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 Webseiten-Check 2018

Für den SIWECOS KMU Webseiten-Check wurden 1.142 Webseiten kleiner und mittelständischer Unternehmen aus Deutschland mit den Scannern des SIWECOS Projekts auf mögliche Schwachstellen hin geprüft.

eco
VERBAND DER INTERNETWIRTSCHAFT

RUHR
UNIVERSITÄT
BOCHUM
RUB

Projektpartner

HACKMANIT

cms garden

Unterstützt durch

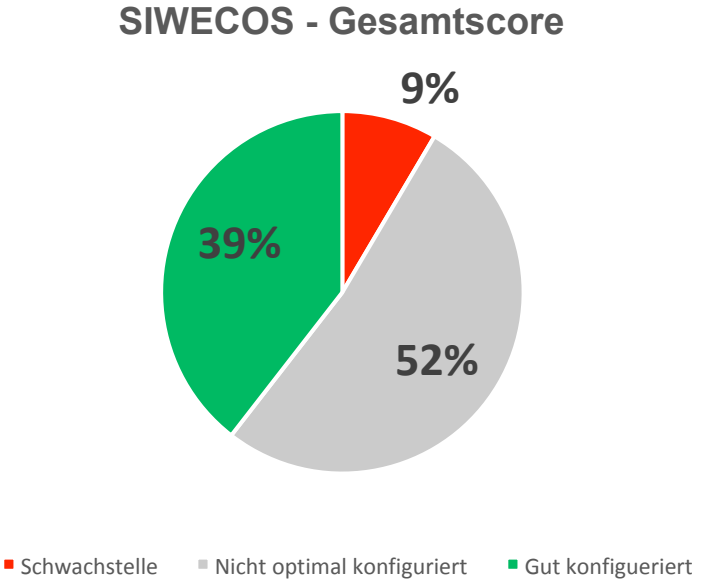
SIWECOS
Auf der sicheren Seite

IT-Sicherheit
IN DER WIRTSCHAFT

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

Über Hälfte aller KMU Webseiten sind aus Sicherheitssicht nicht optimal konfiguriert, fast jede 10 Webseite weist eklatante Sicherheitsmängel auf.

9% aller Webseiten weisen eklatante Sicherheitsmängel auf. Es besteht hier akuter Handlungsbedarf seitens der Webseitenbetreiber.
Außerdem konnten die Experten mit dem SIWECOS Scanner feststellen, dass 52% der geprüften KMU Webseiten nicht optimal konfiguriert sind.
Rund jede zweite Webseite weist zwar keine aktuellen Schwachstellen auf, die eingesetzte Konfiguration ermöglicht jedoch auf mittlere Sicht möglicherweise Cyberangriffe.
Eine Minderheit von 39% der geprüften Webseiten können anhand der von SIWECOS untersuchten Schwachstellen als relativ sicher bezeichnet werden, auch wenn es an der ein oder anderen Stelle sicherlich weitere Optimierungsmaßnahmen gibt. Den Idealwert von 100 erreicht keine der überprüften KMU-Webseiten.



RUHR UNIVERSITÄT BOCHUM RUB

eco

HACKMANIT

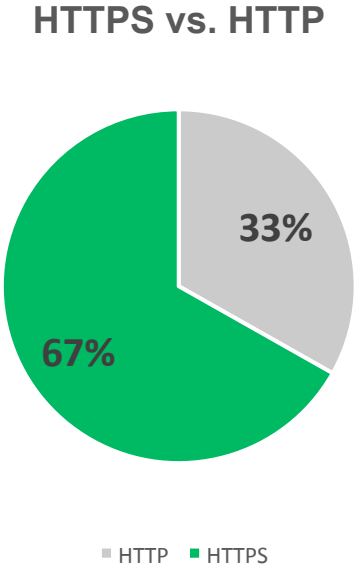
cms garden

Lediglich 67% der KMUs nutzen HTTPs

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“.

Kleinen und mittelständische Unternehmen empfehlen Experten, künftig auf HTTPS zu setzen, um ihre eigene Unternehmenswebseite gegenüber ihren Kunden wieder als sicher auszuweisen.



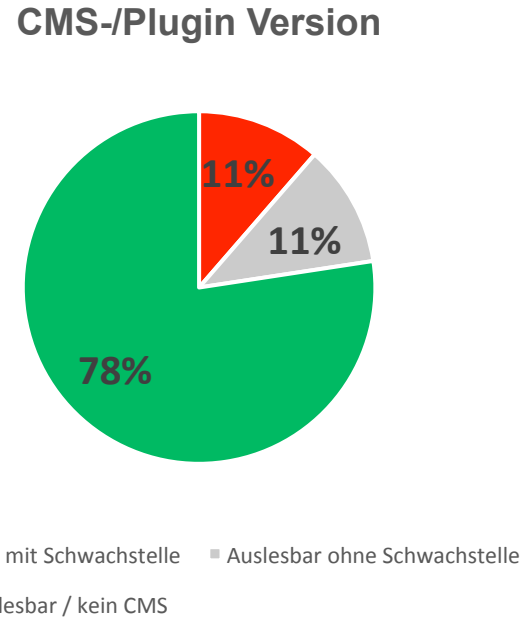
SIWECOS
Auf der sicheren Seite

IT-Sicherheit
IN DER WIRTSCHAFT

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

Bei 22% aller geprüften KMU-Webseiten lässt sich die Version des Content Management Systems oder eines darin installierten Plugins auslesen. Die Hälfte dieser Seiten arbeitet mit einer Version mit bekannten Schwachstellen.

Fast jede vierte übergeprüfte 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. Mehr als jede 10. KMU Webseite weist somit direkt Dritten gegenüber aus, dass Sie verwundbar ist.



RUHR UNIVERSITÄT BOCHUM RUB

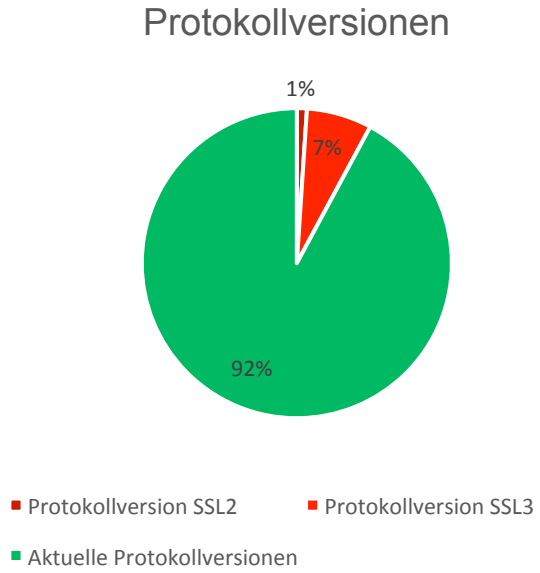
eco

HACKMANIT

cms garden

Etwa 8% der geprüften KMU-Webseiten, die HTTPS einsetzen, nutzen noch die veralteten SSL2/SSL3 Protokolle

SSL2/SSL3 sind veraltete Versionen zur Transportschicht-Sicherheit und werden von modernen Browsern nicht mehr unterstützt. Die überprüften KMU-Webseiten lassen solche Verbindungen weiter zu und ermöglichen es somit möglicherweise Angreifern, die verschlüsselte Kommunikation zwischen Client und Server aufzubrechen.



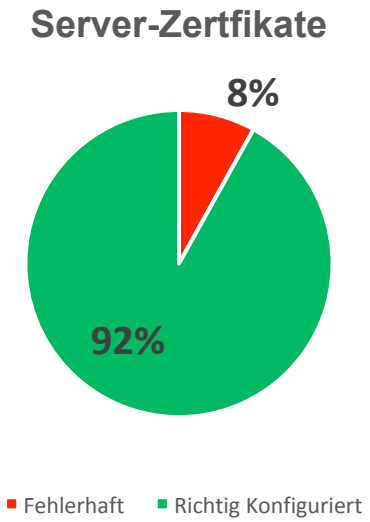
SIWECOS
Auf der sicheren Seite

IT-Sicherheit
IN DER WIRTSCHAFT

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

Über 8% der geprüften KMU-Webseiten weisen abgelaufene Zertifikate auf

Jede 12. geprüfte Webseite, die ein Server-Zertifikat einsetzt, tut 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.



RUHR UNIVERSITÄT BOCHUM RUB

eco

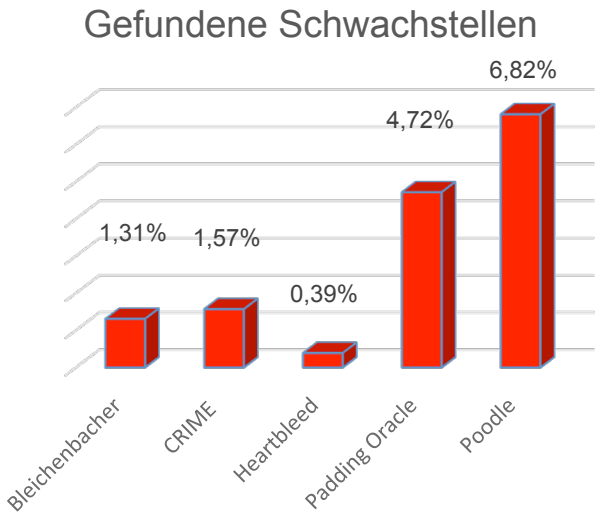
HACKMANIT

cms garden

6,8 Prozent der geprüften KMU Webseiten weisen die Poodle-Schwachstelle auf,

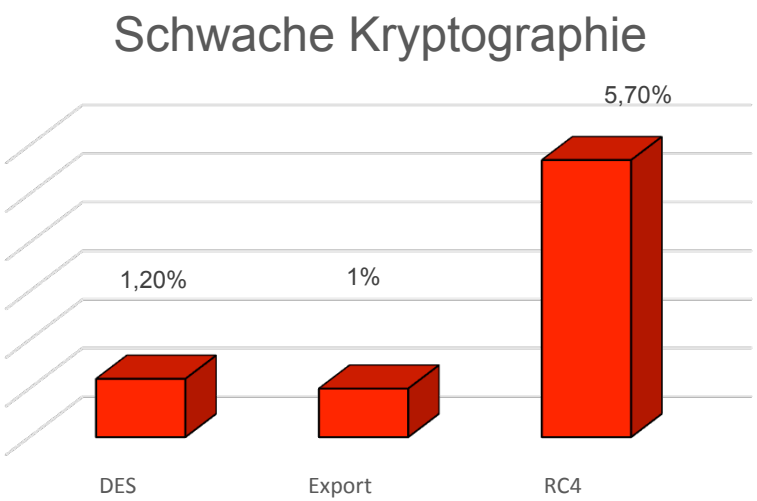
eine 2014 bekannt gewordene schwerwiegende Sicherheitslücke im TLS-Protokoll. Sie erhöht die Gefahr, dass über verschlüsselte Verbindungen private Daten von Clients und Servern ausgelesen werden können durch sogenannte Man-in-the-Middle Angriffe. Weitere 4,7 Prozent der geprüften KMU Webseiten weisen eine Padding-Oracle Schwachstelle auf.

Jede zwölfte geprüfte Webseite, die ein Server-Zertifikat einsetzt, tut dies fehlerhaft. Der überwiegende Teil der Zertifikate ist bei der ausstellenden Zertifizierungsstelle abgelaufen oder setzen schwache kryptographische Funktionen wie etwa SHA1 oder MD5 ein. In beiden Fällen führt dies dazu, dass ein Besucher beim Aufruf der Webseite gewarnt wird.



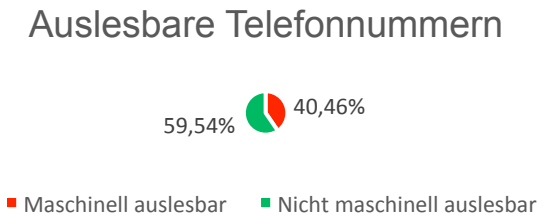
Fast 6% der geprüften KMU Webseiten setzen eine schwache Kryptographische Verschlüsselung (Ciphersuites) ein

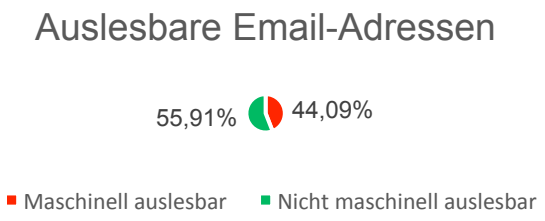
Ciphersuites bezeichnet das kryptographische Verschlüsselungsverfahren bei der Kommunikation zwischen Client und Server. Mit dem Einsatz von Chiffreverfahren wie RC4 riskieren Webseitenbetreiber die Sicherheit ihrer Kunden erheblich.



40,5% aller geprüften KMU-Webseiten haben maschinell auslesbare Telefon-Nummern auf der Startseite, 44,1 % maschinell auslesbare Email-Adressen.

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 – Oktober 2018
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 von Angriffen direkt bei den Webhostern anhand von proaktiven MOD-Security Regeln
- Der SIWECOS Hoster Service schützt Millionen installierten CMS-Systemen, ohne dass ein Webseiten-Betreiber selbst und sofort aktiv werden muss

RUHR UNIVERSITÄT BOCHUM RUB

eco

HACKMANIT

cms garden

HTTPS://SIWECOS.DE

SIWECOS
Auf der sicheren Seite

IT-Sicherheit
IN DER WIRTSCHAFT

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

Kontakt

Peter Meyer
Projektleiter SIWECOS
peter.meyer@eco.de

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

Fon +49 (0) 221 – 7000 48-194
info@siwecos.de

RUHR UNIVERSITÄT BOCHUM RUB

eco

HACKMANIT

cms garden

„IT-Sicherheit in der Wirtschaft"

Projekt im Rahmen der Initiative "IT-Sicherheit in der Wirtschaft" des BMWi (Sep 2016 – Nov 2018)

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. Gemein-sam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseins-bildung 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.

RUHR UNIVERSITÄT BOCHUM RUB

eco

Partner und Unterstützer

HACKMANIT

cms garden