CONFIRMATE

Konformitätsbewertung, Metriken und Compliance-Automatisierung für den Cyber Resilience Act

Methodik für Penetrationstests

Ausgabedatum: 2025-08-05
Status: Überprüft
Version: 0.3

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Das im Rahmen der Fördervereinbarung **Nr. 101190193** finanzierte Projekt wird vom Europäischen Kompetenzzentrum für Cybersicherheit unterstützt. Die geäußerten Ansichten und Meinungen sind jedoch ausschließlich diejenigen der Autoren und spiegeln nicht unbedingt die Ansichten der Europäischen Union oder des Europäischen Kompetenzzentrums für Cybersicherheit wider. Weder die Europäische Union noch die Bewilligungsbehörde können dafür haftbar gemacht werden.

Änderungsliste

Version	Datum	Beschreibung	Autor(en)
0.1	21/03/25	Erster Entwurf der Methodik, der den Partnern zur Überprüfung und Rückmeldung vorgelegt wurde	Cyen
0.2	08/04/25	Aufgrund des Feedbacks von Partnern wurden Änderungen vorgenommen	Cyen
0.3	05/08/25	Aufgrund von Rückmeldungen von Kolleg*innen wurden Änderungen vorgenommen	Cyen

Wir bedanken uns herzlich bei den Fachgutachtern, insbesondere Krasen Parvanov (QRTECH), Stijn Horemans (Refracted), Ayman Khalil und Romain Muguet (Red Alert Labs), Peter Kuzmin (Kikimora) und Dominik Holzapfel (Nviso), für ihre kritischen Anmerkungen und ihr konstruktives Feedback, die wesentlich zur Verbesserung der Genauigkeit und Klarheit dieser Methodik beigetragen haben.

CRA-Compliance-Penetrationstest-Methodik für KMU

Inhalt

1. Referenzen

- Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) Nr. 2019/1020 sowie der Richtlinie (EU) 2020/1828 (Cyber-Resilienz-Gesetz), abrufbar unter: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
- Institut für Sicherheit und offene Methoden (ISECOM). (2010). Open Source Security Testing Methodology Manual (OSSTMM) Version 3.0, verfügbar unter: https://www.isecom.org/OSSTMM.3.pdf
- Penetration Testing Execution Standard (PTES) PTES Organization. (o. J.). Penetration Testing Execution Standard (PTES), verfügbar unter: https://www.pentest-standard.org/index.php/Main_Page
- Scarfone, K., & Mell, P. (2008). Technical Guide to Information Security Testing and Assessment (NIST SP 800-115), verfügbar unter: https://csrc.nist.gov/pubs/sp/800/115/final
- OWASP Foundation. (o. J.). OWASP Web Security Testing Guide (WSTG), verfügbar unter: https://owasp.org/www-project-web-security-testing-guide/
- MITRE Corporation. (o. J.). MITRE ATT&CK® Framework, verfügbar unter: https://attack.mitre.org/
- Open Information Systems Security Group (OISSG). (2005). Information Systems Security Assessment Framework (ISSAF) Draft 0.2, verfügbar unter: https://untrustednetwork.net/files/issaf0.2.1.pdf
- Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) Europäische Zentralbank. (2023). TIBER-EU-Rahmenwerk: Bedrohungsinformationsbasiertes ethisches Red Teaming, verfügbar unter: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
- ETSI TS 103 701 V1.1.1 (2021-08): Cybersicherheit für das Internet der Dinge für Verbraucher: Konformitätsbewertung der Grundanforderungen. Available here: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

2. Glossar: Akronyme, Begriffe und Abkürzungen

Abkürzungen

OSSTMM:	**Handbuch zur Open-Source-Sicherheitstestmethodik**
OWASP:	**Open Web Application Security Project**
PTES:	**Standard für die Durchführung von Penetrationstests**
NIST:	**Nationales Institut für Standards und Technologie**
SIEM:	**Sicherheitsinformations- und Ereignismanagement**
IAM:	**Identitäts- und Zugriffsmanagement (kontextbezogen abgeleitet)**
API:	**Anwendungsprogrammierschnittstelle**
VPN:	**Virtuelles Privates Netzwerk**
SSO:	**Einmalige Anmeldung**
IoT:	**Internet der Dinge**
GDPR:	**Datenschutz-Grundverordnung**
ISO:	**Internationale Organisation für Normung**
IEC:	**Internationale Elektrotechnische Kommission**
CIS:	**Center for Internet Security**
CMMC:	**Cybersecurity Maturity Model Certification**
PSD2:	**Revidierte Zahlungsdiensterichtlinie**
SWIFT CSP:	**Society for Worldwide Interbank Financial Telecommunication Customer Security Programme**

Bedingungen

Penetrationstests (oder Pen-Tests):	Eine Sicherheitsübung, bei der ein Cybersicherheitsexperte versucht, Schwachstellen in einem Produkt und dessen Umgebung, einschließlich Hardware, Software, Schnittstellen und Benutzeroberflächen, zu finden und auszunutzen.

Sicherheitslücke:	Eine Schwäche oder ein Fehler in einem System, einer Anwendung oder einem Netzwerk, die ausgenutzt werden kann, um die Sicherheit zu gefährden.
Exploit:	Ein Stück Code, eine Technik oder ein Prozess, der eine Schwachstelle ausnutzt, um ein unbeabsichtigtes Verhalten in einem System zu verursachen.
Bedrohungsakteur:	Eine Person oder Gruppe, die ein potenzielles Risiko für die Cybersicherheit eines Unternehmens darstellt, kann aus Hackern, Insidern oder Wettbewerbern bestehen.
Risikobewertung:	Der Prozess der Identifizierung von Risiken, die sich negativ auf die Geschäftstätigkeit eines Unternehmens auswirken könnten.
Sicherheitsaudit:	Eine systematische Bewertung der Sicherheitslage eines Produkts mit digitalen Elementen, bei der die Übereinstimmung mit vordefinierten technischen und regulatorischen Anforderungen, wie z. B. der CRA, gemessen wird.
Plan zur Reaktion auf Vorfälle:	Eine Reihe von Anweisungen, die Unternehmen dabei helfen, Sicherheitsvorfälle in Computernetzwerken zu erkennen, darauf zu reagieren und sie zu beheben.
Verschlüsselung:	Die Methode, mit der Informationen in einen geheimen Code umgewandelt werden, der die wahre Bedeutung der Informationen verbirgt.
Hersteller:	Eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder Produkte mit digitalen Elementen entwerfen, entwickeln oder herstellen lässt und diese unter ihrem Namen oder ihrer Marke gegen Entgelt, zur Monetarisierung oder kostenlos vermarktet.
Multi-Faktor-Authentifizierung (MFA):	Eine Authentifizierungsmethode, bei der der Benutzer zwei oder mehr Verifizierungsfaktoren angeben muss, um Zugriff auf eine Ressource zu erhalten, z. B. eine Anwendung, ein Online-Konto oder ein VPN.
Social Engineering:	Die Taktik, ein Opfer zu manipulieren, zu beeinflussen oder zu täuschen, um die Kontrolle über ein Computersystem zu erlangen oder persönliche und finanzielle Informationen zu stehlen.

Taktiken, Techniken und Verfahren (TTP):	Beschreibt das Verhalten eines Bedrohungsakteurs und einen strukturierten Rahmen für die Durchführung eines Cyberangriffs.
CIA-Triad (Vertraulichkeit, Integrität, Verfügbarkeit):	Ein Informationssicherheitsmodell zum Schutz sensibler Informationen vor Datenverletzungen.
Produkt mit digitalen Elementen (PDE):	Ein Produkt, das Software oder Firmware enthält oder mit dieser verbunden ist und Daten erfassen, übertragen oder verarbeiten kann. PDEs umfassen sowohl physische Geräte als auch softwaredefinierte Produkte, die auf den Markt gebracht oder in Betrieb genommen werden.

3. Einführung

3.1 Zweck und Ziele

Dieses Dokument beschreibt, wie Penetrationstests für Produkte mit digitalen Elementen (PDEs) verwaltet und durchgeführt werden, um die Überprüfung der Konformität mit dem Cyber Resilience Act (CRA) zu unterstützen. Diese Methodik schließt die praktische Lücke, indem sie einen CRA-konformen Pentesting-Workflow definiert, der auf das Risiko auf Produktebene zugeschnitten ist und sich darauf konzentriert, wie solche Tests eine Konformitätserklärung unterstützen. Obwohl das CRA weder auf Penetrationstests verweist noch diese vorschreibt, bleiben diese eine der wirksamsten Techniken, um festzustellen, inwieweit potenzielle Schwachstellen von einem Angreifer ausgenutzt werden können. Folglich kann eine erfolgreiche Penetrationstestung die Evidenzbasis für eine Konformitätserklärung stärken.

Bei der Entwicklung dieser Methodik wurde ein Satz von Produkten berücksichtigt, die in Anhang A aufgeführt sind. Diese Produkte umfassen verschiedene Kritikalitätsstufen, die im Cyber Resilience Act (CRA) definiert sind. Diese Produkte wurden ausgewählt, um sicherzustellen, dass die Methodik für verschiedene Anwendungsfälle anwendbar und praktikabel ist, und sie dienen als Entwicklungsziel für alle Confirmate-Tools.

Der Ansatz basiert auf einer anerkannten Methodik (OSSTMM3), die in einer offenen Community entwickelt und einer Peer- und interdisziplinären Überprüfung unterzogen wurde. OSSTMM3 bietet einen strukturierten Ansatz zur Identifizierung von Schwachstellen und deren Zuordnung zu möglichen Cyberangriffen, wodurch eine genauere Bewertung potenzieller Sicherheitsrisiken ermöglicht wird.

Die Ziele des vorgeschlagenen Ansatzes sind wie folgt:

- Bereitstellung einer strukturierten Methode für Penetrationstests von Produkten mit digitalen Elementen bei gleichzeitiger Flexibilität hinsichtlich der verwendeten Techniken.
- Definition eines Standardsatzes von Ergebnissen, die zur Untermauerung der Konformitätserklärung des Herstellers gegenüber der CRA verwendet werden können.
- Veranschaulichung der Anwendung des Ansatzes durch Erläuterung, wie er auf mehrere Produkte aus den von der CRA definierten Kategorien „wichtige Produkte" (Klasse I und Klasse II) und „kritische Produkte" angewendet werden kann.
- Diese Methodik deckt keine generischen IT-Bewertungen von Unternehmen oder eigenständige Penetrationstests von Webanwendungen ab, die keine PDE im Sinne der CRA darstellen. Web-o- und OWASP-Methodiken decken häufig nur webbasierte Assets ab, die nicht mit dem hier erforderlichen produktzentrierten Regulierungsumfang übereinstimmen.

3.2 Zielgruppe

Die Zielgruppe dieses Dokuments sind Hersteller von Produkten mit digitalen Elementen gemäß der Definition der CRA.

4. Umfang

4.1 Anwendbarkeit auf KMU

Der in diesem Dokument vorgeschlagene Ansatz für Penetrationstests wurde für kleine und mittlere Unternehmen (KMU) entwickelt. Dabei wurde besonders darauf geachtet, den Ansatz einfach und verständlich zu halten und unnötige Fachbegriffe zu vermeiden, damit die vorgeschlagenen Methoden auch für kleinere Unternehmen zugänglich sind.

Diese Methodik ist sowohl auf eigenständige als auch auf eingebettete digitale Produkte im Geltungsbereich der CRA anwendbar, einschließlich Verbrauchergeräte, industrielle Steuerungen, intelligente Gateways und sicherheitskritische Komponenten. Sie wurde in erster Linie für Tests vor der Markteinführung und während des Betriebs entwickelt, kann jedoch auch in früheren Entwicklungsphasen eingesetzt werden, um Sicherheitslücken vor der Markteinführung zu identifizieren.

4.2 Grenzen und Einschränkungen

Dieses Dokument beschreibt, wie Penetrationstests mit dem Ziel durchgeführt und verwaltet werden, die Einhaltung der CRA-Anforderungen nachzuweisen. Es behandelt keine Strategien zur Behebung von Schwachstellen, Kontrollmaßnahmen zur Risikominderung oder korrigierende Sicherheitsmaßnahmen, die nach der Aufdeckung von Schwachstellen während der Tests erforderlich sein können.

Im Gegensatz zu klassischen Penetrationstests, die auf eine Umgebung abzielen, beziehen sich die in diesem Dokument beschriebenen Tests auf ein Produkt. Dies ist jedoch nur sinnvoll, wenn das Produkt in einer geeigneten Umgebung untergebracht ist. In diesem Sinne spielt die Umgebung, in der ein Produkt während der Tests gehostet wird, eine Rolle bei der Bestimmung der Gültigkeit der Endergebnisse. Penetrationstests finden in diesem Zusammenhang in der Regel in einer kontrollierten Laborumgebung statt. Das Testteam sollte die Testumgebung entweder bereitstellen oder genehmigen und sicherstellen, dass sie realistische Betriebsbedingungen widerspiegelt, ohne die Sicherheitsannahmen zu schwächen.

4.3 Annahmen und Einschränkungen

Die wichtigsten Annahmen, die bei dem vorgestellten Ansatz getroffen wurden, lauten wie folgt:

- Das Produkt wird in einer „Laborumgebung“ getestet und nicht unter realen Bedingungen.
- Die Umgebung, in der das Produkt getestet wird, entspricht weitgehend der Zielumgebung (d. h. der Umgebung, in der das Produkt betrieben wird).

Obwohl in diesem Ansatz Beispiel-Testszenarien vorgeschlagen werden, wird davon ausgegangen, dass die Hersteller diese Szenarien an die Eigenschaften des zu testenden Produkts anpassen werden.

Einschränkungen des Prozesses werden im Rahmen der Aktivitäten der Phase 1 ermittelt. Die wichtigste Einschränkung besteht darin, dass die Tests so konzipiert sein müssen, dass sie keine negativen Auswirkungen auf den Betrieb der Prüfstelle haben.

5. Industriestandards für Tests

5.1 ETSI EN 303 645

Die Norm wird begleitet von einer Prüfspezifikation (TS 103 701) und einem Leitfaden zur Umsetzung (TR 103 621) https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf.

ETSI TS 103 701 enthält strukturierte Testgruppen und Konformitätsbewertungen, die auf IoT-Geräte für Verbraucher zugeschnitten sind. Die Testfälle umfassen Anforderungen an Funktionalität, Ausfallsicherheit, Schnittstellen und Datenschutz. Bei dieser Methodik werden relevante Testgruppen aus TS 103 701 selektiv auf die in Anhang A aufgeführten Produktkategorien angewendet.

ETSI EN 303 645 ist die grundlegende europäische Cybersicherheits-Norm für Verbrauchergeräte im Internet der Dinge (IoT). Sie enthält Bestimmungen zur Bekämpfung der häufigsten und folgenschwersten Angriffsvektoren. Die Norm soll eine Mindestsicherheitsbasis gewährleisten und als Referenz für nationale Vorschriften und Konformitätsbewertungen dienen.

5.2 OSSTMM3

Ein OSSTMM-Audit ist eine genaue Messung der Sicherheit auf operativer Ebene, die frei von Annahmen und anekdotischen Beweisen ist. Als Methodik ist sie so konzipiert, dass sie konsistent und wiederholbar ist. Als Open-Source-Projekt ermöglicht es jedem Sicherheitstester, Ideen für genauere, umsetzbare und effizientere Sicherheitstests einzubringen. Darüber hinaus ermöglicht es die freie Verbreitung von Informationen und geistigem Eigentum.

Im Vergleich zu compliance-basierten Standards konzentriert sich OSSTMM 3 auf die Validierung der realen Sicherheit in mehreren Bereichen, darunter:

- **Datennetzwerke**: Router, Firewalls, SIEM, intelligente Zähler und IoT-Geräte.
- **Telekommunikation**: Fernzugriffssicherheit, VPN-Konfigurationen.
- **Drahtlose Sicherheit**: Wi-Fi-Schwachstellen, Verschlüsselungsstandards.

Außerdem wurden Risikobewertungswerte (RAVs) eingeführt, mit denen Sicherheitsteams Sicherheitsrisiken quantifizieren und Schwachstellen im Laufe der Zeit verfolgen können, wodurch das Risikomanagement und die Entscheidungsfindung verbessert werden.

5.3 OWASP Testleitfaden

Der OWASP-Testleitfaden wurde im Rahmen des OWASP-Testprojekts des Open Web Application Security Project (OWASP) entwickelt. Er ist keine vollständige Methodik für einen umfassenden Penetrationstest, sondern konzentriert sich ausschließlich auf die Kernphasen der Sicherheitstests für Webanwendungen.

Der Leitfaden enthält eine detaillierte Erörterung der Sicherheitsbewertung von Webanwendungen sowie ihres Bereitstellungsstacks, einschließlich der Webserverkonfiguration. Er folgt einem Black-Box-Pentesting-Ansatz und behandelt umfassend die Fragen „Was?“ und „Wann?“. Es gibt auch einige Leitfäden zum „Wie“, hauptsächlich in Form einer Auflistung der Tools, die in den einzelnen Schritten oder Aufgaben verwendet werden können.

5.4 PTES

Der Penetration Testing Execution Standard (PTES) ist die bislang aktuellste Methodik für Penetrationstests. Er wurde von einem Team aus Fachleuten für Informationssicherheit entwickelt, um den Bedarf an einem umfassenden und aktuellen Standard für Penetrationstests zu decken.

Er dient nicht nur als Leitfaden für Sicherheitsexperten, sondern soll auch Unternehmen darüber informieren, was sie von einem Penetrationstest erwarten können, und ihnen dabei helfen, den Umfang erfolgreicher Projekte zu definieren und zu verhandeln. Er behandelt nicht nur das „Was” und „Wann”, sondern geht auch viel tiefer auf das „Wie” ein.

Der PTES besteht aus zwei sich ergänzenden Teilen. Die Pentest-Richtlinien beschreiben die wichtigsten Abschnitte und Schritte eines Penetrationstests, während die technischen Richtlinien die spezifischen Tools und Techniken behandeln, die in den einzelnen Schritten zum Einsatz kommen.

5.5 NIST SP 800-15

NIST 800-115 mit dem Titel „Technical Guide to Information Security Testing and Assessment” (Technischer Leitfaden für die Prüfung und Bewertung der Informationssicherheit) ist eine Veröffentlichung, die Leitlinien und Empfehlungen für die Durchführung von Informationssicherheitsbewertungen zur Beurteilung der Sicherheitslage von Informationssystemen und Netzwerken enthält.

Sie soll Organisationen dabei unterstützen, die verschiedenen Arten von Sicherheitsbewertungen zu verstehen, die geeigneten Bewertungstechniken auszuwählen und umfassende Bewertungsprogramme zu entwerfen. Die Leitlinien können auf verschiedene Organisationen angewendet werden, darunter Bundesbehörden, Organisationen des privaten Sektors und Bildungseinrichtungen.

Weitere Einzelheiten zu gängigen Pentesting-Methoden und deren Vergleich finden Sie in Anhang D: Vergleich der Methoden. Darüber hinaus sind in Anhang E gängige Sicherheitsrichtlinien und bewährte Verfahren aufgeführt.

6. Führende Methodik

Das Open Source Security Testing Methodology Manual (OSSTMM 3) ist die führende Methodik, die bei diesem Penetrationstestansatz verwendet wird. Es bietet eine Methodik für einen gründlichen Sicherheitstest, der hier als OSSTMM-Audit bezeichnet wird.

Während OSSTMM 3 die primäre Methodik ist, integriert dieses Penetrationstest-Framework auch Elemente aus:

- **ETSI TS 103 701 –** Relevante Testfälle aus diesem Konformitätsteststandard werden in unseren Testdurchführungsprozess integriert, insbesondere für IoT und Verbraucher-PDEs.
- **OWASP Testing Guide** – Wir haben die Testfälle von OWASP in die Erkundungs- und Ausnutzungsphasen für Webanwendungen und APIs integriert. Dabei werden die OWASP-Richtlinien befolgt, um Schwachstellen wie SQL-Injection, Cross-Site-Scripting und unsichere Sitzungsverwaltung zu identifizieren.
- **PTES** (Penetration Testing Execution Standard) – PTES definiert einen strukturierten Lebenszyklus für Aufträge, den wir in unsere Methodik integriert haben. Um sicherzustellen, dass jede Phase klare Ziele, Ergebnisse und Kommunikationsprotokolle hat, haben wir die OSSTMM3-Phasen an PTES angepasst, was zu einem konsistenten und wiederholbaren Testprozess führt.

NIST SP 800-115 – NIST SP 800-115 bietet einen soliden Rahmen für risikobasierte Sicherheitstests. Die Phasen der Ausnutzung und der Folgenanalyse wurden an die Richtlinien angepasst, um eine systematische Identifizierung von Schwachstellen, eine umfassende Risikobewertung und eine detaillierte Berichterstattung zu gewährleisten.

7. Vorbereitung auf ein Pentesting

Warum testen? Die CRA verlangt von PDE, „wirksame und regelmäßige Tests und Überprüfungen der Sicherheit des Produkts mit digitalen Elementen durchzuführen“ (Anhang I, Teil II, Punkt 3). Die Planung regelmäßiger Sicherheitsbewertungen gewährleistet eine kontinuierliche Überwachung und proaktive Identifizierung von Schwachstellen, wodurch die Widerstandsfähigkeit gegenüber neuen Bedrohungen aufrechterhalten wird.

Wer führt die Tests durch? Im Rahmen von CRA-konformen Bewertungen hat die Wahl eines Penetrationstesters (oder Anbieters) direkten Einfluss auf die Zuverlässigkeit, Reproduzierbarkeit und regulatorische Relevanz der Ergebnisse. KMU können Pentester auswählen, die Folgendes nachweisen können:

- *Technische Kompetenz*: Nachgewiesene Fachkenntnisse in den Bereichen Produktsicherheit, eingebettete Systeme, Firmware-Tests und Analyse von Software-Schwachstellen. Anbieter müssen die Unterschiede zwischen Produkttests und traditionellen Bewertungen von Unternehmensumgebungen verstehen.
- *CRA-Kenntnisse*: Nachgewiesene Kenntnisse des Cyber Resilience Act, einschließlich der Anforderungen in Anhang I Teil I und II, sowie die Fähigkeit, Ergebnisse zu liefern, die CRA-Konformitätserklärungen unterstützen.
- *Branchenspezifische Erfahrung*: Wählen Sie gegebenenfalls Anbieter mit Erfahrung im Produktbereich.
- *Rechtliche und ethische Sicherheit*: Vergewissern Sie sich, dass die Tester klare ethische Richtlinien befolgen, Versicherungsschutz bieten und gut abgestimmte Verträge abschließen, die Haftungs- und Datenschutzklauseln enthalten.
- *Zertifizierungen und Akkreditierungen*: Zertifizierungen wie OSCP, OSCE, CREST oder gleichwertige nationale Qualifikationen auf europäischer Ebene sind hilfreich. Für risikoreiche oder kritische Produkte sollten Sie TIBER-EU- oder Red-Team-Zertifizierungen in Betracht ziehen.

Wie lange dauert es? Die Zeitpläne können je nach Produktkomplexität, Wissensstand (Black/Grey/White Box) und CRA-Klassifizierung (Standard, wichtig oder kritisch) variieren, aber eine allgemeine Schätzung der für jede Phase benötigten Zeit lässt sich wie folgt zusammenfassen:

1. Vorbereitung (5–10 Werktage, *Zusammenarbeit zwischen Tester und Hersteller*), einschließlich:

- Festlegung des Umfangs, der Ziele und der Testgrenzen
- CRA-Anhang-I-Anforderungsabgleich
- Rechtliche Vereinbarungen und Abstimmung mit den Beteiligten
- Bereitstellung der technischen Dokumentation durch den Kunden

2. Durchführung der Tests und Berichterstattung (3–10 Werktage, *unter der Leitung des Testers*), einschließlich:

- Informationsbeschaffung, Auswertung und Folgenanalyse
- Testen der Produktfirmware, Schnittstellen, APIs und Sicherheitskontrollen
- Erstellung von Berichten und Kommunikation

3. Behebung (1–4 Wochen, *unter Federführung des Herstellers*)

- Entwicklung von Patches, Konfigurationskorrekturen, interne Qualitätssicherung
- Optionale Risikoakzeptanz und Aktualisierung der Dokumentation

4. Erneute Tests (1–2 Werktage, *in Zusammenarbeit zwischen Tester und Hersteller*)

- Erneute Validierung der behobenen Probleme
- Abschließende technische Bestätigungen und Sammlung von Nachweisen

8. Methodik für Penetrationstests

8.1 Vorbereitung und Planung

Der erste Schritt besteht darin, unter Berücksichtigung der Produktreife, der für das Produkt identifizierten Sicherheitsrisiken (intern/extern), der verfügbaren Dokumentation und der möglichen Angriffsvektoren (wie ein Produkt ausgenutzt werden kann) zu definieren, welche Art von Test am besten geeignet ist. Der Test könnte wie folgt aussehen:

- **Black-Box**: Die Tester verfügen über keine internen Kenntnisse und simulieren einen externen Angreifer.
- **Grey-Box**: Die Tester verfügen über Teilkenntnisse. Oftmals mit teilweisem Zugriff.
- **White-Box**: Vollständige interne Kenntnisse (Quellcode, Architektur); ermöglicht tiefgehende Tests.

Beachten Sie, dass Labortests teilweise oder vollständige Kenntnisse (White-Box) voraussetzen.

Eingaben:

- *Produktidentifikation*. Für White- und Grey-Box-Tests: Technische Dokumentation ist erforderlich, einschließlich: Anwendungsfälle, Architekturdiagramme, Firmware-/Softwareversion, Liste der Schnittstellen – intern und extern (z. B. USB, BLE, APIs, Web-UI, Ports, Protokolle) oder alle bekannten Assets/Komponenten, die für die Tests relevant sind, Bedrohungsmodell (falls verfügbar). Darüber hinaus können Details zu früheren Bewertungen oder Audits (sofern verfügbar), einschließlich offener Bug-Tickets oder ungelöster Testergebnisse, hilfreich sein.
- Branchenrahmenwerke (z. B. OSSTMM3, PTES, NIST SP 800-115, OWASP)
- Regulatorische Anforderungen und Compliance-Dokumentation, einschließlich der Anforderungen von CRA Anhang I, Teil I und II (siehe Anhang B: CRA-Anforderungen)
- Ansprechpartner und Notfallprotokolle, einschließlich eines Notfallverfahrens (Vorgehensweise bei unerwarteten Ereignissen, z. B. Dienstunterbrechungen) während der Tests.
- Vertragliche Dokumentation (bei Einsatz externer Tester): Dienstleistungsverträge, NDAs, Testgenehmigungen und Haftungsausschlüsse.

Aktivitäten:

- *Definition der Ziele und Festlegung des Umfangs*: Diese Phase beginnt mit der klaren Definition der Ziele und des Umfangs. Der Schwerpunkt liegt darauf, sicherzustellen, dass jedes System auf seine spezifischen Funktionen getestet wird. Die Festlegung des Umfangs ist entscheidend für die Ausrichtung der Penetrationstests auf die Ziele der CRA und die besonderen Eigenschaften des zu testenden Produkts. Die Festlegung des Umfangs umfasst:
    - *Definition der Produktgrenzen*: Definieren Sie den technischen Umfang (Software, Hardware, APIs, Schnittstellen) des Produkts mit digitalen Elementen (PDE).
    - *CRA-Zuordnung*: Identifizieren Sie anhand der Risikoklasse des Produkts, welche Anforderungen aus Anhang I der CRA gelten.
    - *Eingaben für die Bedrohungsmodellierung*: Berücksichtigung bekannter Bedrohungsakteure, Angriffsflächen und des Produktkontexts.
- *Testtiefe: Die Tiefe der Penetrationstests entspricht der Kritikalitätsklassifizierung des Produkts gemäß dem Cyber Resilience Act (CRA).*
    - *Standard- und wichtige Klasse-I-Produkttests* konzentrieren sich in der Regel auf extern exponierte Dienste und Schnittstellen, Zugriffskontrollmechanismen, den Schutz von Daten während der Übertragung und die Identifizierung bekannter Schwachstellen.
    - *Ein wichtiges Produkt der Klasse II* erfordert eine gründlichere Überprüfung der Firmware, der Aktualisierungsmechanismen, der Kommunikation zwischen Gerät und Cloud, der Authentifizierungsabläufe und der Szenarien für den Missbrauch von Protokollen.
    - *Kritische Produkttests* umfassen Sicherheitsüberprüfungen auf Hardware-Ebene, wie z. B. Manipulationserkennung, Fehlerinjektionsresistenz und Überprüfung des sicheren Startvorgangs.
- *Rechtliche, regulatorische und ethische Überlegungen*: Die Tests werden unter Einhaltung der gesetzlichen und regulatorischen Anforderungen (z. B. Datenschutz, IP-Gesetze) und interner Richtlinien durchgeführt. Alle erforderlichen Genehmigungen werden eingeholt und Einschränkungen dokumentiert, damit die Testumgebung keinen Einfluss auf den Produktionsbetrieb hat. (Siehe Anhang B: CRA-Anforderungen, CRA-Anhang I, Teil I, Punkte 1, 2(b), 2(g), 2(j) und Anhang I, Teil II, Punkt 1.)
- *Einrichtung eines Testlabors*, das die Betriebsumgebung des PDE nachbildet.

Ergebnisse für nachfolgende Phasen:

- Methodikdokument auf hoher Ebene
- Formulare für rechtliche Genehmigungen

- Definition des Umfangs
- Richtlinien für die Zusammenarbeit
- Bericht zur Produktrisikobewertung
- Briefing für die Beteiligten

Endgültige Ergebnisse:

- Planungs- und Anforderungsdokument (D1): Ein detaillierter Plan für das Penetrationstest-Projekt mit einer Beschreibung des Umfangs, der Rollen, der Ziele, der Genehmigungen, des Zeitplans und der Einrichtung des Labors.
- Risikobewertung vor dem Test und Abstimmung mit den Beteiligten (D2): Vor Beginn der Tests muss eine produktspezifische Risikobewertung durchgeführt werden, um potenzielle Risiken zu identifizieren, die der Penetrationstest für die Funktionalität, Datenintegrität oder Verfügbarkeit des Produkts darstellen könnte. Dazu gehört auch die Bewertung, wie sich der Test auf kritische Schnittstellen, Dienste und Daten auswirken könnte, die vom Produkt verarbeitet werden. Die Stakeholder werden informiert, und der Pentesting-Plan muss mit ihren Sicherheitsanforderungen (einschließlich Anhang B: CRA-Anforderungen, CRA-Anhang I, Teil I) und ihrer Risikotoleranz abgestimmt werden.

8.2 Informationsbeschaffung und Aufklärung

Eingaben:

- Umfangsdefinition
- Produkt-Risikobewertungsbericht

Aktivitäten:

- Open-Source-Intelligence und Asset Discovery: In dieser Phase werden Open-Source-Informationen genutzt, um möglichst umfassende Informationen zu sammeln. Dazu gehört auch die Erfassung der digitalen Spuren jedes Produkts und Elements.
- Ziel-Profiling und Analyse der Bedrohungslage: Für jedes Asset ist eine Analyse erforderlich, um potenzielle Schwachstellen zu ermitteln. Außerdem wird die Bedrohungslage überprüft, um sicherzustellen, dass für das Pentesting

realistische Szenarien verwendet werden und die Taktiken der Angreifer in den simulierten Angriffen während des Tests berücksichtigt werden.
- Szenarioentwicklung auf der Grundlage des Verhaltens der Angreifer: Aus den gesammelten Informationen und Daten werden spezifische Angriffsszenarien formuliert.

Ergebnisse für nachfolgende Phasen:

- Szenarien zum Verhalten der Angreifer und Zielprofile
- Erste Version des Schwachstellenberichts (D3): Detaillierte Ergebnisse der externen und internen Bewertungen des Produkts, einschließlich Risikobewertungen, Eintrittswahrscheinlichkeit und Abhilfevorschläge, die einen umfassenden Überblick über die Schwachstellen des Produkts selbst bieten.

Endgültige Ergebnisse:

- In dieser Phase werden keine Ergebnisse finalisiert.

8.3 Testdurchführung und Auswertung

Eingaben:

- Erste Version des Schwachstellenberichts (D3): Detaillierte Ergebnisse aus externen und internen Bewertungen des Produkts, einschließlich Risikobewertungen, Ausnutzbarkeit und Abhilfevorschläge, die einen umfassenden Überblick über die Schwachstellen des Produkts selbst bieten.
- Szenarien für das Verhalten von Angreifern und Zielprofile
- Testtools (z. B. Nessus, Metasploit, Wireshark). Beispiele für Testtools und Frameworks sind in Anhang E aufgeführt.
- (falls verfügbar) Software-Quellcode.

Aktivitäten:

- Identifizierung von Schwachstellen und Angriffssimulation: Schwachstellen werden mithilfe von Techniken wie statischer (SAST) und dynamischer Anwendungssicherheitsanalyse (DAST) oder manueller Codeüberprüfung identifiziert, sofern zutreffend. KI-gesteuerte Bedrohungsinformationen können

zur Verbesserung der Effizienz bei der Erkennung von Schwachstellen verwendet werden. Jedes Produkt wird gemäß festgelegten Standards getestet. Die Aktivitäten zur Schwachstellenbewertung werden während der gesamten Testdurchführung iterativ durchgeführt und fließen direkt in die Erstellung des Schwachstellenberichts D4 ein und dienen als primäre Grundlage für die spätere Risikobewertung. Ausgewählte Testszenarien, die aus ETSI TS 103701 stammen, sind in Anhang C aufgeführt, da sie als Teil des Pentestings durchgeführt werden könnten, das zusätzlich zur Sicherheit die Konformität mit der CRA in Abstimmung testet. Die Aktivitäten in dieser Phase validieren auch die CRA-konformen Anforderungen an ein sicheres Design und den Schutz. Siehe Anhang B: CRA Anhang I, Teil I, Punkte 2(a), 2(b), 2(d), 2(e), 2(j), 2(k) und Anhang I, Teil II, Punkt 3.

- Ausnutzungstechniken und Emulation von Angreifern: Validierung von Schwachstellen durch den Versuch, diese in einer kontrollierten Umgebung auszunutzen. Wenn entsprechende Tools verfügbar sind, kann ein KI-gestütztes Scanning eingesetzt werden. KMU, die nicht über solche Tools verfügen, können auf manuelle Überprüfungen oder einfachere Automatisierungslösungen zurückgreifen. Beispiele hierfür sind die Erkennung von Anomalien in Protokollen oder maschinelles Lernen-basiertes Fuzzing. Außerdem wird bewertet, in welchen Situationen Angreifer Sicherheitsvorkehrungen umgehen und sich unbefugten Zugriff verschaffen könnten.
- Analyse nach dem Eintritt: Bewertung der Auswirkungen eines erfolgreichen Angriffs, einschließlich der Ausweitung von Berechtigungen im gesamten System und der potenziellen seitlichen Bewegung zu anderen Benutzern, Komponenten oder verbundenen Systemen. Dazu gehört auch die Feststellung, ob ein Angreifer auf sensible Daten zugreifen, zwischen Anwendungsmodulen oder Infrastruktursegmenten wechseln oder kritische Dienste kompromittieren kann. Details zu den funktionalen Auswirkungen werden durch die Analyse der potenziellen Folgen jeder ausgenutzten Schwachstelle erfasst.
- Die Ergebnisse der Testfälle werden in die Endergebnisse dieser Phase eingebettet, um die Rückverfolgbarkeit der Testaktivitäten gegenüber den erwarteten Verhaltensweisen zu gewährleisten.

Ergebnisse für nachfolgende Phasen:

- Liste der Schwachstellen
- Nachweis der Eintrittswahrscheinlichkeit(Proof-of-Concept)
- Vorläufige Risikobewertungen
- Bericht zur Eintrittswahrscheinlichkeit
- Bericht zur Simulation von Angreifer-Taktiken

Endergebnisse:

- Schwachstellenbericht (D3): Detaillierte Ergebnisse aus externen und internen Bewertungen des Produkts, einschließlich Risikobewertungen, Eintrittswahrscheinlichkeit und Abhilfevorschläge, die einen umfassenden Überblick über die Schwachstellen des Produkts selbst bieten.

8.4 Auswirkungsanalyse und Berichterstattung

Eingaben:

- Liste der Schwachstellen
- Nachweis der Ausnutzung (Proof-of-Concept)
- Vorläufige Risikobewertungen
- Branchenspezifische Standards für die Risikobewertung
- Richtlinien zur Datenklassifizierung.

Aktivitäten:

- Risikobewertung und Bewertung der funktionalen Auswirkungen: Analyse der Schwere der identifizierten Schwachstellen, Messung ihrer Auswirkungen auf CIA (Vertraulichkeit, Integrität oder Verfügbarkeit). Zuweisung einer Risikobewertung zur Priorisierung der Abhilfemaßnahmen. Darüber hinaus können KI-basierte Risikobewertungsmodelle eingesetzt werden, um die Gesamtbewertungsphase zu verbessern, indem Risikostufen auf der Grundlage von Echtzeit-Bedrohungsinformationen und Daten zur Ausnutzbarkeit zugewiesen werden. Dies umfasst eine CRA-konforme Bewertung der Datenintegrität, der Widerstandsfähigkeit und der Reaktion auf Schwachstellen. Siehe Anhang B: CRA Anhang I, Teil I, Punkte 2(e), 2(f), 2(i); Anhang I, Teil II, Punkte 1, 2.
- Dokumentation der Ergebnisse und Sammlung von Beweisen: Erstellung ausführlicher Berichte mit Beschreibungen der Schwachstellen, technischen Nachweisen und Beweisen für die Ausnutzung. Sicherstellung, dass alle Beteiligten ein klares Verständnis der Sicherheitslücken haben.
- Kennzeichnung der Einhaltung gesetzlicher Vorschriften: Übersetzung der Testergebnisse in Begriffe zur Einhaltung gesetzlicher Vorschriften durch Kennzeichnung der Ergebnisse, die mit den in Anhang B aufgeführten Anforderungen von CRA Anhang I und II in Zusammenhang stehen. Auf diese

Weise wird ein Beitrag zu einem Bericht über die Einhaltung gesetzlicher Vorschriften geleistet, der zur Begründung der Konformitätserklärung eines Herstellers herangezogen werden kann.
- Empfehlungen und umsetzbare Strategien zur Behebung: Bereitstellung detaillierter Anleitungen zur Minderung der identifizierten Risiken. Vorschläge für Sicherheitskontrollen, Konfigurationsänderungen und Patch-Strategien, um das System widerstandsfähiger zu machen (siehe Anhang B: CRA-Anforderungen).

Ergebnisse für nachfolgende Phasen:

- Risikobewertungsbericht
- Umfassendes Dokument mit den Ergebnissen
- Details zu den funktionalen Auswirkungen
- Empfehlungen zur Behebung
- Priorisierter Plan zur Behebung
- Bericht zur Angleichung der Einhaltung gesetzlicher Vorschriften

Endgültige Ergebnisse:

- Empfehlungen und Roadmap zur Behebung (D5): Priorisierte Empfehlungen mit einer klaren Roadmap zur Behebung, einschließlich kurz-, mittel- und langfristiger Maßnahmen.

8.5 Nachbereitung nach der Beauftragung

Eingaben:

- Berichte über Abhilfemaßnahmen
- Aktualisierte Systemkonfigurationen und Ergebnisse der erneuten Tests.

Aktivitäten:

- Überprüfung der Abhilfemaßnahmen und erneute Tests: Führen Sie erneute Tests durch, um zu überprüfen, ob die Sicherheitsmängel behoben wurden. Stellen Sie sicher, dass die Abhilfemaßnahmen die Schwachstellen wirksam beseitigen. Nach den Tests wird überprüft, ob die Sicherheitsupdates und die Offenlegung den Erwartungen der CRA entsprechen. Siehe Anhang B: CRA-Anhang I, Teil I, Punkte 2(h), 2(m) und Anhang I, Teil II, Punkte 2, 4, 7, 8.
- Kontinuierliche Verbesserung und Integration der gewonnenen Erkenntnisse: Aktualisierung der Testmethoden und Sicherheitsrichtlinien auf der Grundlage der Ergebnisse. KI-gestützte Analysen tragen dazu bei, zukünftige

Sicherheitsbewertungen zu verbessern, indem sie die aus früheren Tests gewonnenen Erkenntnisse nutzen. (siehe: Anhang: CRA-Anforderungen, CRA-Anhang I, Teil I)

- Offenlegung und Kommunikation von Schwachstellen: Nach der Verfügbarkeit von Sicherheitsupdates müssen Hersteller Details zu behobenen Schwachstellen vorbereiten und öffentlich bekannt geben. In Fällen, in denen eine Offenlegung ein unangemessenes Risiko darstellen würde, kann die Veröffentlichung bis zur flächendeckenden Bereitstellung von Patches gerechtfertigt verzögert werden (CRA-Anhang I, Teil II, Punkt 4).

Endgültige Ergebnisse:

- Pentesting-Bericht (D5): Ein typischer Pentesting-Bericht umfasst eine Zusammenfassung (allgemeiner Überblick, Gesamtrisikobewertung, Testergebnisse und Prioritätsempfehlungen), den Testumfang und die Testmethode (D1), die durchgeführten Aktivitäten, die Ergebnisse (mit weiteren Details, einschließlich Schwachstellen (D2) und Nachweisen für deren Ausnutzung) sowie Empfehlungen (D4). Dieses Dokument könnte als „Überprüfung der Sicherheit des Produkts mit digitalen Elementen“ im Sinne der CRA-Anforderung in Anhang I Teil II Punkt 3 (Durchführung wirksamer und regelmäßiger Tests und Überprüfungen der Sicherheit des Produkts mit digitalen Elementen) angesehen werden.

8.6 Ergebnisse

Jeder Auftrag führt zu umfassenden Ergebnissen, die sowohl technische als auch strategische Anforderungen erfüllen. In jeder Phase der Methodik gibt es zwei Arten von Ergebnissen: (a) Ergebnisse, die als Input für eine nachfolgende Phase dienen, und (b) Ergebnisse der gesamten Übung. Die Ergebnisse der gesamten Übung sind nachstehend aufgeführt:

- Planungs- und Anforderungsdokument (D1): Ein detaillierter Pentesting-Projektplan mit einer Beschreibung der Ziele, des Umfangs, der Rollen, der Notfallmaßnahmen, der Genehmigungen, des Zeitplans und der Laborausstattung.
- Risikobewertung vor dem Test und Abstimmung mit den Stakeholdern (D2): Eine gründliche Analyse der potenziellen Risiken vor Beginn des Tests, um sicherzustellen, dass alle Stakeholder hinsichtlich des Umfangs, der Prioritäten und der Ziele aufeinander abgestimmt sind.

- Schwachstellenbericht (D3): Detaillierte Ergebnisse aus externen und internen Bewertungen des Produkts, einschließlich Risikobewertungen, Ausnutzbarkeit und Abhilfevorschläge, die einen umfassenden Überblick über die Schwachstellen des Produkts selbst geben.
- Empfehlungen und Roadmap für Abhilfemaßnahmen (D4): Priorisierte Empfehlungen mit einer klaren Roadmap für Abhilfemaßnahmen, einschließlich kurz-, mittel- und langfristiger Maßnahmen.
- Penetrationstestbericht (D5): Eine allgemeine Übersicht für nicht-technische Stakeholder, in der die wichtigsten Ergebnisse und strategischen Empfehlungen zusammengefasst sind.

8.7 Beispielszenarien

Der Zweck dieses Abschnitts besteht darin, anschauliche Beispiele für Penetrationstest-Szenarien einschließlich der ungefähren Ressourcenanforderungen und des voraussichtlichen Zeitaufwands zu liefern. Diese Szenarien dienen lediglich als Anhaltspunkte und können von Übung zu Übung erheblich variieren.

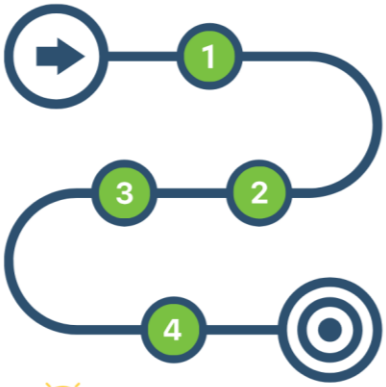
Szenario 1: Identitäts- und Zugriffsmanagement (wichtiges Produkt von CRA: Klasse I)

Testansatz

- **Testtyp:** Grey Box (Es wurden grundlegende Anmeldeinformationen bereitgestellt. Der Pentester muss interne IAM-Funktionen und -Berechtigungen aufzählen).
- **Komplexität:** Mittel (5–15 IAM-Funktionen/Module).
- **Aufwandsschätzung:** 8–12 Arbeitstage (~15–20 Tage vergangen).

Ergebnisse und Auswirkungen

- Durch unsachgemäße Sitzungsverarbeitung wurden Sitzungstoken für nicht autorisierte Benutzer preisgegeben.
- Die Fallback-MFA-Logik ermöglichte die Umgehung mithilfe sozialer Wiederherstellungsmethoden.
- IAM-Protokolle haben keine Rechteausweitung durch Rollenmanipulation angezeigt.



Angriffspfad

1. **Aufklärung:** Aufzählen von IAM-Anmeldeendpunkten, MFA-Mechanismen und Sitzungsverwaltungslogik.
2. **Ausnutzung von Sicherheitslücken:** Umgehen Sie die Fallback-MFA über Social Recovery. Kapern Sie die Administratorsitzung durch Token-Harvesting.
3. **Auswirkungsanalyse und -berichterstattung:** Identifizieren Sie das Risiko eines unbefugten Zugriffs auf das Admin-Portal und interne Konfigurationen.
4. **Folgemaßnahme:** Patchen Sie die MFA-Fallback-Logik und konfigurieren Sie die Sitzungsverwaltung neu.

Empfehlungen

- Implementieren Sie sichere Sitzungstoken mit den Attributen HttpOnly, Secure und SameSite.
- Erzwingen Sie strenge Multi-Faktor-Authentifizierungsabläufe ohne nicht verifizierten Fallback.
- Aktivieren Sie die Protokollierung und Warnmeldung bei Versuchen zur Rechteerweiterung und Rollenänderungen.

Auswirkungen der CRA-Compliance

Unsicherer MFA-Fallback verstößt gegen CRA Anhang I, Teil I, Punkt 2(d): "Sorgen Sie durch geeignete Kontrollmechanismen für Schutz vor unbefugtem Zugriff."

Das Fehlen einer Protokollierung der Rechteerweiterung verstößt gegen CRA Anhang I, Teil I, Punkt 2(l): "Stellen Sie sicherheitsrelevante Informationen bereit, indem Sie relevante interne Aktivitäten aufzeichnen und überwachen."

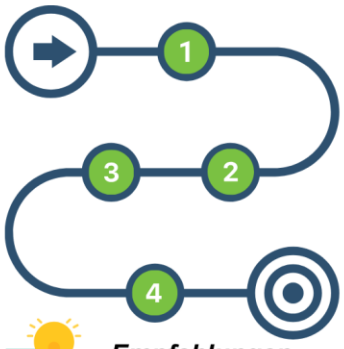
Szenario 2: Sicherheitsinformations- und Ereignismanagement (SIEM) (Wichtiges Produkt von CRA: Klasse II)

Testansatz

Testtyp: Grey Box (SIEM-Anmeldeinformationen bereitgestellt; Pentester simuliert gegnerische Eingaben und Protokollmanipulationen).
Komplexität: Hoch (15–30 Protokollquellen, Regelsätze und Integrationen).
Aufwandsschätzung: 12–15 Arbeitstage (~20–25 Tage vergangen).

Ergebnisse und Auswirkungen

- *SIEM konnte bei wiederholten fehlgeschlagenen Anmeldeversuchen keine Warnungen auslösen.*
- *Durch die Syslog-Injektion konnten Einbruchsprotokolle ausgeblendet werden.*
- *Durch Payload-Evasion könnten Protokollintegritätsprüfungen umgangen werden.*



Empfehlungen

- *Konfigurieren Sie Regeln zur Anomalieerkennung für authentifizierungsbasierte Schwellenwerte.*
- *Bereinigen Sie die Protokolleingaben, um eine Protokolleinschleusung zu verhindern.*
- *Verwenden Sie kryptografische Protokollsignaturen und -validierungen, um die Integrität sicherzustellen.*

Angriffspfad

1. **Aufklärung:** Überprüfen Sie SIEM-Aufnahmepunkte, Korrelationsregeln und Warnschwellenwerte.
2. **Ausnutzung von Sicherheitslücken:** Einfügen manipulierter Protokolle, um echte Angriffe zu verbergen. Ausnutzung fehlender Ereigniskorrelation bei fehlgeschlagenen Anmeldungen.
3. **Auswirkungsanalyse und -berichterstattung:** Bewerten Sie, wie die Unterdrückung von Warnungen dauerhaften Zugriff ermöglicht.
4. **Folgemaßnahme:** Verschärfen Sie die Analyselogik und prüfen Sie Regelsätze.

Auswirkungen der CRA-Compliance

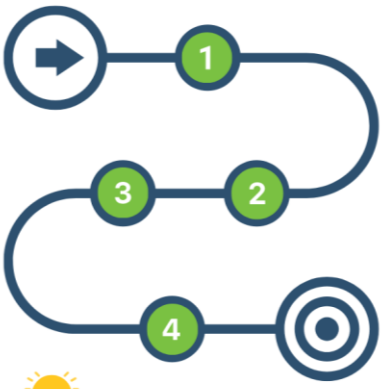
Unbemerkte Manipulation von Protokollen verstößt gegen Anhang I, Teil I, Punkt 2(l) des CRA: "Aufzeichnung und Überwachung relevanter interner Aktivitäten."

Umgehung von Warnungen bei wiederholten Anmeldefehlern, die gegen Anhang I, Teil I, Punkt 2(h) des CRA verstoßen: "Schutz der Verfügbarkeit wesentlicher und grundlegender Funktionen … einschließlich der Abwehr von Denial-of-Service-Angriffen."

Szenario 3: Smart Meter Gateway (CRA-kritisches Produkt)

Testansatz

Testtyp: Grey Box (Firmware- und Schnittstellenspezifikationen werden bereitgestellt; Pentester führt Protokoll- und eingebettete Tests durch).
Komplexität: Hoch (Komplexe eingebettete Systeme und proprietäre Protokolle).
Aufwandsschätzung: 15–20 Arbeitstage (~25–30 Tage vergangen).



Angriffspfad

1. **Aufklärung:** Identifizieren Sie Endpunkte und Kommunikationsmuster für Firmware-Updates.
2. **Ausnutzung der Sicherheitslücke:** Wiederverwendung des erfassten Firmware-Update-Datenverkehrs. Bereitstellung betrügerischer Firmware.
3. **Auswirkungsanalyse und -berichterstattung:** Demonstrieren Sie die vollständige Übernahme der Smart Meter-Gateway-Logik.
4. **Follow-up:** Neugestaltung des sicheren Bootvorgangs mit kryptografischer Kette und Patch-Replay-Exposition.

Ergebnisse und Auswirkungen

- *Der Firmware-Aktualisierungsprozess akzeptierte nicht signierte Bilder.*
- *Die sichere Boot-Validierung wurde durch Bootloader-Fehler umgangen.*
- *Replay-Angriffe wurden erfasst und gültige verschlüsselte Kommunikationen erneut gesendet.*

Empfehlungen

- *Erzwingen Sie während der Firmware-Installation die Prüfung digitaler Signaturen.*
- *Härten Sie den Bootloader, um kryptografische Vertrauensketten zu validieren.*
- *Fügen Sie Nonces und Aktualitätsprüfungen hinzu, um Replay-Angriffe abzuschwächen.*

Auswirkungen der CRA-Compliance

Eine fehlende Firmware-Validierung verstößt gegen Anhang I, Teil I, Punkt 2(k) des CRA: "Reduzieren Sie die Auswirkungen eines Vorfalls durch geeignete Techniken zur Eindämmung der Ausnutzung."

Replay-Angriffe, die Firmware-Kommunikationsverletzungen ausnutzen. CRA Anhang I, Teil I, Punkt 2(e): "Schützen Sie die Vertraulichkeit gespeicherter oder übertragener Daten durch den Einsatz modernster Mechanismen."

Anhang A: Auswahl der berücksichtigten PDEs

IWichtig: Klasse I

- *Identitätsmanagementsysteme*
- *Browser*
- *Passwortmanager*
- *Software zur Ausstellung digitaler Zertifikate*
- *Router*
- *Smart-Home-Produkte*
- *Wearables zur Gesundheitsüberwachung*
- *SIEM-Systeme*

Wichtig: Klasse II

- *Firewalls*

Kritische Produkte

- *Smart Meter Gateway*

Anhang B: CRA-Anforderungen

1. Anhang I Teil I – Grundlegende Anforderungen an die Cybersicherheit

CRA-Anforderung	CRA-Anforderungsreferenz
Produkte mit digitalen Elementen müssen so entworfen, entwickelt und hergestellt werden, dass sie ein angemessenes Cybersicherheitsniveau gewährleisten, das den Risiken entspricht.	Anhang I, Teil I, Punkt 1
(a) Sie müssen mit einer standardmäßig sicheren Konfiguration auf dem Markt bereitgestellt werden, sofern zwischen dem Hersteller und dem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen Elementen nichts anderes vereinbart wurde, einschließlich der Möglichkeit, das Produkt in seinen ursprünglichen Zustand zurückzusetzen.	Anhang I, Teil I, Punkt 2(a)
(b) Sie müssen mit einer standardmäßig sicheren Konfiguration auf dem Markt bereitgestellt werden, einschließlich der Möglichkeit, den ursprünglichen Zustand wiederherzustellen.	Anhang I, Teil I, Punkt 2(b)
(c) Sie müssen gewährleisten, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls durch automatische Sicherheitsaktualisierungen, die innerhalb eines angemessenen Zeitraums installiert werden, standardmäßig aktiviert sind, über einen klaren und benutzerfreundlichen Mechanismus zum Deaktivieren verfügen und den Nutzern mitgeteilt werden, wobei die Möglichkeit besteht, diese vorübergehend auszusetzen.	Anhang I, Teil I, Punkt 2(c)

(d) Sie müssen Schutz vor unbefugtem Zugriff durch geeignete Kontrollmechanismen, einschließlich, aber nicht beschränkt auf Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, gewährleisten und über möglichen unbefugten Zugriff Bericht erstatten.	Anhang I, Teil I, Punkt(d)
(e) Sie müssen die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, beispielsweise durch Verschlüsselung der relevanten Daten im Ruhezustand oder während der Übertragung durch modernste Mechanismen und durch den Einsatz anderer technischer Mittel.	Anhang I, Teil I, Punkt 2(e)
(f) Sie müssen die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor Manipulationen oder Änderungen, die nicht vom Nutzer autorisiert sind, schützen und jede Beschädigung melden	Anhang I, Teil I, Punkt 2(f)
(g) Es findet eine Verarbeitung nur von personenbezogenen oder sonstigen Daten, die angemessen, relevant und auf das für den vorgesehenen Zweck des Produkts mit digitalen Elementen erforderliche Maß beschränkt sind (Datenminimierung) statt.	Anhang I, Teil I, Punkt 2(g)
(h) Sie schützen die Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach einem Vorfall, unter anderem durch Resilienz- und Abhilfemaßnahmen gegen Denial-of-Service-Angriffe.	Anhang I, Teil I, Punkt 2(h)
(i) Es besteht eine Minimierung der negativen Auswirkungen der Produkte selbst oder der verbundenen Geräte auf die Verfügbarkeit von Diensten, die von anderen Geräten oder Netzen bereitgestellt werden.	Anhang I, Teil I, Punkt 2(i)
j) Sie müssen so entworfen, entwickelt und hergestellt sein, dass Angriffsflächen, einschließlich externer Schnittstellen, begrenzt sind.	Anhang I, Teil I, Punkt 2(j)

k) Sie müssen so entworfen, entwickelt und hergestellt sein, dass die Auswirkungen eines Vorfalls durch geeignete Mechanismen und Techniken zur Abwehr von Ausbeutung verringert werden.	Anhang I, Teil I, Punkt 2(k)
(l) Es gibt eine Bereitstellung sicherheitsrelevanter Informationen durch Aufzeichnung und Überwachung relevanter interner Aktivitäten, einschließlich des Zugriffs auf oder der Änderung von Daten, Diensten oder Funktionen, mit einer Opt-out-Möglichkeit für den Nutzer.	Anhang I, Teil I, Punkt 2(l)
(m) Es gibt die Möglichkeit für Nutzer, alle Daten und Einstellungen sicher und einfach dauerhaft zu löschen, und, sofern diese Daten auf andere Produkte oder Systeme übertragen werden können, Gewährleistung, dass dies auf sichere Weise erfolgt.	Anhang I, Teil I, Punkt 2(m)

2. Anhang I Teil II – Anforderungen an den Umgang mit Schwachstellen

CRA-Anforderung	CRA-Zitat
Identifizierung und Dokumentation von Schwachstellen und Komponenten in Produkten mit digitalen Elementen, unter anderem durch Erstellung einer Software-Stückliste in einem gängigen und maschinenlesbaren Format, die mindestens die Abhängigkeiten der obersten Ebene der Produkte abdeckt	Anhang I, Teil II, Punkt 1
In Bezug auf die Risiken für Produkte mit digitalen Elementen sind Schwachstellen unverzüglich zu beheben, unter anderem durch Bereitstellung von Sicherheitsupdates; soweit technisch möglich, sind neue Sicherheitsupdates getrennt von Funktionsupdates bereitzustellen.	Anhang I, Teil II, Punkt 2

Die Sicherheit des Produkts mit digitalen Elementen ist durch wirksame und regelmäßige Tests und Überprüfungen zu gewährleisten.	Anhang I, Teil II, Punkt 3
Sobald ein Sicherheitsupdate verfügbar ist, sind Informationen über behobene Schwachstellen zu teilen und öffentlich bekannt zu geben, einschließlich einer Beschreibung der Schwachstellen, Informationen, die es den Nutzern ermöglichen, das betroffene Produkt mit digitalen Elementen zu identifizieren, der Auswirkungen der Schwachstellen, ihrer Schwere sowie klarer und zugänglicher Informationen, die den Nutzern helfen, die Schwachstellen zu beheben. In hinreichend begründeten Fällen, in denen die Hersteller die Sicherheitsrisiken einer Veröffentlichung als größer als die Sicherheitsvorteile erachten, können sie die Veröffentlichung von Informationen über eine behobene Schwachstelle aufschieben, bis die Nutzer die Möglichkeit hatten, den entsprechenden Patch anzuwenden.	Anhang I, Teil II, Punkt 4
Einführung und Durchsetzung einer Politik zur koordinierten Offenlegung von Schwachstellen	Anhang I, Teil II, Punkt 5
Maßnahmen, um den Austausch von Informationen über potenzielle Schwachstellen in Produkten mit digitalen Elementen sowie in darin enthaltenen Komponenten von Drittanbietern zu erleichtern, unter anderem durch die Bereitstellung einer Kontaktadresse für die Meldung von Schwachstellen, die in Produkten mit digitalen Elementen entdeckt wurden	Anhang I, Teil II, Punkt 6
Mechanismen zur sicheren Verteilung von Updates für Produkte mit digitalen Elementen, um sicherzustellen, dass Schwachstellen rechtzeitig behoben oder gemindert werden, und gegebenenfalls für automatische Sicherheitsupdates	Anhang I, Teil II, Punkt 7
Sicherstellen, dass Sicherheitsaktualisierungen, die zur Behebung festgestellter Sicherheitsprobleme verfügbar sind, unverzüglich und, sofern zwischen einem Hersteller und einem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen Elementen nichts	Anhang I, Teil II, Punkt 8

anderes vereinbart wurde, kostenlos verbreitet werden, zusammen mit Hinweisen, die den Nutzern die relevanten Informationen, einschließlich potenzieller Maßnahmen, zur Verfügung stellen	

Anhang C: Auswahl von ETSI TS 103701-Testgruppen und Testfällen mit Zuordnung zu den CRA-Anforderungen

Testgruppe ID	Testfall (konzeptionell)	Verbundene CRA-Anforderung Ref.
TSO 5.1: Keine universellen Standardpasswörter	(5.1-1) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der passwortbasierten Authentifizierungsmechanismen.	Anhang I, Teil I, Punkt 2 (d)
	(5.1-2) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Generierungsmechanismen für vorinstallierte Passwörter.	Anhang I, Teil I, Punkt 2(d)
TSO 5.2: Implementierung einer Möglichkeit zur Verwaltung von Schwachstellenmeldungen	(5.2-1) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Veröffentlichung der Richtlinie zur Offenlegung von Sicherheitslücken.	Anhang I, Teil II, Punkt 5
	(5.2-2) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Art und Weise, wie auf Schwachstellen reagiert wird, a), und die Bestätigung, dass die Voraussetzungen für die Umsetzung gewährleistet sind, b).	Anhang I, Teil II, Punkt 2
TSO 5.3: Software auf dem neuesten	(5.3-1) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Aktualisierbarkeit von Softwarekomponenten hinsichtlich des Fehlens von Software-Updates, a), und der Aktualisierungsmechanismen, b).	Anhang I, Teil II, Punkt 7

Stand halten	(5.3-2) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung des Mechanismus zur Installation von Updates hinsichtlich geeigneter Maßnahmen, um einen Angreifer daran zu hindern, die Installation von Updates auf dem Prüflingsgerät zu missbrauchen.	Anhang I, Teil II, Punkt 7
	(5.3-3) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Update-Mechanismen hinsichtlich ihrer Einfachheit für den Benutzer.	Anhang I, Teil I, Punkt 2 (c) Anhang I, Teil II, Punkt 8
TSO 5.4: Sichere Speicherung sensibler Sicherheitsparameter	(5.4-1) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der sicheren Speicherung sensibler Sicherheitsparameter hinsichtlich der Sicherheitsanforderungen (a-c) und der Vollständigkeit der IXIT-Dokumentation (d).	Anhang I, Teil I , Punkt 2 (e)
	(5.4-2) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der manipulationssicheren Speicherung fest codierter Identitäten.	Anhang I, Teil I, Punkt 2 (e)
TSO 5.5: Sichere Kommunikation	(5.5-1) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der für die Kommunikationsmechanismen verwendeten Kryptografie hinsichtlich der Verwendung bewährter Kryptografieverfahren (a-c) und der Anfälligkeit für einen realisierbaren Angriff (d).	Anhang I, Teil I, Punkt 2 (e)
	(5.5-4) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Gerätefunktionalität über eine Netzwerkschnittstelle im initialisierten Zustand hinsichtlich Authentifizierung und Autorisierung.	Anhang I, Teil I, Punkt 2 (d)
TSO 5.7: Gewährleistung der Softwareintegrität	(5.7-1) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der sicheren Startmechanismen des geprüften Produkts.	Anhang I, Teil I, Punkt 2 (f)
	(5.7-2) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Warnmechanismen a) und der Mechanismen zur Einschränkung der Kommunikation b) im Falle der Erkennung einer unbefugten Softwareänderung.	Anhang I, Teil I, Punkt 2 (f)

TSO 5.8: Gewährleistung der Sicherheit personenbezogener Daten	(5.8-1) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Kryptografie, die für die Kommunikation personenbezogener Daten zwischen einem Gerät und einem Dienst verwendet wird.	Anhang I, Teil I, Punkt 2 (e)
TSO 5.9: Ausfallsicherheit der Systeme	(5.9-1) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Ausfallsicherheitsmechanismen in Bezug auf Netzwerk- und Stromausfälle.	Anhang I, Teil I, Punkt 2 (h)
	(5.9-3) Der Zweck dieses Testfalls ist die konzeptionelle Bewertung der Ausfallsicherheitsmaßnahmen für die Kommunikationsmechanismen.	Anhang I, Teil I, Punkt 2 (h)

Anhang D: Vergleich der Methoden

Weit verbreitete Pentesting-Methoden der Branche			
Umfang	**Rolle in diesem Leitfaden**		
	Haupt	**Mittel**	**Keine**
Produktspezifische Testgruppen und Verfahren gemäß CRA Anhang I	**ETSI TS 103 701**		
Umreißt grundlegende Cybersicherheitsanforderungen für Verbraucher-IoT-Geräte. In dieser Methodik ergänzt es TS 103 701 durch die Definition der erwarteten Secure-by-Design-Sicherheitslage, die durch Tests überprüft wird.	**ETSI EN 303 645**		
Bietet eine strukturierte Methode zur Messung der Sicherheitslage anhand definierter Metriken (z. B. RAV-Werte). Die Anwendung der OSSTMM3-Metriken kann die interne Reifegradverfolgung unterstützen und bei Bedarf in der CRA-Dokumentation referenziert werden.	**OSSTMM3**		
Breit anwendbar auf IT-Systeme, Netzwerke und Anwendungen. Außerdem ist sie die detaillierteste Methode mit expliziten Phasen für die Analyse nach der Ausnutzung und die Analyse der Auswirkungen auf das Geschäft.		**PTES**	
Weniger präskriptiv in Bezug auf die Schritte vor und nach dem Engagement, Fokus auf der technischen Ausführung.		**NIST SP 800-115**	
Anwendungsorientiert, mit begrenzten IoT-spezifischen Leitlinien.		**OWASP Testleitfaden**	
Konzentriert sich auf die Erfassung von Verhaltensmustern und TTPs von Angreifern. Bietet keine strukturierte Testmethodik, verbessert jedoch Angriffssimulationen und Sicherheitsmaßnahmen.			**MITRE ATT&CK Rahmen**
Konzentriert sich auf technische, verfahrenstechnische und Compliance-Aspekte von Sicherheitsbewertungen.			**ISSAF**

Intelligence-basiertes Red Teaming, das auf kritische Sektoren zugeschnitten ist und den Schwerpunkt auf realistische Angriffssimulationen auf Basis neuer Bedrohungen legt.			**TIBER-EU**

Anhang E: Testwerkzeuge und Frameworks

Kategorie	**Werkzeuge**
Regulatorische und Compliance-Richtlinien	CRA (Cyber Resilience Act), PSD2 (überarbeitete Zahlungsdiensterichtlinie), SWIFT CSP (Kundensicherheitsprogramm)
Informationsbeschaffung	recon-ng (Aufklärungsframework), Maltego (Datenauswertung und Link-Analyse), Shodan (Internetscan nach verbundenen Geräten), theHarvester (Tool zur Informationsbeschaffung), SpiderFoot (automatisierte OSINT-Erfassung)
Netzwerksicherheit	Nmap (Netzwerkscanning), Wireshark (Paketanalyse), Nessus (Schwachstellenscanning), OpenVAS (Open-Source-Schwachstellenscanning)
Web- und API-Sicherheit	Burp Suite (Web-Sicherheitstests), Checkmarx ZAP (automatisiertes Web-Schwachstellenscanning), Bruno (API-Sicherheitstests), Caido
Ausnutzung und Red Teaming	Metasploit (Exploitation-Framework), BloodHound (Analyse von Angriffspfaden in Active Directory), Cobalt Strike (Red-Teaming-Tool)
Cloud-Sicherheit	ScoutSuite (Multi-Cloud-Sicherheitsaudits), Prowler (AWS-Sicherheitsbewertung), CloudMapper (Visualisierung der AWS-Architektur und Sicherheitsprüfungen)
Sicherheit in der Fertigung	FactorySecure (Sicherheitsüberwachung von Fertigungssystemen), OTORIO RAM2 (Sicherheitsplattform für Betriebstechnologien), Claroty (industrielle Cybersicherheitstests)

KI und Automatisierung	Darktrace (Anomalieerkennung durch maschinelles Lernen), Vectra AI (KI-gestützte Bedrohungserkennung), MITRE CALDERA (automatisierte Emulation von Angreifern), SnapAttack (automatisiertes Red-Teaming-Tool)
Firmware-Analyse	binwalk (Firmware-Reverse-Engineering), Ghidra (Software-Reverse-Engineering-Suite)
IoT-Scanning	Shodan (Geräteerkennung und Schwachstellensuche), Firmwalker (Firmware-Konfigurationsscanner), JTAGulator (Hardware-Schnittstellenidentifizierung)
Hardware-Schnittstellen	USBlyzer (USB-Protokollanalyse), Logikanalysatoren (digitale Signalprüfung), UART/Serial-Tools (Debugging serieller Schnittstellen)
Protokolltests	Scapy (Tool zur Paketmanipulation), Wireshark (Protokollanalyse), CAN-utils (Controller Area Network-Protokolltest)

Anhang E: Sicherheitsrichtlinien und bewährte Verfahren

Während Kapitel 5 die in diese Penetrationstest-Methodik integrierten Teststandards und -methoden beschreibt, enthält dieser Anhang bewährte Sicherheitsverfahren und Implementierungshinweise, die nach Produktkategorien gegliedert sind.

Produktkategorie	**Relevante Normen und Richtlinien**
Identitätsmanagementsysteme, Browser, Passwortmanager, Software für digitale Zertifikate, SIEM-Systeme	OWASPASVS Anwendungs-Sicherheitsverifizierungsstandard ISO/IEC 27001 Informationssicherheits-Management CIS Benchmarks Richtlinien für sichere Konfiguration ISVS Sicherheitsverifizierungsstandard für das Internet der Dinge
IoT-Geräte für Verbraucher: Router, Smart-Home-Geräte, Wearables zur Gesundheitsüberwachung,	ETSI EN 303 701 Cybersicherheit für das Internet der Dinge für Verbraucher: Konformitätsbewertung der Grundanforderungen ISO/IEC 27400:2022, Cybersicherheit. IoT-Sicherheit und Datenschutz. Leitlinien ENISA Leitfaden für bewährte Verfahren für die Sicherheit des IoT, sicherer Softwareentwicklungslebenszyklus DSGVO (Datenschutz-Grundverordnung), ISO/IEC 27701 (Datenschutz-Management), IoT Security Foundation Guidelines
Firewalls, Smart-Meter-Gateways	NIST SP 800-82 Leitfaden zur Sicherheit industrieller Steuerungssysteme, IEC 62443 Industrielle Kommunikationsnetze – Netzwerk- und Systemsicherheit
Fertigungssektor	ISA/IEC 62443 Sicherheit industrieller Automatisierungs- und Steuerungssysteme ISO 9001 Qualitätsmanagementsysteme CMMC Cybersecurity Maturity Model Certification