

Webinar
IHK Spezial

Update Cyber Resilience Act: Ist Ihr Schwachstellenmanagement bereit für den CRA?

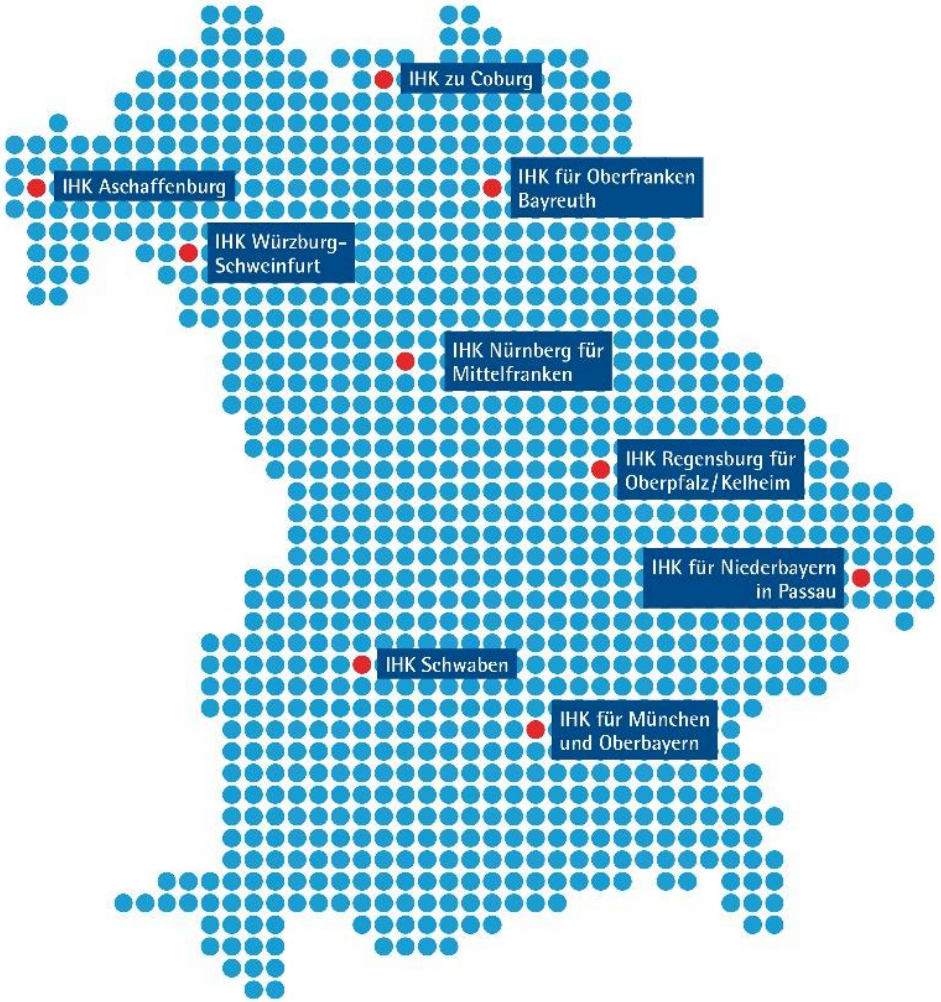
IHK Schwaben

IHK Schwaben

Digitalisierungsinitiative Ihrer bayerischen IHKs

IHK Industrie- und Handelskammern in Bayern

https://www.bihk.de/cra



Digitalimpulse

Digitalimpulse im Rahmen des bayerischen Pakts für berufliche Weiterbildung

Kooperation von:

IHK Industrie- und Handelskammern in Bayern

Bayerisches Staatsministerium für Digitales

https://www.kommweiter.bayern.de/mit-unterstuetzung/pakt-fuer-berufliche-weiterbildung/

und

https://www.bihk.de/data-act

Unterstützer

CYBERsicher
EASY.CRA
Tool zur Umsetzung
des Cyber Resilience Act

CYBERsicher
OT-CRAft
Sichere Geräte.
Resiliente Anlagen.

DIHK
Deutsche
Industrie- und Handelskammer

bayern
innovativ
Sicherheit
Cybersecurity

STE WERK18®
Weichen in die
digitale Zukunft

Sicherheitsnetzwerk
München

ITSECURITY
www.it-sicherheitscluster.de

ROSIK e.V.

Allianz für
Cyber-Sicherheit
Multiplikator

NL Niederlande

Webinarreihe:
Cyber Resilience Act



03.09.2026 Wie Unternehmen künftig sicherere Soft- und Hardware beschaffen können

04.09.2026 Wen betrifft es und was bedeutet es für diese Unternehmen?

08.09.2026 Ist Ihr Schwachstellenmanagement bereit für den CRA?

16.09.2026 Meldepflichten für betroffene Unternehmen

06.10.2026 Deep Dive SBOM: Wie setzte ich es in der Praxis um?

Anmeldung und weitere Infos:

www.bihk.de/cra

Was müssen Unternehmen jetzt konkret umsetzen?



- EU-Regeln für sichere digitale Produkte
- Cybersecurity über den gesamten Produktlebenszyklus
- Pflichten für Hersteller: Updates, Schwachstellen & CE-Kennzeichnung

PROF. DR. DOMINIK MERLI

Professor für IT-Sicherheit @ THA

- **Praktiker**
  - Praxiserfahrung @ Fraunhofer und Siemens CT
  - Seit 2017 mehr als 60 Kooperationsprojekte mit Unternehmen
- **Forscher**
  - Institutsleiter THA_innos mit 6 Nachwuchsforschern im Team
- **Autor**
  - Buch „Engineering Secure Devices“ (No Starch Press, Juni 2024)



AUS AKTUELLEM ANLASS

Was gilt ab dem 11. September 2026 bzgl. Cyber Resilience Act (CRA)?



↗ **Meldepflichten**

- für aktiv ausgenutzte Schwachstellen
- und schwerwiegende Sicherheitsvorfälle mit Auswirkungen auf die Sicherheit von Produkten mit digitalen Elementen

AKTIV AUSGENUTZTE SCHWACHSTELLEN

Schwachstellen, für die „verlässliche Nachweise vorliegen, dass ein böswilliger Angreifer sie […] ausgenutzt hat“.

- **Verlässliche Nachweise?**
  - Eigene oder durch Kunden/Benutzer/Dritte bereitgestellte, belastbare Monitoring Daten

- **Beispiel-Schwachstellen:**
  - Umgehung von Authentifizierungsmaßnahmen
  - Manipulation oder Exfiltration von Daten



SCHWERWIEGENDE SICHERHEITSVORFÄLLE

… mit Auswirkungen auf die Sicherheit von Produkten mit digitalen Elementen!

- **Sicherheitsvorfälle beim Nutzer/Kunden?**
  - Nein!
- **Sicherheitsvorfälle beim Hersteller, z.B.**
  - Kompromittierung der Entwicklungsumgebung
  - Manipulation der Produktionsumgebung
  - Unberechtigter Zugriff auf Cloudservice für Produkte



JETZT SCHON?!

Gilt das auch schon für Produkte, die vor dem 11. Dezember 2027 auf den Markt gebracht wurden?

↗ JA!



ABER WO MELDEN?

ENISA Single Reporting Platform (SRP):

- https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp

- **Verfügbarkeit**
  - Ab dem 11. September 2026

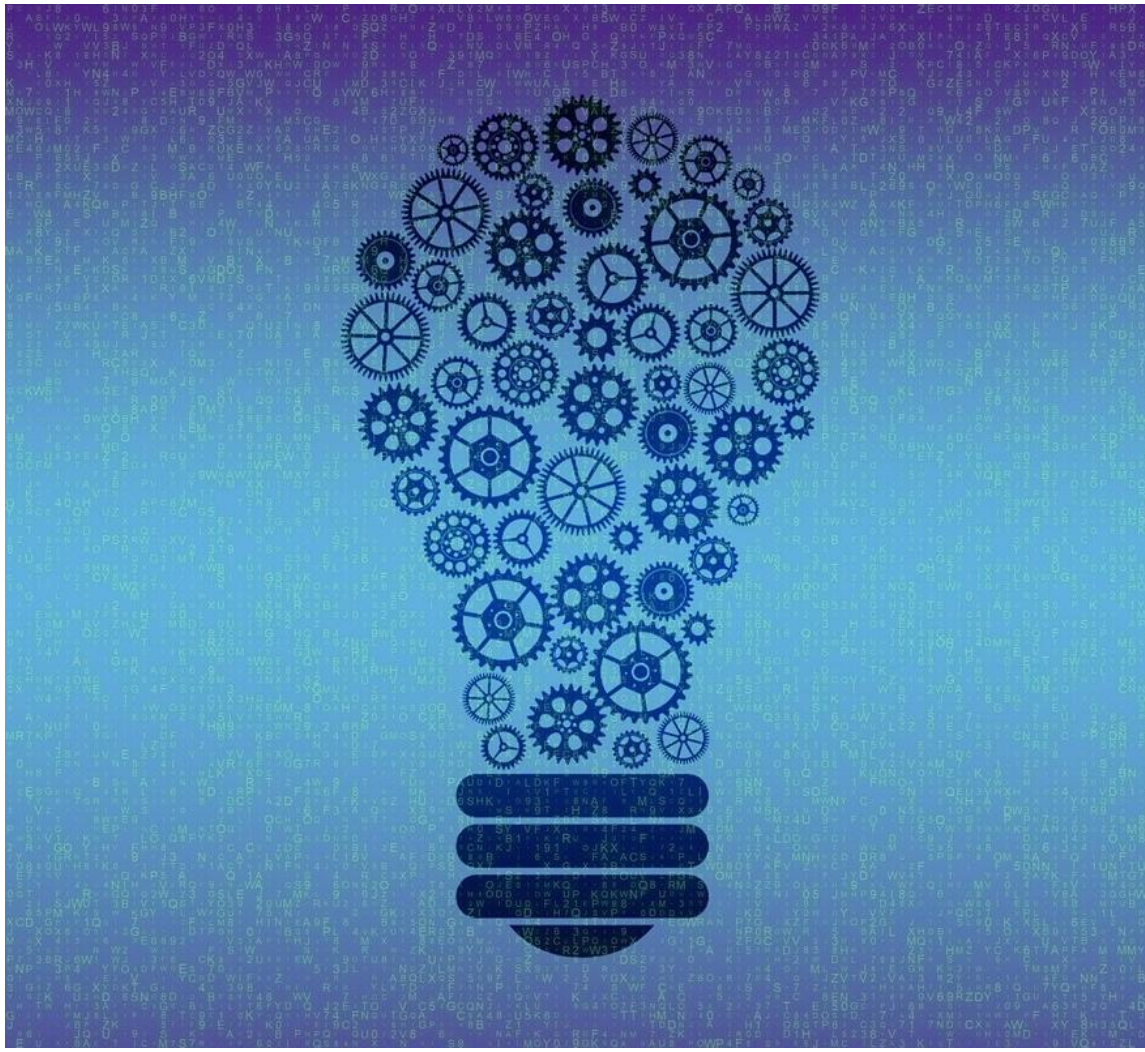
- **Aktuell bereits viele Informationen online**
  - 25 FAQs und „Guidance“ Dokumente



SCHWACHSTELLENMANAGEMENT

… ist komplex und braucht belastbare Prozesse!

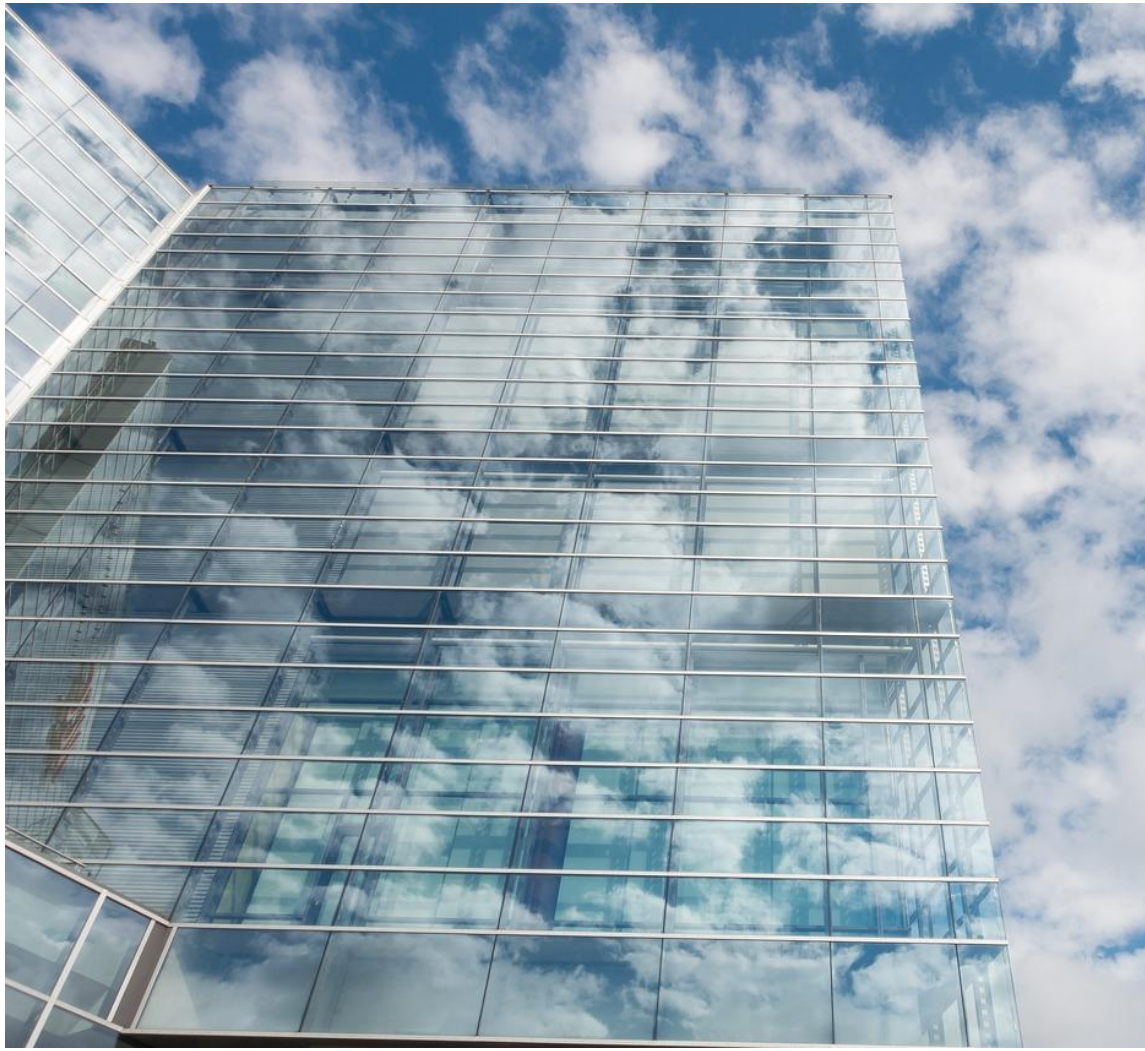
- **Verantwortung und Ressourcen**
  - Wert hat den Product-Security-Hut auf?
  - Klares Management Commitment nötig
- **Koordination des Schwachstellenmanagements**
  - Process-Owner, Knotenpunkt für Informationen
  - Interne Vernetzung und Kommunikation
  - Update-Entwicklung, Offenlegung, etc.



TRANSPARENZ

Wer hat den Überblick was alles im Produkt steckt?

- **Software-Bill-of-Materials (SBOM)**
  - Maschinenlesbare „Liste“ für Softwarekomponenten
- **Third-Party Komponenten**
  - Anforderungen an externe Komponenten?
  - Ansprechpartner/Prozesse im Schwachstellenfall?
- **Chance: Ausmisten!**
  - Transparenz kann viele positive Effekte haben!



SECURITY TESTING

… um die „Sicherheit des Produkts mit digitalen Elementen regelmäßig und wirksam“ zu testen!

- **Bereits während der Entwicklung**
  - Kurze Feedbackschleifen = Kostenersparnis
- **Validierung von Sicherheitsmaßnahmen**
  - z.B. korrekte Funktion von Authentifizierungsmodulen
- **Penetration Testing**
  - Simulierte Angriffe, oft durch Externe



EINE KONTAKTMÖGLICHKEIT ZUM MELDEN VON SCHWACHSTELLEN

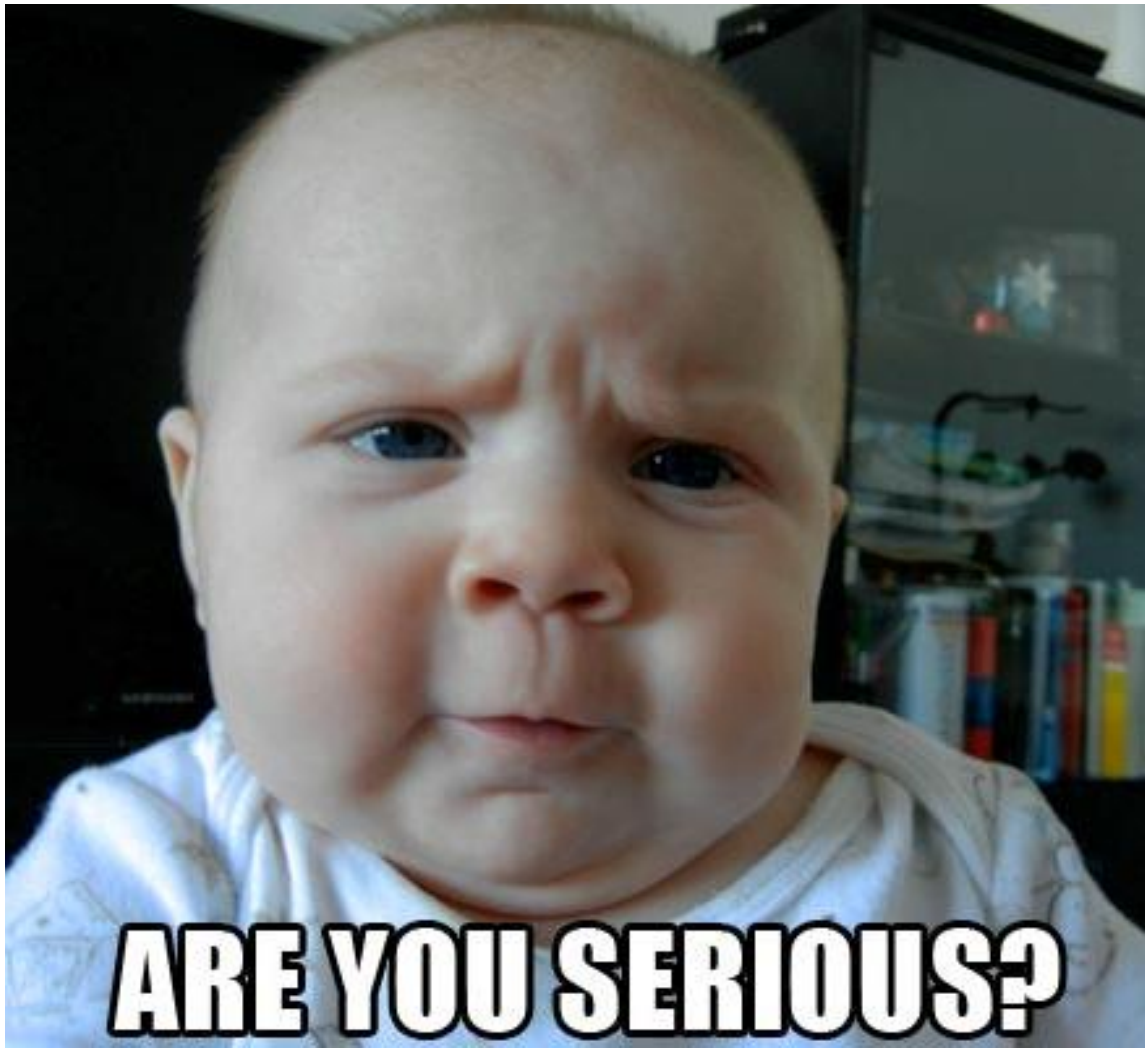
… ist unverzichtbar!

- **An wen sollen Externe Schwachstellen melden?**
  - info@... ? datenschutz@... ? heise.de ? Handelsblatt ?
- **Einfache und gleichzeitig moderne Lösung**
  - security.txt nach RFC 9116: https://securitytxt.org/
  - standardisiert, maschinenlesbar, klar



SECURITY.TXT IN DER PRAXIS

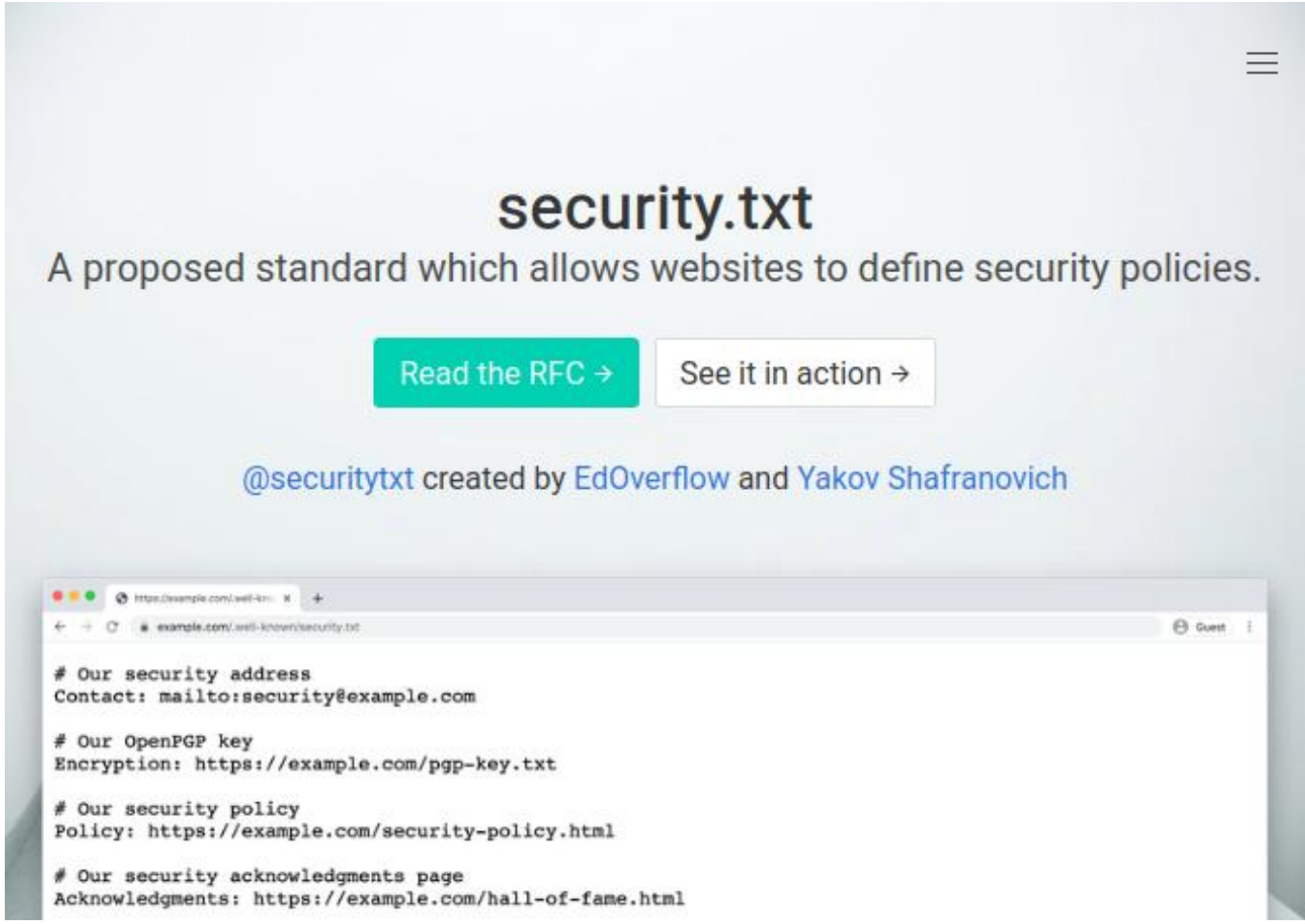
- **Analyse der security.txt bei Mitgliedern des VDMA**
  - durchgeführt Anfang September 2026
- **3084 „Unique Hosts“ für 3552 VDMA Mitglieder**
  - 2773 (90%) stellen keine security.txt bereit
  - 125 (4%) haben eine RFC-konforme security.txt
  - 83 (2.7%) liefern eine security.txt mit kleineren Mängeln
  - 103 (3.3%) weisen grobe Mängel in der security.txt auf



WAS STEHT FÜR DIESE WOCHE NOCH AUF IHRER TODO-LISTE?

Genau! … security.txt einrichten!

- **Hier geht‘s zur Website:**
  - https://securitytxt.org/
- **Und hier zum RFC 9116 mit allen Details:**
  - https://www.rfc-editor.org/info/rfc9116/



FREQUENTLY ASKED QUESTIONS

FAQs zur Umsetzung des CRA:

↗ https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions

↗ **Praxisnahe Fragen**

- Mehr als 70 Fragen in 7 Kategorien

↗ **Antworten zur Unterstützung der CRA Umsetzung**

- Ausführliche Informationen auf 66 Seiten



FAZIT

Schwachstellenmanagement ist jetzt Pflicht!

- Klären Sie die **Verantwortlichkeiten**.
- Schaffen Sie **Kontaktmöglichkeiten**.
- Etablieren Sie **Schwachstellenmanagementprozesse**.
- Und – falls noch nicht geschehen:
  Analysieren Sie Ihre **Produkt-Cybersicherheitsrisiken**!



Cyber-Security-Awareness-Test

IHK Schwaben

Wie fit ist Ihr Team in Sachen Cyber Security?



kostenfrei anmelden:

Veranstaltungstipp

IHK Schwaben

Unsere nächsten Webinare im Themenfeld Digitalisierung und KI

Digitale Souveränität durch Open Source

Donnerstag, 24.09.2026 | 10:00 - 11:00 Uhr

Maximilian Arnold

Technischer Leiter QA & Installationen | TUXEDO Computers GmbH

Anmeldung:

BIHK: Reihe IT-Sicherheit

Mit KI statt gegen KI: Mitarbeitende motivieren, Ängste abbauen, Erwartungen klären

Mittwoch, 14.10.2026 | 10:00 - 11:00 Uhr

Dr. Jens Nachtwei

Humboldt-Universität zu Berlin | Hochschule für angewandtes Management

Anmeldung:

BIHK: Webinarreihe KI

AI Convention 2027

IHK Schwaben



Kommen Sie bei Fragen gerne auf mich zu!

Luzia Ghoggal



Digitale Innovation und Künstliche Intelligenz

luzia.ghoggal@schwaben.ihk.de

0821/3162-230



IHK Schwaben



Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen unter
ihk.de/schwaben/ihkspezial