SIWECOS
Auf der sicheren Seite

IT-Sicherheit
IN DER WIRTSCHAFT

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

Auf der sicheren Seite – Mittelstandsgerechte Lösungen zum Webseitenschutz

Cornelia Schildt
eco e.V

Projektpartner

RUHR UNIVERSITÄT BOCHUM
RUB

eco
Verband der Internetwirtschaft e.V.

Unterstützt durch

cms garden

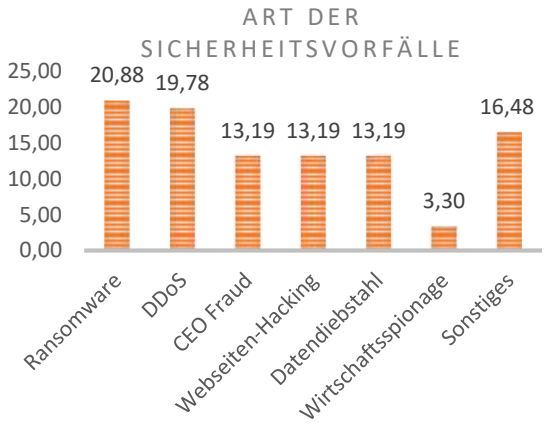
HACKMANIT

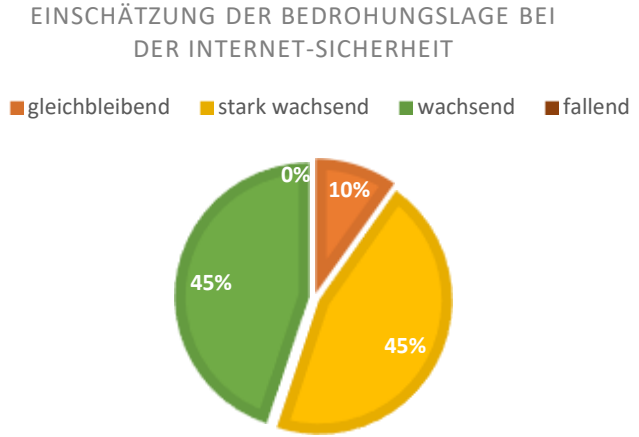
Aktuelle Lage der IT-Sicherheit in KMU

http://www.wik.org/index.php?id=869&L=2

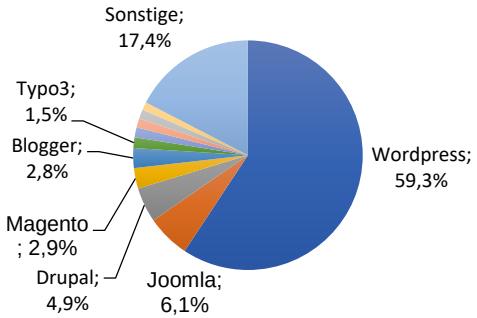
eco Sicherheitsumfrage 2019

- KMUs beliebtes Ziel, weil oft Wissen und Ressourcen zur Schutz vor Cyber-Angriffen fehlen
- Insbesondere bei IT-fernen Branchen fehlt oft das Bewusstsein für Cyberkriminalität
- Haupt-Angriffs-Vektor bei KMUs sind Sicherheitslücken bei Webanwendungen und Webservern





Einfallstor Webseite

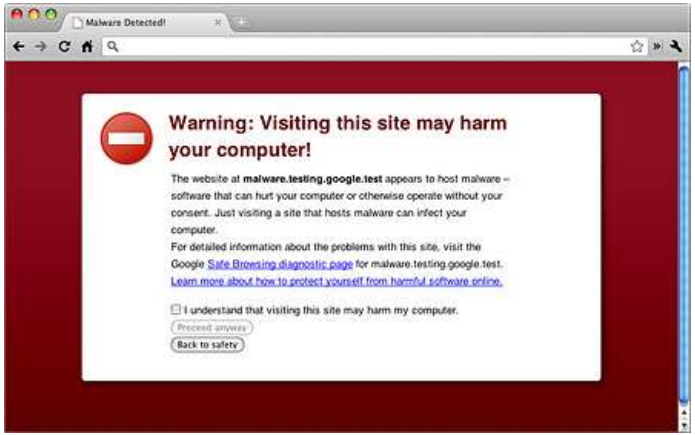


- 97% der Cyberangriffe erfolgen auf Sicherheitslücken bei weit verbreiteter Standardsoftware
- Die meisten Angriffe sind dabei gestreut, nicht gezielt
- Sicherheit der Webseite wird bei KMU oft vernachlässigt

Viele Risiken lassen sich mit einfachen Mitteln mindern:

- Sichere Zertifikate und Webserver-Verschlüsselung
- Sicher konfigurierte Webserver und Webseiten
- Zeitnahe, im Idealfall automatisierte Sicherheits-Updates
- Regelmäßige Überprüfung der Webseite und Benachrichtigung bei Schwachstellen oder Virenbefall

Warnung an Besucher



- Automatische Warnung an Besucher bzw. Kunden
- Warnhinweis bleibt i.d.R. 30 Tage bestehen
- Nicht sehr einfach, sich eher “entlisten” zu lassen
- Das Internet vergisst nicht – die Informationen lässt sich auch viele Jahre später finden

Warnung an Besucher

- Beim Besuch von unsicheren Webseiten wird automatisch gewarnt (ohne HTTPS)
- Trotz Ausnahme-Funktion erweckt diese Meldung bei Kunden einen schlechten Eindruck

SIWECOS steht für Sichere Webseiten und Content Management Systeme und hilft Unternehmen Sicherheitsprobleme auf Webseiten rasch **zu erkennen und zu beheben**.

Partner und Unterstützer

IT-Sicherheit in der Wirtschaft

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 – Oktober 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.

SIWECOS – auf der sicheren Seite

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

Ziele:

- Erkennung und Behebung von Sicherheitslücken auf Webseiten
- Stärkung des Bewusstsein für sicheren Webseiten bei KMU

Partner und Unterstützer

SIWECOS – in 2 Minuten

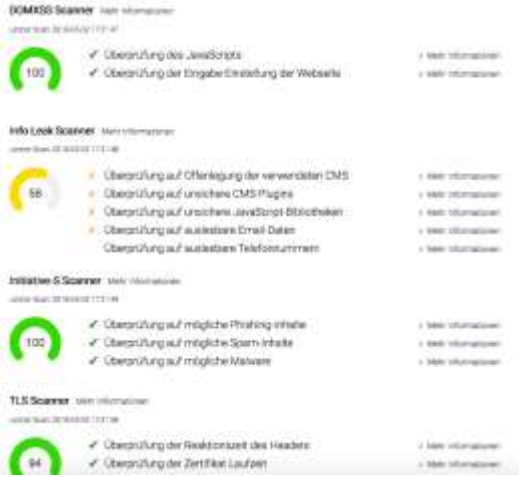
https://www.youtube.com/watch?v=HfwMBpjIlHE&

5 Scanner – 5 Angriffsvektoren

- **TLS-Scanner** überprüft Zertifikate, Protokollversionen & Verschlüsselungsalgorithmen
- **DOMXSS-Scanner** zur Schwachstellenerkennung bei *DOM* Cross-Site Scripting Anfälligkeit
- **HTTP-Security-Header-Scanner** prüft die Privatsphäre sowie den Clickjacking-und XSS-Schutz um Spoofing-Angriffe zu verhindern
- **Information-Leakage-Scanner** prüft die Privatsphäre-Einstellungen des CMS
- **Initiative-S Scanner** prüft Webseite auf Virenbefall oder Kompromittierung durch Fremdinhalte wie Phishing

Partner und Unterstützer

SIWECOS – Auf der sicheren Seite



Signal-Anzeige für die unterschiedlichen Schwachstellen

Einfache Erklärungen und Beschreibungen – auch für „nicht-Techniker“

Ausführliches WIKI zur Erläuterung der Begriffe

Partner und Unterstützer

SIWECOS – CMS-Plugin

SIWECOS Sicherheits-Informationen für die eigene Webseite direkt im CMS

- Einfache Implementierung und Nutzung als Add-On der CMS-Installation
- Direkte Sichtbarkeit im CMS erzielt eine höhere Aufmerksamkeit beim Nutzer
- Aktuell stehen SIWECOS Plugins für WordPress, Joomla und Contao bereit.

Partner und Unterstützer

SIWECOS – Hoster Service

- Direkte Schnittstelle zu beteiligten Webhostern in Deutschland
- Aktive Kommunikation von Filter-Regeln zur Abwehr von Angriffen (ModSecurity)
- Serverseitiger Schutz von Angriffen auf die beim Webhoster installierte Webseiten – bevor die Webseiten-Betreiber infiziert werden können.
- Ermöglicht den proaktiven Schutz von Millionen installierten CMS-Systemen, ohne dass der Webseiten-Betreiber selbst und sofort aktiv werden muss.

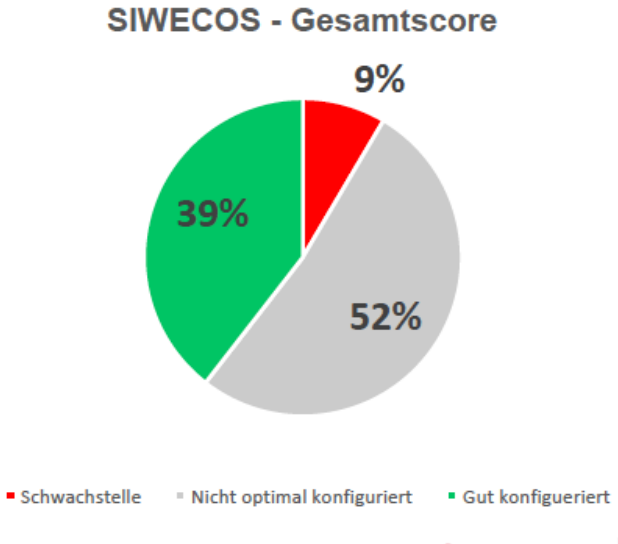
Weitere Informationen und Kontakt:
https://siwecos.de/service-fuer-webhoster/
hosterservice@siwecos.de

Partner und Unterstützer

SIWECOS – KMU Check

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.



Partner und Unterstützer

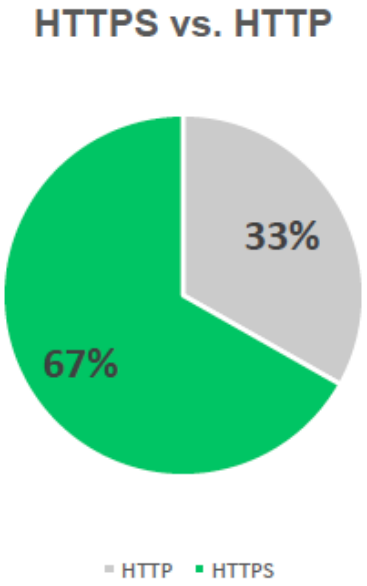
SIWECOS – KMU Check

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.

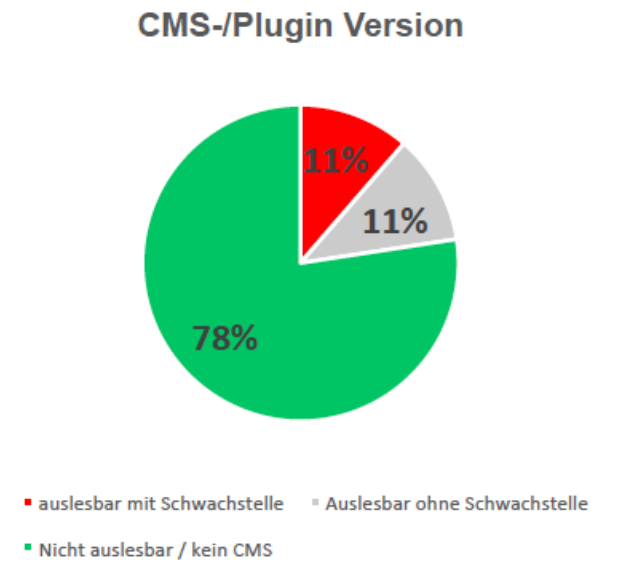


Partner und Unterstützer

SIWECOS – KMU Check

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 Versionsangebe.
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.

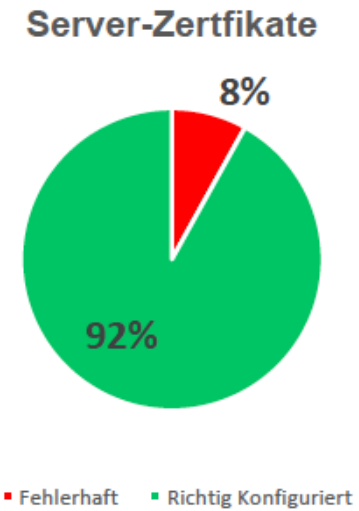


Partner und Unterstützer

SIWECOS – KMU Check

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.



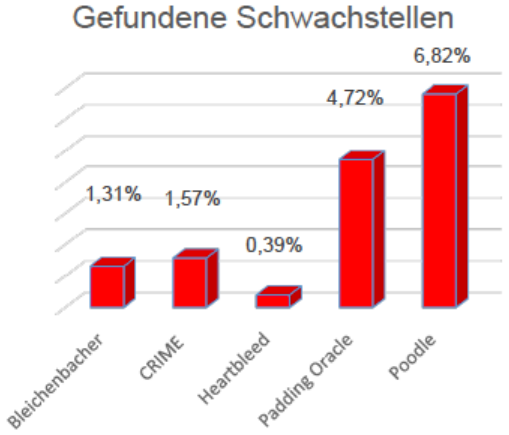
Partner und Unterstützer

SIWECOS – KMU Check

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.



Partner und Unterstützer

SIWECOS bietet

- einen Webseitencheck, der Sicherheitslücken in Content Management Systemen aufdeckt.
- individuelle Benachrichtigungen und Handlungsempfehlungen zu Sicherheitsproblemen auf Ihrer Webseite.
- kompetente Ansprechpartner mit jahrelanger Erfahrung im Bereich IT-Sicherheit.
- und das alles völlig kostenlos

Partner und Unterstützer

Kontakt

Cornelia Schildt
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
https://www.eco.de
https://www.siwecos.de