

► WAS IST DAS?

Ein schrittweiser Ansatz für das Pentesting von Produkten mit digitalen Elementen (PDE) in Übereinstimmung mit dem Cyber Resilience Act (CRA).

► FÜR WEN IST ES GEDACHT?

Kleine und mittlere Unternehmen (KMU), die Produkte mit digitalen Elementen herstellen.

CRA-KONFORME PENETRATIONSTEST-METHODIK



CONFIRMATE

Das im Rahmen der Fördervereinbarung Nr. 101190193 finanzierte Projekt wird vom Europäischen Kompetenzzentrum für Cybersicherheit unterstützt.

► WICHTIGE HINWEISE !!!

Die CRA verlangt keine Penetrationstests an sich, schreibt jedoch „wirksame und regelmäßige Überprüfungen und Tests“ der Produktsicherheit vor. Testmaßnahmen können die Evidenzbasis für eine Erklärung zur Einhaltung der wesentlichen Cybersicherheitsanforderungen der CRA stärken.

► IST ALLES NEU?

Nein, die Methode basiert auf Industriestandards: OSSTMM3, ETSI EN 303 645 und TS 103 701, OWASP Testing Guide, PTES und NIST SP 800-115.

► SCHRITT FÜR SCHRITT



1. Vorbereitungsphase und Planung

Festlegung des Umfangs, der CRA-Anforderungen, der Testumgebungen und der Genehmigungen sowie Abstimmung mit den Beteiligten

Ergebnis: Testplan, rechtliche Dokumente, erste Risikobewertung



2. Informationsbeschaffung und Aufklärung

Angriffsfläche kartieren, OSINT sammeln und realistische Angriffsszenarien definieren

Ergebnis: Profil des Angreifers, erste Erkenntnisse über Schwachstellen



3. Ausführung und Ausnutzung

Schwachstellen mit Tools und manuellen Überprüfungen testen und Simulation von Angriffen im Labor

Ergebnis: Vollständiger Schwachstellenbericht



4. Auswirkungsanalyse und Berichterstattung

Schweregrad bewerten, CRA zuordnen, Abhilfemaßnahmen festlegen

Ergebnis: CRA-zugeordnete Ergebnisse, Strategie für Abhilfemaßnahmen



5. Nachbereitung und Follow-up

Korrekturen überprüfen, Durchführung erneuter Tests, Sammeln von Feedback und gegebenenfalls Vorbereitung von Offenlegungen

Ergebnis: Abschließender Pentest-Bericht zur Einhaltung der CRA-Vorschriften

ÜBER CONFIRMATE

Optimieren und automatisieren Sie die Einhaltung des Cyber Resilience Act (CRA)! Durch die Entwicklung von Open-Source-Tools, standardisierten Methoden und Schulungsressourcen versetzen wir KMU in die Lage, Cybersicherheitsanforderungen einfach und effizient zu erfüllen. Unser Ziel ist es, ein dynamisches Ökosystem zu schaffen, in dem Interessengruppen bewährte Verfahren austauschen, sich über regulatorische Entwicklungen auf dem Laufenden halten und zur Weiterentwicklung sicherer digitaler Produkte beitragen können.

MEHR SEHEN



[CONFIRMATE](#)



www.confirmate-project.eu



confirmate.project@gmail.com



[cyen-cybersecurity](https://www.youtube.com/c/cyen-cybersecurity)