CONFIRMATE

Valutazione della conformità, metriche e automazione dei processi di conformità per il Cyber Resilience Act

Metodologia dei test di penetrazione

Data di emissione: 2025-08-05

Stato: Revisionato

Versione:0.3

Il progetto finanziato nell'ambito della convenzione di sovvenzione **n. 101190193** è sostenuto dal Centro europeo per la competenza in materia di sicurezza informatica. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione europea o del Centro europeo per la competenza in materia di sicurezza informatica. Né l'Unione europea né l'autorità che concede la sovvenzione possono essere ritenute responsabili per tali opinioni e pareri.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Elenco delle modifiche

Versione	Data	Descrizione	Autore/i
0.1	21/03/25	Bozza iniziale della metodologia condivisa con i partner per revisione e feedback	Cyen
0.2	08/04/25	Revisioni incorporate sulla base dei feedback ricevuti dai partner.	Cyen
0.3	05/08/25	Revisioni incorporate sulla base dei feedback ricevuti dai colleghi	Cyen

Ringraziamo sinceramente i revisori, in particolare Krasen Parvanov (QRTECH), Stijn Horemans (Refracted), Ayman Khalil e Romain Muguet (Red Alert Labs), Peter Kuzmin (Kikimora) e Dominik Holzapfel (Nviso), per le loro osservazioni critiche e i loro commenti ponderati, che hanno contribuito in modo significativo a migliorare l'accuratezza e la chiarezza di questa metodologia.

Metodologia di test di penetrazione per la conformità CRA per le PMI

Contenuti

1. Riferimenti

- Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, recante requisiti orizzontali di sicurezza informatica per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) n. 2019/1020 e la direttiva (UE) 2020/1828 (Legge sulla resilienza informatica), disponibile qui: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
- Istituto per la sicurezza e le metodologie aperte (ISECOM). (2010). Manuale di metodologia per i test di sicurezza open source (OSSTMM) versione 3.0, disponibile qui: https://www.isecom.org/OSSTMM.3.pdf
- Standard di esecuzione dei test di penetrazione (PTES) Organizzazione PTES. (n.d.). Standard di esecuzione dei test di penetrazione (PTES), disponibile qui: 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), disponibile qui: https://csrc.nist.gov/pubs/sp/800/115/final
- OWASP Foundation. (n.d.). OWASP Web Security Testing Guide (WSTG), disponibile qui: https://owasp.org/www-project-web-security-testing-guide/
- MITRE Corporation. (n.d.). MITRE ATT&CK® Framework, disponibile qui: https://attack.mitre.org/
- Open Information Systems Security Group (OISSG). (2005). Information Systems Security Assessment Framework (ISSAF) Draft 0.2, disponibile qui: https://untrustednetwork.net/files/issaf0.2.1.pdf
- Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) Banca centrale europea. (2023). Quadro TIBER-EU: Ethical Red Teaming basato sull'intelligence sulle minacce, disponibile qui: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

- ETSI TS 103 701 V1.1.1 (2021-08): Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements. Available here: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

2. Glossario: acronimi, termini e abbreviazioni

Acronimi

OSSTMM:	**Manuale sulla metodologia di test di sicurezza open source**
OWASP:	**Progetto sulla sicurezza delle applicazioni web aperte**
PTES:	**Standard per l'esecuzione dei test di penetrazione**
NIST:	**Istituto nazionale per gli standard e la tecnologia**
SIEM:	**Gestione delle informazioni e degli eventi di sicurezza**
IAM:	**Gestione delle identità e degli accessi (dedotto dal contesto)**
API:	**Interfaccia di programmazione dell'applicazione**
VPN:	**Rete privata virtuale**
SSO:	**Accesso singolo**
IoT:	**Internet delle cose**
GDPR:	**Regolamento generale sulla protezione dei dati**
ISO:	**Organizzazione internazionale per la standardizzazione**
IEC:	**Commissione elettrotecnica internazionale**
CIS:	**Centro per la sicurezza Internet**
CMMC:	**Certificazione del modello di maturità della sicurezza informatica**
PSD2:	**Direttiva sui servizi di pagamento aggiornata**
SWIFT CSP:	**Società per le telecomunicazioni finanziarie interbancarie mondiali Programma di sicurezza dei clienti**

Termini

Test di penetrazione (o pen testing):	Un esercizio di sicurezza in cui un esperto di cybersecurity cerca di individuare e sfruttare le vulnerabilità di un prodotto e del suo ambiente, comprese hardware, software, interfacce e punti di interazione con l'utente
Vulnerabilità:	Una debolezza o un difetto in un sistema, un'applicazione o una rete che può essere sfruttata per compromettere la sicurezza
Exploit:	Un codice, una tecnica o un processo che sfrutta una vulnerabilità per causare un comportamento indesiderato in un sistema.
Attore di minaccia:	Un individuo o un gruppo che rappresenta un potenziale rischio per la sicurezza informatica di un'organizzazione, come hacker, insider o concorrenti.
Valutazione del rischio:	Il processo di identificazione dei rischi che potrebbero influire negativamente sulle operazioni di un'organizzazione.
Audit di sicurezza:	Valutazione sistematica della sicurezza di un prodotto digitale, volta a verificare la conformità a requisiti tecnici e normativi prestabiliti, quali quelli del Cyber Resilience Act (CRA
Piano di risposta agli incidenti:	Una serie di istruzioni per aiutare le organizzazioni a rilevare, rispondere e riprendersi da incidenti di sicurezza della rete informatica
Crittografia:	Il metodo con cui le informazioni vengono convertite in un codice segreto che nasconde il loro vero significato.
Produttore:	Soggetto fisico o giuridico che sviluppa, produce o detiene prodotti digitali e li commercializza a proprio nome o marchio, a titolo oneroso o gratuito, per finalità di monetizzazione
Autenticazione a più fattori (MFA):	Un metodo di autenticazione che richiede all'utente di fornire due o più fattori di verifica per ottenere l'accesso a una risorsa, come un'applicazione, un account online o una VPN.
Ingegneria sociale:	Tattica che consiste nel manipolare, influenzare o ingannare una vittima per ottenere il controllo di un

	sistema informatico o per rubare informazioni personali e finanziarie.
Tattiche, tecniche e procedure (TTP):	Descrive il comportamento di un autore di minacce e un modello strutturato per condurre attacchi informatici.
Triade CIA (riservatezza, integrità, disponibilità):	Modello di sicurezza delle informazioni progettato per proteggere le informazioni sensibili dalle violazioni dei dati.
Prodotto con elementi digitali (PDE):	Prodotto che contiene o è interconnesso con software o firmware ed è in grado di raccogliere, trasmettere o elaborare dati. I PDE includono sia dispositivi fisici che prodotti definiti dal software immessi sul mercato o messi in servizio.

3. Introduzione

3.1 Scopo e obiettivi

Il presente documento descrive come gestire e condurre test di penetrazione su prodotti con elementi digitali (PDE) al fine di verificare la conformità al Cyber Resilience Act (CRA). Questa metodologia colma una lacuna pratica definendo un processo di lavoro di pentesting allineato al CRA e adattato all'esposizione al rischio per il prodotto, concentrandosi su come tali test supportino una dichiarazione di conformità. Sebbene il CRA non citi né imponga test di penetrazione, questi rimangono una delle tecniche più potenti per determinare in che misura le potenziali vulnerabilità sono sfruttabili da un aggressore. Di conseguenza, un test di penetrazione riuscito può consolidare la base probatoria a sostegno di una dichiarazione di conformità.

Lo sviluppo di questa metodologia si è focalizzato in particolar modo su una serie di prodotti presenti nell'allegato A. Questi prodotti coprono vari livelli di criticità definiti nel Cyber Resilience Act (CRA). Essi sono stati selezionati proprio al fine garantire l efficacia della metodologia in diversi casi d'uso e fungono da punto di riferimento per tutti gli strumenti Confirmate.

L'approccio si basa su una metodologia riconosciuta (OSSTMM3), sviluppata in una comunità aperta e sottoposta a revisione tra pari e interdisciplinare. OSSTMM3 offre un approccio strutturato per identificare le vulnerabilità passibili di attacchi informatici, consentendo una valutazione più accurata dei potenziali rischi per la sicurezza.

Gli obiettivi dell'approccio proposto sono i seguenti:

- Fornire un metodo strutturato per testare la penetrazione dei prodotti con elementi digitali, offrendo al contempo flessibilità nelle tecniche utilizzate.
- Stabilire un insieme standard di risultati che possano supportare la dichiarazione di conformità alla CRA del produttore.
- Illustrare il metodo spiegando come potrebbe essere applicato a diversi prodotti tratti dai prodotti importanti (classe I e classe II) e dai prodotti critici definiti dalla CRA
- Questa metodologia non copre le valutazioni IT generiche delle imprese o i test di penetrazione di applicazioni web autonome che non costituiscono un PDE come definito dalla CRA. Le risorse esclusivamente web sono spesso coperte dalle metodologie OWASP, ma non sono in linea con l'ambito normativo incentrato sul prodotto in questione.

3.2 Destinatari

Il documento è rivolto ai fornitori di prodotti con componenti i digitali, come definiti dalla CRA.

4. Settore di applicazione

4.1 Applicabilità alle PMI

L'approccio ai test di penetrazione proposto nel presente documento è stato concepito per essere utilizzato dalle piccole e medie imprese (PMI). L'approccio mira ad essere di facile comprensione, ogni gergo tecnico superfluo è stato eliminato affinché esso sia alla portata delle aziende di piccole dimensioni.

Questa metodologia è applicabile sia ai prodotti digitali autonomi che a quelli integrati nell'ambito di applicazione della CRA, compresi i dispositivi di consumo, i controllori industriali, i gateway intelligenti e i componenti critici per la sicurezza. Sebbene sia stata progettata principalmente per i test pre-commercializzazione e in servizio, può essere applicata anche nelle fasi iniziali di sviluppo per identificare le vulnerabilità prima della distribuzione.

4.2 Confini e limitazioni

Il presente documento descrive come gestire ed eseguire test di penetrazione con l'obiettivo di garantire una dichiarazione di conformità ai requisiti della CRA. Non rientrano in questo ambito le strategie di riparazione, i controlli di mitigazione o le misure di sicurezza da adottare a seguito della scoperta di punti deboli durante i test.

Inoltre, a differenza dei test di penetrazione classici, che mirano a valutare la sicurezza di un ambiente informatico, i test descritti nel presente documento si concentrano su un prodotto. Pertanto tale approccio è significativo solo se il prodotto è ospitato in un ambiente adeguato. L'ambiente di esecuzione è quindi determinante per definire la validità dei risultati finali. In questo contesto, i test di penetrazione si svolgono tipicamente all'interno di un laboratorio controllato, in cui il team deve predisporre o approvare il banco di prova, garantendo che esso riproduca condizioni operative realistiche senza compromettere i presupposti di sicurezza.

4.3 Ipotesi e vincoli

Le ipotesi principali formulate nell'approccio presentato sono le seguenti:

- Il prodotto sarà testato in un “ambiente di laboratorio” anziché sul campo.
- L'ambiente in cui il prodotto sarà testato sarà molto simile all'ambiente di destinazione (ovvero l'ambiente in cui il prodotto verrà utilizzato).

Sebbene in questo approccio vengano proposti scenari di prova esemplificativi, si presume che i fabbricanti li adattino in modo da riflettere le caratteristiche del prodotto oggetto di test.

I vincoli relativi al processo saranno individuati nell'ambito delle attività previste per la fase 1. Il vincolo principale è che le prove devono essere progettate in modo da non avere un impatto negativo sulle attività dell'ente di prova.

5. Standard industriali per i test

5.1 ETSI EN 303 645

La norma è accompagnata da una specifica di prova (TS 103 701) e da una guida all'implementazione (TR 103 621)
https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

ETSI TS 103 701 fornisce gruppi di test strutturati e valutazioni di conformità su misura per i dispositivi IoT di consumo. I casi di test coprono i requisiti funzionali, di resilienza, di interfaccia e di protezione dei dati. In questa metodologia, i gruppi di test pertinenti della TS 103 701 sono applicati in modo selettivo alle categorie di prodotti descritte nell'allegato A.

ETSI EN 303 645 è lo standard europeo di base per la sicurezza informatica dei dispositivi IoT di consumo. Stabilisce disposizioni necessarie per affrontare i vettori di attacco più comuni e di maggiore impatto. Lo standard mira a garantire un livello minimo di sicurezza e funge da riferimento per le normative nazionali e le valutazioni di conformità.

5.2 OSSTMM3

Un audit OSSTMM fornisce una misurazione oggettiva e precisa della sicurezza a livello operativo, basata su dati verificabili e procedure standardizzate. La metodologia è progettata per essere coerente e ripetibile. Essendo un progetto open source, OSSTMM consente a qualsiasi tester di sicurezza di contribuire con idee per rendere i test più accurati, praticabili ed efficienti, promuovendo al contempo la libera diffusione delle informazioni e della proprietà intellettuale.

Rispetto agli standard basati sulla conformità, OSSTMM 3 si concentra sulla convalida della sicurezza nel mondo reale, comprendendo più domini, tra cui:

- **Reti di dati**: router, firewall, SIEM, contatori intelligenti e dispositivi IoT.
- **Telecomunicazioni**: sicurezza dell'accesso remoto, configurazioni VPN.
- **Sicurezza wireless**: vulnerabilità Wi-Fi, standard di crittografia.

Un elemento innovativo introdotto da OSSTMM 3 sono i valori di valutazione del rischio (RAV), che permettono ai team di sicurezza di quantificare il livello di esposizione, monitorare l'evoluzione delle vulnerabilità nel tempo e migliorare così la gestione dei rischi e il processo decisionale.

5.3 Guida ai test OWASP

La Guida ai test OWASP è stata sviluppata nell'ambito del Progetto di testing OWASP dell'Open Web Application Security Project (OWASP). La metodologia non fornisce un test di penetrazione completo, ma si concentra solo sulle fasi principali dei test di sicurezza delle applicazioni web.

La guida fornisce un'analisi dettagliata della valutazione della sicurezza delle applicazioni web e del relativo stack di distribuzione, compresa la configurazione del server web. Adotta un approccio di penetration testing black-box, fornendo indicazioni complete sul *cosa* testare e *quando*. Include inoltre alcune indicazioni sul *come*, principalmente sotto forma di elenchi di strumenti utilizzabili in ciascuna fase o attività.

5.4 PTES

Lo Standard di esecuzione dei test di penetrazione (PTES) rappresenta la metodologia di penetration testing più recente. È stato sviluppato da un team di professionisti della sicurezza informatica con l'obiettivo di fornire uno standard completo e aggiornato per le attività di penetration testing.

Oltre a fungere da guida per i professionisti della sicurezza, orienta le aziende nelle aspettative rispetto a un penetration test e le assiste nella definizione dell'ambito e nella negoziazione di progetti efficaci. Copre il "cosa" e il "quando", ma approfondisce molto di più il "come".

Il PTES è composto da due parti principali, tra loro complementari. Le linee guida Pentest descrivono le sezioni principali e le fasi di un test di penetrazione, mentre le linee guida tecniche discutono gli strumenti e le tecniche specifiche da utilizzare in ciascuna fase.

.

5.5 NIST SP 800-15

Il documento NIST 800-115, intitolato "Guida tecnica per il collaudo e la valutazione della sicurezza delle informazioni", fornisce linee guida e raccomandazioni per valutare la sicurezza delle informazioni e, di conseguenza, lo stato di protezione dei sistemi e delle reti informatiche.

Esso mira ad aiutare le organizzazioni a comprendere i vari tipi di valutazioni di sicurezza, a selezionare le tecniche di valutazione appropriate e progettare programmi di valutazione completi.

Le linee guida possono essere applicate a diverse organizzazioni, tra cui agenzie federali, organizzazioni del settore privato e istituti di istruzione.

Maggiori dettagli sulle metodologie di pentesting più diffuse e sul loro confronto sono disponibili nell'Allegato D: Confronto tra metodologie. Inoltre, nell'Allegato E sono elencate le linee guida di sicurezza e le pratiche più diffuse.

6. Metodologia all'avanguardia

Il Manuale sulla metodologia di test di sicurezza open source (OSSTMM 3) è la metodologia principale utilizzata in questo approccio di test di penetrazione. Fornisce un quadro metodologico per condurre test di sicurezza approfonditi, qui denominati audit OSSTMM.

Sebbene OSSTMM 3 sia la metodologia principale, questo framework di test di penetrazione integra anche elementi provenienti da:

- **ETSI TS 103 701 –** I casi di test rilevanti di questo standard di conformità sono stati incorporati nel nostro processo di esecuzione dei test, in particolare per l'IoT e i PDE consumer.
- **Guida ai test OWASP** – Abbiamo integrato i casi di test OWASP nelle fasi di ricognizione e sfruttamento per le applicazioni web e le API, seguendo le linee guida OWASP per identificare vulnerabilità quali SQL injection, cross-site scripting e gestione non sicura delle sessioni..
- **PTES** (Standard di esecuzione dei test di penetrazione) – PTES definisce un ciclo di vita strutturato che abbiamo integrato nella metodologia. Per garantire che ogni fase abbia obiettivi, risultati e protocolli di comunicazione chiari, abbiamo allineato le fasi OSSTMM3 con PTES, ottenendo un processo di test coerente e ripetibile.

NIST SP 800-115 – NIST SP 800-115 fornisce un solido quadro di riferimento per i test di sicurezza basati sul rischio. Le fasi di sfruttamento e analisi dell'impatto sono state allineate a tali linee guida per garantire un'individuazione sistematica delle vulnerabilità, una valutazione completa dei rischi e una reportistica dettagliata.

7. Preparazione per un test di penetrazione

Perché effettuare i test? Il CRA richiede al PDE di "effettuare test efficaci e revisioni regolari della sicurezza del prodotto con elementi digitali" (Allegato I, Parte II, Punto 3). La pianificazione di valutazioni regolari della sicurezza garantisce un monitoraggio continuo e permette di individuare proattivamente le vulnerabilità, rafforzando la protezione contro le minacce esterne.

Chi effettuerà i test? Nel contesto delle valutazioni allineate al CRA, la scelta di un penetration tester (o fornitore) è importante per l'affidabilità, la riproducibilità e la rilevanza normativa dei risultati. Le PMI possono affidarsi a pentester che soddisfino i seguenti requisiti:

- *Competenza tecnica*: comprovata esperienza nella sicurezza dei prodotti, nei sistemi integrati, nei test del firmware e nell'analisi delle vulnerabilità del software. I fornitori devono comprendere le differenze tra i test sui prodotti e le valutazioni tradizionali dell'ambiente aziendale.
- *Familiarità con il CRA*: conoscenza dimostrabile del Cyber Resilience Act, compresi i requisiti dell'Allegato I Parte I e II e la capacità di produrre risultati che supportino le dichiarazioni di conformità al CRA.
- *Conoscenza del settore:* scegliere fornitori già attivi o con esperienza nel campo del prodotto.
- *Garanzia legale ed etica*: assicurarsi che i tester rispettino linee guida etiche chiare, dispongano di adeguata copertura assicurativa e sottoscrivano contratti trasparenti, comprensivi di clausole sulla responsabilità e sul trattamento dei dati.
- *Certificazioni e accreditamenti*: sono utili certificazioni quali OSCP, OSCE, CREST o credenziali nazionali equivalenti a livello europeo. Per prodotti ad alto rischio o critici, prendere in considerazione l'esperienza di certificazione TIBER-EU o Red Team.

Quanto tempo ci vorrà? Le tempistiche possono variare in base alla complessità del prodotto, al livello di conoscenza (black/grey/white box) e alla classificazione CRA (predefinita, importante o critica), ma una stima generica del tempo necessario per ciascuna fase può essere riassunta come segue:

1. Preparazione (5-10 giorni lavorativi, *collaborazione tra tester e produttore*), che include:

- Definizione dell'ambito, degli obiettivi e dei limiti dei test
- Mappatura dei requisiti dell'allegato I della CRA

- Accordi legali e allineamento delle parti interessate
- Consegna della documentazione tecnica da parte del cliente

2. Esecuzione dei test e report (3-10 giorni lavorativi, condotti dal tester), che include:

- Raccolta di informazioni, sfruttamento e analisi dell'impatto
- Test del firmware del prodotto, delle interfacce, delle API e dei controlli di sicurezza
- Preparazione e diffusione dei report

3. Correzione (1-4 settimane, a cura del produttore)

- Sviluppo di patch, correzioni di configurazione, controllo qualità interno
- Eventuale accettazione del rischio e aggiornamento della documentazione

4. Nuovi test (1-2 giorni lavorativi, collaborazione tra tester e produttore)

- Convalida delle correzioni implementate
- Conferme tecniche finali e raccolta delle prove

8. Metodologia dei test di penetrazione

8.1 Pre-impegno e pianificazione

- Il primo passo consiste nel definire il tipo di test appropriato, sulla base della maturità del prodotto, dei rischi per la sicurezza identificati (interni/esterni), della documentazione disponibile e dei possibili vettori di attacco (le modalità con cui un prodotto potrebbe essere sfruttato). Il test può essere:
- Black-box: i tester non hanno alcuna conoscenza interna e simulano un attacco esterno.
- Grey-box: i tester dispongono di conoscenze parziali e di un accesso limitato.
- White-box: i tester hanno una conoscenza completa del sistema (codice sorgente, architettura), consentendo test approfonditi.
- Si segnala che i test in laboratorio presuppongono generalmente una conoscenza parziale o completa (white-box).
- Input:
- Identificazione del prodotto. Per i test white-box e grey-box: è necessaria la documentazione tecnica, che include: casi d'uso operativi, diagrammi dell'architettura, versione del firmware/software, elenco delle interfacce interne ed esterne (ad es. USB, BLE, API, interfaccia utente web, porte, protocolli) o qualsiasi risorsa/componente noto rilevante per il test, modello di minaccia (se disponibile). Inoltre, potrebbero essere utili dettagli di precedenti valutazioni o audit (se disponibili), inclusi i ticket di bug aperti o i risultati dei test non risolti.
- Framework di settore (ad esempio OSSTMM3, PTES, NIST SP 800-115, OWASP)
- Requisiti normativi e documentazione di conformità, compresi i requisiti dell'Allegato I, Parte I e II del CRA (vedere Allegato B: Requisiti CRA)
- Punti di contatto e protocolli di emergenza, compresa una procedura di emergenza (cosa fare in caso di eventi imprevisti, come interruzioni del servizio) durante i test.

- Documentazione contrattuale (per tester esterni): contratti di servizio, accordi di non divulgazione, autorizzazioni ai test e liberatorie di responsabilità.

- Attività:
- Definizione degli obiettivi e dell'ambito: questa fase inizia con la chiara definizione degli obiettivi e dell'ambito dei test, con particolare attenzione alla verifica delle funzionalità specifiche di ciascun sistema. La definizione dell'ambito è fondamentale per allineare i test di penetrazione agli obiettivi del CRA e alle caratteristiche specifiche del prodotto sottoposto a verifica. Tale fase comprende:
- Definizione dei confini del prodotto: definizione del limite tecnico (software, hardware, API, interfacce) del prodotto con elementi digitali (PDE).
- Mappatura CRA: identificazione dei requisiti dell'allegato I del CRA applicabili al livello di rischio del prodotto.
- Input per la modellazione delle minacce: considerare gli attori delle minacce noti, le superfici di attacco e il contesto del prodotto.
- Profondità dei test: il livello di approfondimento dei test di penetrazione viene determinato in base alla classificazione di criticità del prodotto secondo il Cyber Resilience Act (CRA).
- I test sui prodotti di classe I si concentrano generalmente sui servizi e sulle interfacce esposti all'esterno, sui meccanismi di controllo degli accessi, sulla protezione dei dati in transito e sull'individuazione delle vulnerabilità note.
- Un prodotto di classe II richiede un'ispezione più approfondita del firmware, dei meccanismi di aggiornamento, della comunicazione tra dispositivo e cloud, dei flussi di autenticazione e degli scenari di uso improprio del protocollo.
- I test sui prodotti critici includono la convalida della sicurezza a livello hardware, come il rilevamento delle manomissioni, la resistenza all'iniezione di guasti e la verifica dell'avvio sicuro.
- Considerazioni legali, normative ed etiche: i test sono condotti nel rispetto dei requisiti legali e normativi (ad esempio, privacy, protezione dei dati, leggi sulla proprietà intellettuale) e delle politiche interne.

- Tutte le autorizzazioni richieste sono garantite e i vincoli sono documentati in modo che l'ambiente di test non influisca sulle operazioni di produzione. (vedere Allegato B: Requisiti CRA, Allegato I CRA, Parte I, punti 1, 2(b), 2(g), 2(j); e Allegato I, Parte II, punto 1.)
- Creazione di un laboratorio di prova che riproduca l'ambiente operativo del PDE.

Risultati delle fasi successive:

- Documento metodologico di alto livello
- Moduli di autorizzazione legale
- Definizione dell'ambito dei test
- Linee guida per l'esecuzione
- Rapporto di valutazione dei rischi del prodotto
- Briefing per le parti interessate

Risultati finali:

- Documento di pianificazione e requisiti (D1): un piano dettagliato del progetto di pentesting che delinea l'ambito, i ruoli, gli obiettivi, l'autorizzazione, i tempi e la configurazione del laboratorio.
- Valutazione dei rischi pre-test e allineamento delle parti interessate (D2):

8.2 Raccolta di informazioni e ricognizione

Input:

- Definizione dell'ambito dei test
- Rapporto di valutazione dei rischi del prodotto

Attività:

- Open-Source Intelligence e Asset Discovery: in questa fase viene utilizzata l'intelligence open source per raccogliere quante più informazioni possibili. Essa prevede la mappatura dell'impronta digitale di ogni prodotto ed elemento.
- Profilazione degli obiettivi e analisi delle minacce: è necessaria un'analisi di ciascuna risorsa per determinare vulnerabilità potenziali. Viene inoltre esaminato il quadro delle minacce per garantire che il pentesting impieghi scenari realistici e rifletta le tattiche degli avversari negli attacchi simulati.
- Sviluppo di scenari basati sul comportamento degli avversari: sulla base delle informazioni e dei dati raccolti vengono formulati scenari di attacco specifici.

Risultati per le fasi successive:

- Scenari di comportamento degli avversari e profili degli obiettivi
- Prima versione del rapporto sulle vulnerabilità (D3): risultati dettagliati delle valutazioni esterne e interne del prodotto, comprese le analisi dei rischi, la fattibilità dello sfruttamento e i suggerimenti per le correzioni, che forniscono una visione completa delle vulnerabilità del prodotto.

Risultati finali:

- Nessun risultato in questa fase.

8.3 Esecuzione dei test e sfruttamento

Input:

- Prima versione del rapporto sulle vulnerabilità (D3): risultati dettagliati delle valutazioni esterne e interne del prodotto, comprese le valutazioni dei rischi, la fattibilità dello sfruttamento e i suggerimenti per la correzione, che forniscono una visione completa delle vulnerabilità del prodotto.
- Scenari di comportamento degli avversari e profili degli obiettivi
- Strumenti di test (ad esempio Nessus, Metasploit, Wireshark). Esempi di strumenti di test e framework sono elencati nell'Allegato E.
- (se disponibile) codice sorgente del software.

Attività:

- Identificazione delle vulnerabilità e simulazione degli attacchi: le vulnerabilità vengono rilevate tramite analisi statica (SAST), dinamica (DAST) o revisione manuale del codice, quando applicabile. Per migliorare l'efficienza, è possibile utilizzare intelligence sulle minacce basata su AI. Ogni prodotto viene testato secondo standard definiti, e i risultati delle valutazioni, eseguite ripetutamente, confluiscono nel rapporto sulle vulnerabilità D4, fungendo da base primaria per la successiva valutazione dei rischi. Gli scenari di test selezionati, provenienti dalla norma ETSI TS 103701, sono elencati nell'allegato C in quanto potrebbero essere eseguiti nell'ambito del pentesting che, oltre alla sicurezza, verificherebbe la conformità con il CRA in allineamento. Le attività svolte durante questa fase convalidano anche i requisiti di progettazione sicura e protezione in linea con il CRA. Cfr. allegato B: CRA allegato I, parte I, punti 2, lettere a), b), d), e), j) e k), e allegato I, parte II, punto 3.
- Tecniche di sfruttamento ed emulazione degli avversari: i difetti vengono convalidati cercando di sfruttarli in un ambiente controllato. Se disponibili, possono essere utilizzati strumenti di scansione basati sull'intelligenza artificiale. Le PMI prive di tali strumenti possono ricorrere all'ispezione manuale o a forme di automazione più semplici, come il rilevamento di anomalie nei log o il fuzzing guidato dall'apprendimento automatico. Inoltre, vengono valutate le situazioni in cui gli avversari potrebbero aggirare le misure di sicurezza e ottenere accessi non autorizzati.
- Analisi post-sfruttamento: valutazione dell'impatto di un attacco riuscito, includendo l'escalation dei privilegi all'interno del sistema e il potenziale movimento laterale verso altri utenti, componenti o sistemi collegati. L'analisi considera la possibilità che un aggressore possa accedere a dati sensibili, spostarsi tra moduli applicativi o segmenti dell'infrastruttura, o compromettere servizi critici. Sulla base dell'impatto funzionale vengono raccolti dettagli utili a valutare le conseguenze potenziali di ciascuna vulnerabilità.
- I risultati dei casi di test vengono integrati nei risultati finali di questa fase, garantendo la tracciabilità delle attività di test rispetto ai comportamenti attesi.

Risultati per le fasi successive:

- Elenco delle vulnerabilità
- Prove di sfruttamento (proof-of-concept)
- Valutazioni preliminari dei rischi
- Rapporto sulla fattibilità dello sfruttamento
- Rapporto sulla simulazione delle tattiche degli avversari

Risultati finali:

- Rapporto sulle vulnerabilità (D3): risultati dettagliati delle valutazioni esterne e interne del prodotto, comprese le valutazioni dei rischi, la fattibilità dello sfruttamento e i suggerimenti per la correzione, che forniscono una visione completa delle vulnerabilità.

8.4 Analisi dell'impatto e rendicontazione

Input:

- Elenco delle vulnerabilità
- Prove di sfruttamento (proof-of-concept)
- Valutazioni preliminari del rischio
- Standard di valutazione del rischio specifici del settore
- Politiche di classificazione dei dati.

Attività:

- Valutazione del rischio e valutazione dell'impatto funzionale: analisi della gravità delle vulnerabilità identificate, misurazione del loro impatto su CIA (riservatezza, integrità o disponibilità). Assegnazione di una valutazione del rischio per dare priorità agli interventi di correzione. Inoltre, è possibile utilizzare modelli di valutazione del rischio basati sull'intelligenza artificiale per migliorare la fase di valutazione complessiva, assegnando livelli di rischio basati su informazioni in tempo reale sulle minacce e sui dati di sfruttabilità. Ciò include la valutazione allineata al CRA dell'integrità dei dati, della resilienza e della risposta alle vulnerabilità. Cfr. allegato B: CRA allegato I, parte I, punti 2, lettere e) e f), e 2, lettera i); allegato I, parte II, punti 1 e 2.
- Documentazione dei risultati e raccolta delle prove: creazione di rapporti approfonditi contenenti descrizioni delle vulnerabilità, prove tecniche e prove di sfruttamento, garantendo sempre una chiara comprensione delle lacune di sicurezza.
- Segnalazione di conformità normativa: tradurre i risultati dei test in termini di conformità normativa segnalando i risultati collegati ai requisiti CRA Allegato I e II elencati nell'Allegato B. In tal modo, contribuire a un rapporto di allineamento alla conformità normativa, che può essere utilizzato per giustificare la dichiarazione di conformità di un produttore.

- Raccomandazioni e strategie di mitigazione attuabili: fornire indicazioni dettagliate per ridurre i rischi individuati, suggerendo controlli di sicurezza, modifiche di configurazione e strategie di patch per aumentare la resilienza del sistema. Per approfondimenti, consultare l'Allegato B: Requisiti CRA.

Risultati per le fasi successive:

- Rapporto di valutazione dei rischi
- Documento completo dei risultati
- Dettagli sull'impatto funzionale
- Raccomandazioni di rimedio
- Piano d'azione di rimedio prioritario
- Rapporto di allineamento alla conformità normativa

Risultati finali:

- Raccomandazioni e roadmap di rimedio (D5): raccomandazioni prioritarie con una chiara roadmap di rimedio, comprese azioni a breve, medio e lungo termine.

8.5 Follow-up post-impegno

Input:

- Rapporti sulle misure correttive
- Configurazioni di sistema aggiornate e risultati dei nuovi test.

Attività:

Verifica delle misure correttive e ripetizione dei test: ripetere i test per verificare che le falle di sicurezza siano state risolte. Assicurarsi che le misure correttive eliminino efficacemente le vulnerabilità. Le attività post-test confermano l'allineamento con le aspettative CRA in materia di aggiornamenti di sicurezza e divulgazione.

- Cfr. allegato B: CRA allegato I, parte I, punti 2, lettera h) e 2, lettera m); e allegato I, parte II, punti 2, 4, 7 e 8.
- Miglioramento continuo e integrazione delle lezioni apprese: aggiornamento delle metodologie di test e delle politiche di sicurezza sulla base dei risultati. L'analisi basata sull'intelligenza artificiale contribuisce a migliorare le future valutazioni di sicurezza utilizzando le lezioni apprese dai test precedenti. (vedere: Allegato: Requisiti CRA, Allegato I, Parte I)

- Divulgazione e comunicazione delle vulnerabilità: una volta disponibili gli aggiornamenti di sicurezza, i produttori devono preparare e divulgare pubblicamente i dettagli relativi alle vulnerabilità risolte.Nei casi in cui la divulgazione comporti un rischio eccessivo, la pubblicazione può essere posticipata fino a quando le patch non siano state ampiamente distribuite (Allegato I, Parte II, punto 4).

Risultati finali:

- Rapporto di pentesting (D5): un tipico rapporto di pentesting include una sintesi (panoramica di alto livello, valutazione complessiva del rischio, risultati dei test e raccomandazioni prioritarie), l'ambito e il metodo di prova (D1), le attività, i risultati (con ulteriori dettagli, incluse le vulnerabilità (D2) e le prove di sfruttamento) e le raccomandazioni (D4). Il presente documento potrebbe essere considerato una «revisione della sicurezza del prodotto con elementi digitali» ai fini del requisito CRA di cui all'allegato I, parte II, punto 3 (Applicare test e revisioni efficaci e regolari della sicurezza del prodotto con elementi digitali).

8.6 Risultati

Ogni incarico produrrà una serie completa di risultati progettati per soddisfare sia le esigenze tecniche che strategiche. Per ogni fase della metodologia, i risultati saranno di due tipi: (a) risultati utilizzati come input per una fase successiva e (b) risultati dell'intero esercizio. I risultati dell'intero esercizio sono elencati di seguito;

- Documento di pianificazione e requisiti (D1): un piano dettagliato del progetto di pentesting che delinea obiettivi, ambito, ruoli, misure di emergenza, autorizzazioni, tempistiche e configurazione del laboratorio.
- Valutazione dei rischi pre-test e allineamento delle parti interessate (D2): un'analisi approfondita dei potenziali rischi prima dell'inizio dei test, che garantisce l'allineamento con le parti interessate in merito all'ambito, alle priorità e agli obiettivi.
- Rapporto sulle vulnerabilità (D3): risultati dettagliati delle valutazioni esterne e interne del prodotto, inclusi i livelli di rischio, la fattibilità dello sfruttamento e i suggerimenti per la risoluzione, che forniscono una visione completa delle vulnerabilità che interessano il prodotto stesso.
- Raccomandazioni e roadmap di correzione (D4): raccomandazioni prioritarie con una chiara roadmap di correzione, comprese azioni a breve, medio e lungo termine.

- Rapporto sui test di penetrazione (D5): una panoramica di alto livello per gli stakeholder non tecnici che riassume i risultati chiave e le raccomandazioni strategiche.

8.7 Esempi di scenari

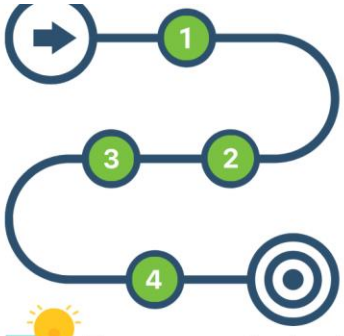
Lo scopo di questa sezione è fornire esempi illustrativi di scenari di test di penetrazione, includendo una stima approssimativa delle risorse necessarie e dei tempi previsti. Questi scenari hanno valore indicativo e possono variare notevolmente da un esercizio all'altro.

Scenario 1: Gestione delle identità e degli accessi (Prodotto importante di CRA: Classe I)

Scenario 2: Gestione delle informazioni e degli eventi di sicurezza (SIEM) (Prodotto importante di CRA: Classe II)

Approccio di test

- **Tipo di test:** Grey Box (credenziali SIEM fornite; il pentester simula input ostili e manomissione dei log).
- **Complessità:** Elevata (15-30 fonti di log, set di regole e integrazioni).
- **Stima dello sforzo:** 12-15 giorni di lavoro (~20-25 giorni trascorsi).



Risultati e impatto

- *SIEM non è riuscito ad attivare gli avvisi in caso di ripetuti tentativi di accesso non riusciti.*
- *L'iniezione di syslog ha consentito di nascondere i registri delle intrusioni.*
- *I controlli di integrità dei registri potevano essere aggirati tramite l'evasione del payload.*

Raccomandazioni

- *Configurare le regole di rilevamento delle anomalie per le soglie basate sull'autenticazione.*
- *Pulire gli input dei log per impedire l'iniezione di log.*
- *Utilizzare la firma e la convalida crittografica dei log per garantirne l'integrità.*

Percorso di attacco

1. **Ricognizione:** riesamina i punti di acquisizione SIEM, le regole di correlazione e le soglie di allerta.
2. **Sfruttamento delle vulnerabilità:** inserisci log appositamente creati per nascondere gli attacchi reali. Sfrutta la mancanza di correlazione degli eventi sui login non riusciti.
3. **Analisi dell'impatto e reporting:** valuta in che modo la soppressione degli avvisi consente un accesso persistente.
4. **Follow-up:** rafforza la logica di analisi e i set di regole di audit.

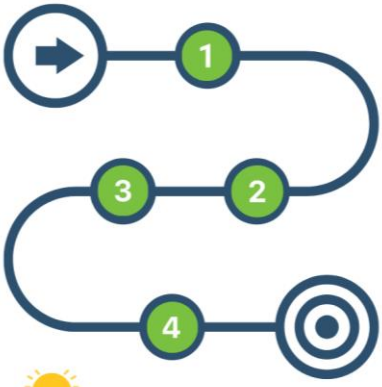
Impatto sulla conformità CRA

La manomissione dei registri senza rilevamento viola l'Allegato I, Parte I, punto 2(l) del CRA: "Registrazione e monitoraggio delle attività interne rilevanti".
L'aggiramento degli avvisi in caso di ripetuti tentativi di accesso non riusciti viola l'Allegato I, Parte I, punto 2(h) del CRA: "Proteggere la disponibilità delle funzioni essenziali e di base... compresa la mitigazione degli attacchi di tipo denial-of-service".

Scenario 3: Gateway per contatori intelligenti (prodotto critico CRA)

Approccio di test

- **Tipo di test:** Grey Box (specifiche firmware e interfaccia fornite; il pentester esegue test di protocollo e integrati).
- **Complessità:** Elevata (sistemi integrati complessi e protocolli proprietari).
- **Stima dello sforzo:** 15-20 giorni di lavoro (~25-30 giorni trascorsi).



Risultati e impatto

- *Il processo di aggiornamento del firmware accettava immagini non firmate.*
- *La convalida dell'avvio sicuro veniva aggirata tramite falle nel bootloader.*
- *Gli attacchi di replay catturavano e inviavano nuovamente comunicazioni crittografate valide.*

Raccomandazioni

- *Applicare controlli della firma digitale durante l'installazione del firmware.*
- *Rafforzare il bootloader per convalidare le catene di fiducia crittografiche.*
- *Includere nonce e controlli di freschezza per mitigare gli attacchi di replay.*

Percorso di attacco

1. **Ricognizione:** identificare gli endpoint degli aggiornamenti del firmware e i modelli di comunicazione.
2. **Sfruttamento delle vulnerabilità:** riutilizzare il traffico degli aggiornamenti del firmware acquisito. Distribuire firmware non autorizzato.
3. **Analisi dell'impatto e reportistica:** dimostrare il controllo completo della logica del gateway dei contatori intelligenti.
4. **Follow-up:** riprogettare l'avvio sicuro con catena crittografica ed esposizione al replay delle patch.

Impatto sulla conformità CRA

La mancanza della convalida del firmware viola l'Allegato I, Parte I, punto 2(k) del CRA: "Ridurre l'impatto di un incidente utilizzando tecniche di mitigazione dello sfruttamento appropriate".
Gli attacchi di replay che sfruttano le comunicazioni del firmware violano l'Allegato I, Parte I, punto 2(e) del CRA: "Proteggere la riservatezza dei dati memorizzati o trasmessi utilizzando meccanismi all'avanguardia".

Allegato A: Selezione delle PDE prese in considerazione

Importante: Classe I

- *Sistemi di gestione delle identità*
- *Browser*
- *Gestori di password*
- *Software per l'emissione di certificati digitali*
- *Router*
- *Prodotti per la casa intelligente*
- *Dispositivi indossabili per il monitoraggio della salute*
- *Sistemi SIEM*

Importante: Classe II

- *Firewall*

Prodotti critici

- *Gateway per contatori intelligenti*

Allegato B: Requisiti CRA

1. Allegato I Parte I – Requisiti essenziali di sicurezza informatica

Requisiti CRA	Riferimento ai requisiti CRA
I prodotti con componenti digitali devono essere progettati, sviluppati e realizzati garantendo un livello di sicurezza informatica adeguato ai rischi associati.	Allegato I, Parte I, Punto 1
(a) devono essere immessi sul mercato con una configurazione sicura di default, salvo diverso accordo tra il fabbricante e l'utilizzatore professionale per prodotti su misura con componenti digitali, garantendo in ogni caso la possibilità di ripristinare il prodotto allo stato originale.	Allegato I, Parte I, Punto 2 (a)
(b) essere messi a disposizione sul mercato con una configurazione sicura di default, compresa la possibilità di ripristinare lo stato originale	Allegato I, Parte I, Punto 2 (b)
(c) devono garantire la correzione delle vulnerabilità tramite aggiornamenti di sicurezza. Questi aggiornamenti, anche automatici, devono essere installati entro tempi adeguati e attivati come impostazione predefinita. Deve essere previsto un meccanismo di rinuncia chiaro e semplice, con notifiche agli utenti sugli aggiornamenti disponibili e la possibilità di posticiparne temporaneamente l'installazione.v	Allegato I, Parte I, Punto 2 (c)

(d) devono garantire la protezione da accessi non autorizzati mediante meccanismi di controllo adeguati, inclusi, a titolo esemplificativo ma non esaustivo, sistemi di autenticazione, di gestione dell'identità o dell'accesso, e segnalare accessi non autorizzati.	Allegato I, Parte I, Punto 2 (d)
(e) devono garantire la protezione dei dati conservati, trasmessi o comunque trattati, personali o di altro tipo. Ciò può essere realizzato, ad esempio, tramite la crittografia dei dati in fase di riposo o in transito, utilizzando meccanismi avanzati e adeguati strumenti tecnici.	Allegato I, Parte I, Punto 2 (e)
(f) devono proteggere l'integrità dei dati conservati, trasmessi o comunque trattati, siano essi personali o di altro tipo, nonché dei comandi, dei programmi e della configurazione, prevenendo qualsiasi manipolazione o modifica non autorizzata dall'utente e segnalando eventuali danneggiamenti.	Allegato I, Parte I, Punto 2 (f)
(g) trattare esclusivamente dati, personali o di altro tipo, adeguati, pertinenti e limitati alla finalità prevista del prodotto con componenti digitali (principio di minimizzazione dei dati).	Allegato I, Parte I, Punto 2 (g)
(h) proteggere la disponibilità delle funzioni essenziali e di base, anche dopo un incidente, anche attraverso misure di resilienza e mitigazione contro gli attacchi di tipo «denial of service»	Allegato I, Parte I, Punto 2 (h)
(i) ridurre al minimo l'impatto negativo dei prodotti stessi o dei dispositivi connessi sulla disponibilità dei servizi forniti da altri dispositivi o reti	Allegato I, Parte I, Punto 2 (i)
(j) essere progettati, sviluppati e prodotti in modo da limitare le superfici di attacco, comprese le interfacce esterne	Allegato I, Parte I, Punto 2 (j)
(k) essere progettati, sviluppati e prodotti in modo da ridurre l'impatto di un incidente grazie a meccanismi e tecniche adeguati di mitigazione dello sfruttamento	Allegato I, Parte I, Punto 2 (k)

(l) devono fornire informazioni relative alla sicurezza, registrando e monitorando le attività interne rilevanti, come l'accesso o la modifica di dati, servizi o funzioni, e prevedere un meccanismo di rinuncia accessibile all'utente."	Allegato I, Parte I, Punto 2 (l)
(m) offrire agli utenti la possibilità di rimuovere in modo sicuro e semplice tutti i dati e le impostazioni in modo permanente e, qualora tali dati possano essere trasferiti ad altri prodotti o sistemi, garantire che ciò avvenga in modo sicuro.	Allegato I, Parte I, Punto 2 (m)

2. Allegato I Parte II – Requisiti per la gestione della vulnerabilità

Requisiti CRA	Citazione CRA
Individuare e documentare le vulnerabilità e i componenti presenti nei prodotti con elementi digitali, creando anche un elenco dei componenti software in un formato standard e leggibile da un computer, che includa almeno le dipendenze principali del prodotto.	Allegato I, Parte II, Punto 1
In base ai rischi associati ai prodotti con componenti digitali, le vulnerabilità devono essere affrontate e risolte senza ritardo, anche tramite aggiornamenti di sicurezza. Quando tecnicamente possibile, i nuovi aggiornamenti di sicurezza devono essere forniti separatamente dagli aggiornamenti funzionali.	Allegato I, Parte II, Punto 2
Applicare test e revisioni efficaci e regolari della sicurezza del prodotto.	Allegato I, Parte II, Punto 3
Una volta reso disponibile un aggiornamento di sicurezza, i fabbricanti devono condividere e rendere pubbliche le informazioni sulle vulnerabilità risolte, includendo una descrizione della vulnerabilità, i dati necessari per identificare il prodotto interessato, l'impatto della vulnerabilità, la loro gravità e indicazioni chiare e accessibili per consentire agli utenti di intervenire. In casi giustificati,	Allegato I, Parte II, Punto 4

qualora i fabbricanti ritengano che i rischi derivanti dalla pubblicazione superino i benefici per la sicurezza, la divulgazione delle informazioni può essere posticipata fino a quando gli utenti non abbiano avuto la possibilità di applicare la patch pertinente.	
Adottare e applicare una politica di divulgazione coordinata delle vulnerabilità.	Allegato I, Parte II, Punto 5
Adottare misure per facilitare la condivisione delle informazioni sulle vulnerabilità dei prodotti, inclusi i componenti di terzi in essi contenuti, fornendo anche un contatto specifico per la segnalazione delle vulnerabilità riscontrate nei prodotti.	Allegato I, Parte II, Punto 6
Prevedere meccanismi per distribuire in modo sicuro gli aggiornamenti, garantendo che le vulnerabilità vengano corrette o mitigate tempestivamente e, quando possibile, consentendo l'installazione automatica degli aggiornamenti di sicurezza.	Allegato I, Parte II, Punto 7
Garantire che gli aggiornamenti di sicurezza, volti a risolvere problemi individuati, siano distribuiti tempestivamente e, salvo diverso accordo tra il fabbricante e un utente aziendale per un prodotto su misura, a titolo gratuito. Gli aggiornamenti devono essere accompagnati da informazioni chiare per gli utenti.	Allegato I, Parte II, Punto 8

Allegato C: Selezione dei gruppi di test ETSI TS 103701 e dei casi di test con mappatura ai requisiti CRA

ID gruppo di test	Caso di prova (concettuale)	Riferimento al requisito CRA collegato.
TSO 5.1: Nessuna password predefinita universale	(5.1-1) Lo scopo di questo caso di prova è la valutazione concettuale dei meccanismi di autenticazione basati su password.	Allegato I, Parte I, Punto 2 (d)
	(5.1-2) Lo scopo di questo caso di prova è la valutazione concettuale dei meccanismi di generazione delle password preinstallate.	Allegato I, Parte I, Punto 2 (d)
TSO 5.2: Implementare un mezzo per gestire le segnalazioni di vulnerabilità	(5.2-1) Lo scopo di questo caso di prova è la valutazione concettuale della pubblicazione della politica di divulgazione delle vulnerabilità.	Allegato I, Parte II, Punto 5
	((5.2-2) Lo scopo di questo caso di prova è la valutazione concettuale delle modalità di intervento sulle vulnerabilità, a), e la conferma che siano garantiti i prerequisiti per l'implementazione, b).	Allegato I, Parte II, Punto 2
TSO 5.3: Mantenere aggiornato il software	(5.3-1) Lo scopo di questo caso di prova è la valutazione concettuale dell'aggiornabilità dei componenti software, sia in relazione all'assenza di aggiornamenti software, a), sia ai meccanismi di aggiornamento, b).	Allegato I, Parte II, Punto 7
TSO 5.4: Archiviazione sicura dei parametri di	(5.3-2) Lo scopo di questo caso di prova è la valutazione concettuale del meccanismo di installazione degli aggiornamenti, verificando che siano previste misure adeguate a impedire a un aggressore di sfruttarlo in modo improprio sul DUT.	Allegato I, Parte I, Punto 7

sicurezza sensibili	(5.3-3) Lo scopo di questo caso di prova è la valutazione concettuale dei meccanismi di aggiornamento per quanto riguarda la semplicità per l'utente.	Allegato I, Parte I, Punto 2(c) Allegato I, Parte II, Punto 8
TSO 5.5: Comunicazione sicura	(5.5-1) Lo scopo di questo caso di prova è la valutazione concettuale della crittografia impiegata nei meccanismi di comunicazione, considerando l'uso delle migliori pratiche di crittografia (a-c) e la resistenza a eventuali attacchi (d).	Allegato I, Parte I, Punto 2 (e)
	(5.5-4) Lo scopo di questo caso di prova è la valutazione concettuale della funzionalità del dispositivo tramite un'interfaccia di rete nello stato inizializzato, con particolare attenzione ai meccanismi di autenticazione e autorizzazione.	Allegato I, Parte I, Punto 2 (d)
TSO 5.7: Garanzia dell'integrità del software	(5.7-1) Lo scopo di questo caso di prova è la valutazione concettuale dei meccanismi di avvio sicuro del DUT.	Allegato I, Parte I, Punto 2(f)
	(5.7-2) Lo scopo di questo caso di prova è la valutazione concettuale dei meccanismi di allerta, a), e dei meccanismi di limitazione della comunicazione, b), in caso di rilevamento di una modifica non autorizzata del software.	Allegato I, Parte I, Punto 2(f)
TSO 5.8: Garanzia della sicurezza dei dati personali	(5.8-1) Lo scopo di questo caso di prova è la valutazione concettuale della crittografia utilizzata per la comunicazione dei dati personali tra un dispositivo e un servizio.	Allegato I, Parte I, Punto 2(e)
TSO 5.9: Resilienza dei sistemi	(5.9-1) Lo scopo di questo caso di prova è la valutazione concettuale dei meccanismi di resilienza relativi alle interruzioni della rete e dell'alimentazione.	Allegato I, Parte I, Punto 2(h)

alle interruzioni	(5.9-3) Lo scopo di questo caso di prova è la valutazione concettuale delle misure di resilienza per i meccanismi di comunicazione.	Allegato I, Parte I, Punto 2 (h)

Allegato D: Confronto tra metodologie

Metodologie di pentesting ampiamente riconosciute nel settore			
Ambito di applicazione	**Ruolo nella presente guida**		
	principale	**Medio**	**Nessuno**
Gruppi di test specifici per prodotto e procedure allineate all'Allegato I del CRA.	**ETSI TS 103 701**		

Delinea i requisiti di base in materia di sicurezza informatica per i dispositivi IoT di consumo. In questa metodologia, integra la norma TS 103 701 definendo la posizione di sicurezza prevista in fase di progettazione, verificata attraverso test.	**ETSI EN 303 645**		
Fornisce un metodo strutturato per valutare il livello di sicurezza tramite metriche definite, come i punteggi RAV. L'applicazione delle metriche OSSTMM3 può supportare il monitoraggio della maturità interna e, se opportuno, essere riportata nella documentazione CRA.	**OSSTMM3**		
Ampiamente applicabile a sistemi IT, reti e applicazioni. Inoltre, è il più dettagliato, con fasi esplicite per l'analisi post-sfruttamento e dell'impatto sul business.		**PTES**	
Meno prescrittivo sulle fasi pre/post-impegno, si concentra sull'esecuzione tecnica.		**NIST SP 800-115**	
Centrato sull'applicazione, con indicazioni specifiche limitate per l'IoT..		**OWASP Guida ai test**	
Si concentra sulla mappatura dei comportamenti degli avversari e dei TTP. Non fornisce una metodologia di test strutturata, ma migliora le simulazioni di attacco e le operazioni di sicurezza.			**MITRE ATT&CK quadro**
Si concentra sugli aspetti tecnici, procedurali e di conformità delle valutazioni di sicurezza.			**ISSAF**
Red teaming basato sull'intelligence, mirato ai settori critici, che privilegia simulazioni di attacco realistiche ispirate alle minacce emergenti.			**TIBER-EU**

Allegato E: Strumenti e framework di test

Categoria	**Strumenti**
Linee guida normative e di conformità	CRA (Cyber Resilience Act), PSD2 (Direttiva sui servizi di pagamento rivista), SWIFT CSP (Programma di sicurezza dei clienti)

Raccolta di informazioni	recon-ng (framework di ricognizione), Maltego (data mining e analisi dei collegamenti), Shodan (scansione Internet alla ricerca di dispositivi connessi), theHarvester (strumento di raccolta informazioni), SpiderFoot (raccolta automatizzata di OSINT)
Sicurezza della rete	Nmap (scansione di rete), Wireshark (analisi dei pacchetti), Nessus (scansione delle vulnerabilità), OpenVAS (scansione delle vulnerabilità open source)
Sicurezza web e API	Burp Suite (test di sicurezza web), Checkmarx ZAP (scansione automatizzata delle vulnerabilità web), Bruno (test di sicurezza API), Caido
Sfruttamento e red teaming	Metasploit (framework di sfruttamento), BloodHound (analisi dei percorsi di attacco Active Directory), Cobalt Strike (strumento di red teaming)
Sicurezza cloud	ScoutSuite (audit di sicurezza multi-cloud), Prowler (valutazione della sicurezza AWS), CloudMapper (visualizzazione dell'architettura AWS e controlli di sicurezza)
Sicurezza della produzione	FactorySecure (monitoraggio della sicurezza dei sistemi di produzione), OTORIO RAM2 (piattaforma di sicurezza della tecnologia operativa), Claroty (test di sicurezza informatica industriale)
IA e automazione	Darktrace (rilevamento delle anomalie tramite machine learning), Vectra AI (rilevamento delle minacce basato sull'intelligenza artificiale), MITRE CALDERA (emulazione automatizzata degli avversari), SnapAttack (strumento automatizzato per il red teaming)
Analisi del firmware	binwalk (reverse engineering del firmware), Ghidra (suite per il reverse engineering del software)
Scansione IoT	Shodan (ricerca di dispositivi e vulnerabilità), Firmwalker (scanner di configurazione firmware), JTAGulator (identificazione interfaccia hardware)

Interfacce hardware	USBlyzer (analisi protocollo USB), Logic Analyzers (ispezione segnale digitale), strumenti UART/Serial (debugging interfaccia seriale)
Test dei protocolli	Scapy (strumento di manipolazione dei pacchetti), Wireshark (analisi dei protocolli), CAN-utils (test dei protocolli Controller Area Network)

Allegato E: Linee guida e best practice per la sicurezza

Mentre il Capitolo 5 illustra gli standard e le metodologie di test incorporati nella presente metodologia di penetration testing, il presente Allegato fornisce le migliori pratiche di sicurezza e le linee guida per l'implementazione, organizzate per categoria di prodotto.

Categoria di prodotto	**Norme e linee guida pertinenti**
Sistemi di gestione delle identità, browser, gestori di password, software per certificati digitali, sistemi SIEM	OWASP ASVS Standard di verifica della sicurezza delle applicazioni ISO/IEC 27001 Gestione della sicurezza delle informazioni CIS Benchmarks Linee guida per la configurazione sicura ISVS Standard di verifica della sicurezza dell'Internet delle cose
Dispositivi IoT consumer: router, dispositivi per la casa intelligente, dispositivi indossabili per il monitoraggio della salute,	ETSI EN 303 701 Sicurezza informatica per l'Internet delle cose di consumo: valutazione della conformità dei requisiti di base ISO/IEC 27400:2022, Sicurezza informatica. Sicurezza e privacy dell'IoT. Linee guida ENISA Guida alle buone pratiche per la sicurezza dell'IoT, ciclo di vita dello sviluppo di software sicuro GDPR (Regolamento generale sulla protezione dei dati), ISO/IEC 27701 (Gestione delle informazioni sulla privacy), Linee guida della IoT Security Foundation
firewall, gateway per contatori intelligenti	NIST SP 800-82 Guida alla sicurezza dei sistemi di controllo industriale, IEC 62443 Reti di comunicazione industriale - Sicurezza delle reti e dei sistemi
Manufacturing Sector	ISA/IEC 62443 Sicurezza dei sistemi di automazione e controllo industriale ISO 9001 Sistemi di gestione della qualità CMMC Certificazione del modello di maturità della sicurezza informatica