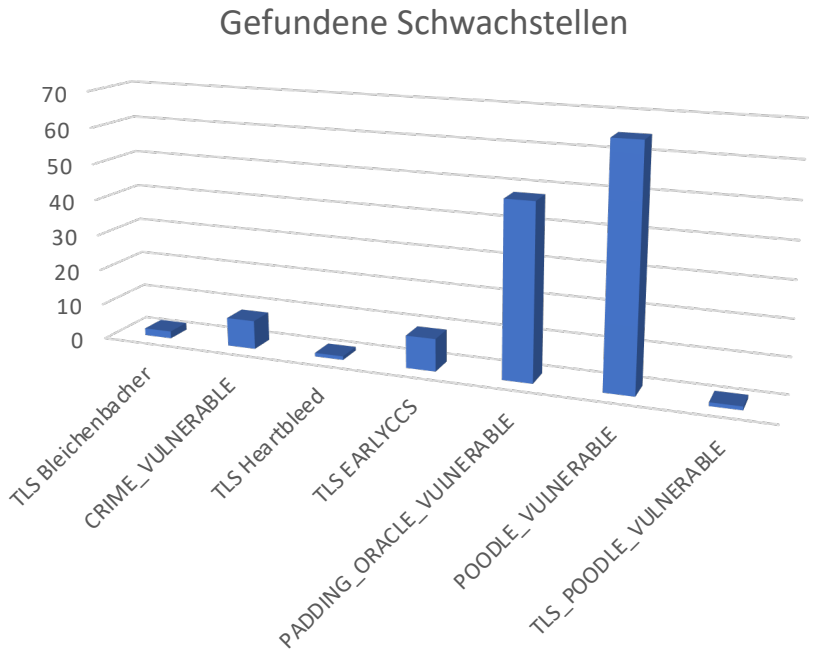
Ein Drittel dieser Seiten arbeitet mit einer Version mit bekannten Schwachstellen.
Fast jede vierte überprüfte KMU-Webseite enthält im Quelltext Informationen über das verwendete Content Management System oder eines darin installierten Plugins, zusammen mit der Versionsangabe.
In der Hälfte aller Fälle sind dies Versionen, die eine bekannte Schwachstelle haben. Dies ermöglicht es möglicherweise Cyberkriminellen, ohne viel Aufwand eine Webseite zu hacken.



Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

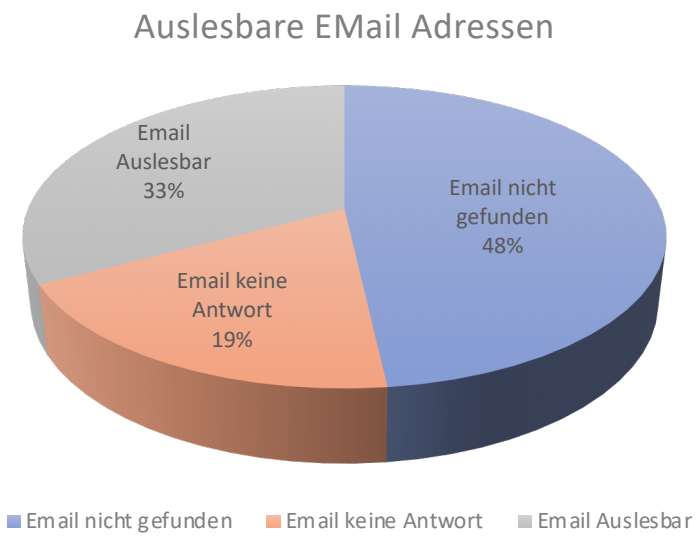
Bei fast 8 % der untersuchten Webseiten lässt sich die Poodle Schwachstelle nachweisen.

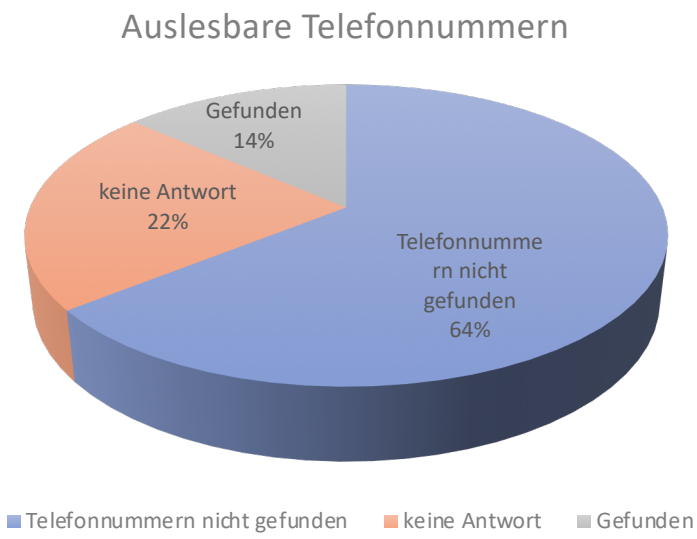
Sie erhöht die Gefahr, dass durch sogenannte Man-In-The-Middle Angriffe über verschlüsselte Verbindungen private Daten von Clients und Servern ausgelesen werden können.
Weitere 5,6 Prozent der geprüften KMU Webseiten weisen eine Padding-Oracle Schwachstelle auf.



Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Die Angabe von Kontaktdaten wie einer Telefonnummer oder einer Kontakt- Email-Adresse sind verpflichtender Teil eines Impressums und selbstverständlich ein guter Service für Kunden. Wir empfehlen jedoch, diese Kontaktdaten nicht maschinell auslesbar zu hinterlegen, denn Cyberkriminelle oder Spammer greifen diese Information gerne automatisiert von Unternehmenswebseiten ab. Das führt zu einem erhöhten Spam-Aufkommen und bildet eine Grundlage für mögliche Spear-Phishing Attacken.





SIWECOS
Auf der sicheren Seite

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

SIWECOS – auf der sicheren Seite

Projektdauer: September 2016 – Dezember 2019
Projektpartner: eco e.V. & Ruhr Universität Bochum
Unterstützer: CMS-Garden & Hackmanit

SIWECOS – Der Webseiten-Schutz für KMU

- Kostenlose Webseiten-Schnellprüfung auf der Startseite
- Erweiterte Webseiten-Prüfung mit zusätzlichen Scans für Webseiteneigentümer nach Registrierung
- Tägliche Prüfung der registrierten KMU Webseiten
- Automatische Email-Benachrichtigung bei Erkennung einer Schwachstelle
- Einfache Erklärungen und Beschreibungen – auch für „Nicht-Techniker“
- 5 Scanner mit 39 unterschiedlichen Tests schützen vor 5 Angriffsvektoren
- Einfache Integration in die eigene Webseite mit speziellen CMS-Plugins

SIWECOS – Hoster Service

- Serverseitiger Schutz vor Angriffen direkt bei den Webhostern anhand von proaktiven MOD-Security Regeln
- Der SIWECOS Hoster Service schützt Millionen installierter CMS-Systeme, ohne dass ein Webseiten-Betreiber selbst sofort aktiv werden muss

SIWECOS
Auf der sicheren Seite

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

SIWECOS hilft

Projektpartner

RUHR UNIVERSITÄT BOCHUM RUB

eco Verband der Internetwirtschaft e.V.

Unterstützt durch

cms garden

HACKMANIT

Projekt im Rahmen der Initiative "IT-Sicherheit in der Wirtschaft" des BMWi (Sep 2016 – Dez 2019)

Initiative „IT-Sicherheit in der Wirtschaft"

Die Initiative „IT-Sicherheit in der Wirtschaft" des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: www.it-sicherheit-in-der-wirtschaft.de abrufbar.

Kontakt

Cornelia Schildt
Projektmanagerin IT-Sicherheit

eco – Verband der Internetwirtschaft e.V.
Lichtstraße 43h
50825 Köln

Fon +49 (0) 221 – 7000 48-175
Fax +49 (0) 221 – 7000 48-111
cornelia.schildt@eco.de

Michael Weirich,
Security Analyst

eco – Verband der Internetwirtschaft e.V.
Lichtstraße 43h
50825 Köln

Fon +49 (0) 221 – 7000 48-193
Fax +49 (0) 221 – 7000 48-111
michael.weirich@eco.de