Istituto nazionale di test per la cibersicurezza

Cibersicurezza dei dispositivi periferici

Rischi nascosti in ufficio: Le tastiere wireless, le cuffie e altri dispositivi simili sono sufficientemente sicuri per l'impiego nelle infrastrutture critiche?

Versione	1.0
Data	26 febbraio 2026
Classificazione	Pubblico

Autori	Tobias Castagna, Andreas Leisibach, Dilip Many, Fabio Zuber, Raphael M. Reischuk
Responsabile	Tobias Castagna

Indice

Ringraziamenti

Un ringraziamento particolare va a tutte le organizzazioni e agli esperti che hanno sostenuto questa indagine, sia mediante la messa a disposizione di dispositivi di test, sia attraverso la condivisione di esperienze sull'impiego di tali dispositivi in diversi contesti, sia mediante una partecipazione ai costi. Il loro impegno straordinario nel campo della cibersicurezza ha contribuito in modo determinante al successo di questa analisi di sicurezza. Tra questi figurano:

- Ufficio federale della cibersicurezza (UFCS)
- Ufficio federale delle comunicazioni (UFCOM)
- Ufficio federale della dogana e della sicurezza dei confini (UDSC)
- Cantone di Svitto
- Digitec Galaxus
- Redguard AG
- Zuger Kantonalbank
- altri istituti finanziari svizzeri (non menzionati per ragioni di discrezione)

1 Introduzione

Nel contesto lavorativo odierno, la sicurezza informatica non si limita al perimetro della rete. Mentre le organizzazioni investono ingenti risorse in misure di protezione quali firewall e protezione degli endpoint, una superficie di attacco facilmente accessibile nella pratica quotidiana viene spesso sottovalutata: i dispositivi periferici del posto di lavoro digitale.

Uno scenario reale illustra chiaramente il rischio: una videoconferenza riservata presso un operatore di infrastrutture critiche. La rete è protetta, la connessione è crittografata end-to-end, il server è rinforzato e il laptop è protetto. Ma l'attaccante punta a qualcos'altro: con un'antenna nel parcheggio vicino, intercetta le comunicazioni radio non crittografate del microfono da tavolo wireless. Dopo pochi secondi, la conversazione riservata viene intercettata: la sicurezza IT è stata compromessa da un dispositivo periferico non sicuro.

Il problema risiede in una pericolosa asimmetria: il costo di un'analisi di sicurezza professionale in grado di individuare tali rischi supera di molte volte il prezzo di acquisto di una webcam o di una tastiera. Nella pratica, i reparti IT fanno quindi spesso affidamento sulle dichiarazioni di sicurezza dei produttori.

Per valutare in modo sistematico il livello di sicurezza dei dispositivi periferici ampiamente utilizzati in Svizzera, l'Istituto nazionale di test per la cibersicurezza NTC ha condotto, nel corso di un anno, un'analisi tecnica approfondita della sicurezza di circa 30 dispositivi. La selezione si è concentrata intenzionalmente su prodotti di produttori affermati, ampiamente diffusi nelle organizzazioni svizzere, in particolare nelle infrastrutture critiche. Sono stati deliberatamente esclusi i prodotti a basso costo di origine sconosciuta.

Nel complesso sono stati individuati oltre 60 rilievi di diversa criticità, tra cui 13 classificati come gravi e tre al livello di criticità più elevato.

L'analisi dimostra che dispositivi periferici moderni e ben progettati – comprese le soluzioni wireless – possono in linea di principio raggiungere un elevato livello di sicurezza. Tuttavia, la sicurezza non dipende esclusivamente dai singoli componenti, bensì anche dalla scelta di configurazioni sicure e da regole chiaramente definite che disciplinano l'uso corretto di tali dispositivi. Ciò include processi organizzativi che garantiscono un esercizio sicuro, come l'installazione regolare degli aggiornamenti del firmware, nonché la chiarezza sulle ipotesi di base.

In particolare, gli operatori di infrastrutture critiche con requisiti di sicurezza elevati devono tenere conto di aggressori particolarmente motivati e dotati di risorse considerevoli. Questi possono utilizzare vettori e tecniche di attacco non convenzionali, poco comuni in altri contesti. Ad esempio, diverse cuffie wireless e sistemi di conferenza testati hanno potuto essere trasformati in dispositivi di intercettazione con uno sforzo minimo. Questi e altri rischi sono illustrati nel presente rapporto e affrontati mediante misure e raccomandazioni concrete.

I risultati dettagliati sono stati comunicati in modo confidenziale ai produttori interessati nell'ambito di un processo di divulgazione responsabile, al fine di consentire una rapida correzione delle vulnerabilità. Di conseguenza, il presente rapporto pubblico rinuncia deliberatamente alla divulgazione di dettagli tecnici e si concentra invece su schemi di rischio ricorrenti e sulle raccomandazioni che ne derivano.

L'analisi è stata condotta nell'ambito di un'iniziativa congiunta dell'Istituto nazionale di test per la cibersicurezza NTC, con il supporto di autorità federali e cantonali nonché di organizzazioni del settore finanziario. Per garantire l'indipendenza dei risultati, i produttori dei dispositivi testati non sono stati coinvolti né nella selezione né nello

svolgimento dei test e sono stati contattati solo al momento della comunicazione delle vulnerabilità.

Cinque misure raccomandate per una maggiore sicurezza

Sulla base dell'analisi di sicurezza effettuata, è possibile individuare cinque ambiti di intervento fondamentali per ridurre in modo efficace i rischi associati all'impiego dei dispositivi periferici:

Standardizzazione e approvvigionamento tramite canali affidabili
Si raccomanda di limitare la varietà dei dispositivi definendo un catalogo vincolante di periferiche testate e approvate. L'approvvigionamento dovrebbe avvenire esclusivamente tramite canali affidabili e autorizzati, al fine di ridurre il rischio di hardware manipolato e di attacchi alla catena di approvvigionamento (supply chain attacks).

Integrazione nella gestione del ciclo di vita
I dispositivi periferici non dovrebbero essere considerati semplici accessori, bensì componenti IT a pieno titolo. I dispositivi rilevanti sotto il profilo della sicurezza dovrebbero pertanto essere registrati nei sistemi di gestione degli asset e dovrebbero essere istituiti processi che garantiscano, ad esempio, l'installazione tempestiva degli aggiornamenti del firmware e la rapida sostituzione di hardware vulnerabile o giunto a fine ciclo di vita.

Segmentazione della rete
Per i sistemi dotati di connettività di rete, quali soluzioni di conferenza o dispositivi IoT, si raccomanda l'esercizio in segmenti di rete isolati. In questo modo si evita che tali dispositivi possano fungere da punto di ingresso nella rete aziendale interna in caso di compromissione.

Sicurezza fisica e sensibilizzazione
I collaboratori dovrebbero essere sensibilizzati a un utilizzo sicuro dei dispositivi periferici. Ciò include l'uso esclusivo di hardware approvato in contesti di telelavoro, nonché la consapevolezza dei rischi associati a dispositivi lasciati incustoditi, come dongle USB o cuffie wireless, in ambienti pubblici o semi-pubblici.

Soluzioni cablate nelle aree ad alta sicurezza
Negli ambienti con requisiti di protezione massimi, dovrebbero essere privilegiate soluzioni periferiche cablate. Le connessioni fisiche eliminano in larga misura i rischi legati alla trasmissione di segnali wireless e riducono in modo significativo la superficie di attacco.

I punti sopra elencati riassumono le raccomandazioni principali. Un'illustrazione dettagliata dei retroscena tecnici e delle misure specifiche è contenuta nel *capitolo 4 Raccomandazioni* del presente rapporto.

2 Contesto e metodologia

I dispositivi periferici sono molto più che semplici accessori: essi costituiscono l'interfaccia fisica tra l'essere umano e il computer e veicolano informazioni sensibili. Per esempio, tramite tastiere vengono immesse delle password, mentre conversazioni confidenziali vengono condotte attraverso microfoni e webcam. Se tali dispositivi sono insicuri o manipolati, possono fungere da porte di accesso per aggirare i meccanismi di sicurezza o essere usati come strumenti di intercettazione. Mentre i computer da lavoro tradizionali e gli smartphone sono sempre meglio protetti, i dispositivi periferici – spesso meno sicuri – rappresentano un rischio significativo e spesso non monitorato.

Due recenti incidenti evidenziano l'importanza di questo tema: nel 2025 sono state scoperte una serie di vulnerabilità[1] nei chip Bluetooth del produttore Airoha, ampiamente diffusi. Ciò consente agli attaccanti di dirottare la connessione Bluetooth e, ad esempio, di ascoltare di nascosto conversazioni riservate. I chip vulnerabili sono installati in dispositivi di marchi quali Bose, Jabra, JBL, Teufel, Sony e Marshall. Il carattere persistente di questo rischio è emerso nuovamente all'inizio del 2026, quando dei ricercatori hanno scoperto, sotto il nome «WhisperPair»[2], gravi lacune nell'implementazione del protocollo «Google Fast Pair». Queste permettono di prendere il controllo di cuffie di produttori come Google, Sony, Xiaomi e OnePlus senza alcuna interazione da parte dell'utente, consentendo l'ascolto delle conversazioni ambientali e il tracciamento della posizione tramite la rete «Find My Device». Tali eventi dimostrano che anche i prodotti di produttori rinomati non sono immuni da gravi errori di implementazione.

Nonostante il loro ruolo critico, le analisi di vulnerabilità dei dispositivi periferici vengono raramente eseguite. Le ragioni sono molteplici:

- **Mancanza di consapevolezza del rischio:** dispositivi come le tastiere sono spesso percepiti come hardware semplice e non autonomo. In realtà, oggi integrano processori propri, firmware e interfacce wireless, diventando parte integrante della superficie di attacco informatica.
- **Vincoli economici:** il costo di un'analisi di sicurezza professionale supera spesso di gran lunga il prezzo di acquisto dei dispositivi, creando un significativo squilibrio economico.
- **Diffusione delle responsabilità:** l'ampia diffusione dei dispositivi periferici genera spesso un falso senso di sicurezza. Molte organizzazioni presumono erroneamente che i prodotti più diffusi siano già stati verificati da terzi e che eventuali vulnerabilità gravi siano state corrette da tempo.
- **Perdita di controllo:** l'aumento del telelavoro e delle pratiche di tipo «bring your own device» (BYOD) ha portato a una varietà di dispositivi difficilmente gestibile, che spesso sfugge al controllo centralizzato dell'IT.

Per questi motivi, l'Istituto nazionale di test per la cibersicurezza NTC ha condotto una valutazione tecnica completa della sicurezza di circa 30 dispositivi periferici comunemente utilizzati. La selezione comprendeva dispositivi sia cablati sia wireless di produttori affermati come Logitech, Yealink, Jabra, HP, Eizo e Cherry, ampiamente impiegati nelle organizzazioni svizzere, in particolare nelle infrastrutture critiche. I

[1] Dettagli CVE: *https://www.airoha.com/product-security-bulletin/2025*;
Analisi: *https://insinuator.net/2025/06/airoha-bluetooth-security-vulnerabilities*
[2] CVE: CVE-2025-36911; Analisi: *https://whisperpair.eu*

dispositivi testati rientrano nelle seguenti categorie:

- **Tastiere e mouse**
- **Cuffie**
- **Webcam**
- **Docking station**
- **Sistemi di conferenza**

Le attività di test e il successivo processo di divulgazione responsabile con i produttori si sono estesi su un periodo di circa un anno. L'analisi è stata condotta da quattro esperti di test dell'Istituto nazionale di test per la cibersicurezza NTC, in collaborazione con diverse autorità federali e cantonali e con organizzazioni del settore finanziario.

Per garantire l'indipendenza dei risultati, i produttori dei dispositivi valutati non sono stati coinvolti né nella selezione né nell'acquisizione dei dispositivi, né nello svolgimento dei test. Essi sono stati contattati esclusivamente al momento della comunicazione delle vulnerabilità identificate.

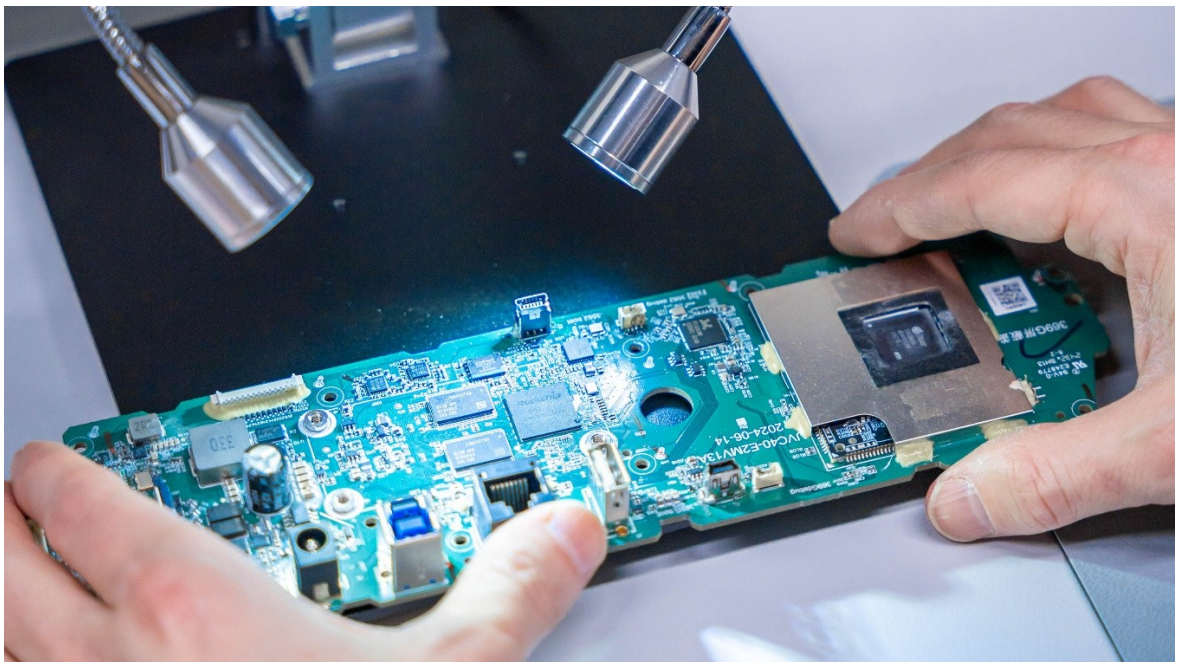

Figura 1: Ispezione visiva dei componenti integrati nei dispositivi periferici presso il laboratorio dell'Istituto nazionale di test per la cibersicurezza NTC a Zugo

Per poter formulare valutazioni fondate sui dispositivi esaminati, i test sono andati ben oltre le semplici verifiche funzionali. L'analisi è stata condotta in più fasi e ha incluso, tra l'altro, i seguenti metodi:

- **Analisi hardware:** i dispositivi sono stati aperti fisicamente per identificare i chip integrati. È stata verificata la presenza di interfacce di manutenzione aperte che avrebbero potuto consentire l'accesso al firmware, nonché di componenti nascosti o inattesi che potessero indicare una manipolazione nella catena di approvvigionamento.
- **Analisi del firmware:** il software dei dispositivi è stato estratto e analizzato mediante tecniche di reverse engineering, con l'obiettivo di individuare credenziali

codificate, backdoor, meccanismi di cifratura insicuri o l'assenza di controlli di integrità che consentissero l'installazione di aggiornamenti manipolati.

- **Analisi radio:** mediante l'intercettazione e l'analisi del traffico radio è stato verificato se la comunicazione tra il dispositivo periferico e la sua controparte (dongle/PC) fosse cifrata e protetta contro manipolazioni.
- **Analisi della configurazione e delle interfacce:** è stato verificato se le interfacce di gestione, le porte di diagnostica o protocolli di comunicazione aggiuntivi ampliassero inutilmente la superficie di attacco e se le impostazioni predefinite rispettassero il principio della sicurezza per impostazione predefinita (security by default).

3 Valutazione complessiva

La maggior parte dei prodotti di produttori noti presenta un livello di sicurezza da accettabile a buono, a condizione che siano configurati in modo sicuro e che il firmware sia mantenuto aggiornato. Tuttavia, nel corso dei test sono stati identificati oltre 60 rilievi, tra cui 13 gravi e tre classificati al livello di criticità più elevato. Le vulnerabilità sono state comunicate in modo confidenziale ai produttori nell'ambito del processo di divulgazione responsabile e sono state in larga misura corrette. Molti dei problemi individuati non si basano su metodi di attacco completamente nuovi, bensì su tecniche note. La possibilità di sfruttare queste vulnerabilità in scenari realistici sottolinea la necessità di agire.

Mentre i dispositivi di input tradizionali come mouse e tastiere sono spesso adeguatamente protetti grazie a standard moderni, i rischi aumentano sensibilmente quando i dispositivi diventano più complessi – ad esempio nel caso dei sistemi di conferenza e di altri dispositivi IoT – o quando vengono utilizzate tecnologie wireless obsolete.

Esempi rappresentativi di rilievi emersi dall'analisi includono:

Vulnerabilità critiche in EZCast Pro II
Il rilievo più grave riguarda il sistema di presentazione wireless *EZCast Pro II*. Gravi errori di progettazione danno luogo a vulnerabilità critiche: chiavi crittografiche codificate consentono l'accesso all'interfaccia di amministrazione e le password Wi-Fi possono essere derivate da identificativi osservabili pubblicamente. Un attaccante nel raggio di copertura radio può assumere il controllo completo del dispositivo e intercettare i contenuti dello schermo in forma non cifrata. Poiché il produttore non ha corretto le vulnerabilità entro i termini previsti, il caso è stato trasmesso all'Ufficio federale della cibersicurezza (UFCS), che ha emesso un avviso ai sensi dell'articolo 73c, capoverso 2, della legge sulla sicurezza delle informazioni (LSIn)[3].

Falsa sicurezza nella crittografia audio
Un sistema di conferenza verificato utilizza una trasmissione radio crittografata per la comunicazione con i microfoni. Tuttavia, la crittografia è così debole che un attaccante può violarla in pochi secondi e ascoltare le conversazioni.

Le cuffie come dispositivi di intercettazione
Diverse cuffie wireless supportano l'associazione simultanea con più dispositivi, come smartphone o computer, come funzionalità desiderata. Un attaccante che ottenga brevemente accesso fisico a una di queste cuffie – ad esempio durante un momento di distrazione su un treno o in occasione di una visita in ufficio – può associare un secondo dispositivo sotto il proprio controllo. In seguito, tutte le conversazioni nelle vicinanze della cuffia possono essere intercettate in modo occulto, a condizione che la cuffia non sia attivamente in uso (ad esempio in modalità standby o nella stazione di ricarica).

Questo esempio dimostra che le vulnerabilità non richiedono necessariamente tecniche di hacking sofisticate né competenze tecniche avanzate. Poiché si tratta di una funzionalità prevista, non esiste una patch software tradizionale. La mitigazione del rischio deve quindi essere realizzata tramite misure organizzative.

[3] *https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/cvd-cases/cvd-case-1-test.html*

«Tastiere fantasma» e attacchi di iniezione
Analogamente allo scenario delle cuffie, un attaccante può associare una «tastiera fantasma» aggiuntiva, invisibile per l'utente, al dongle USB collegato a una postazione di lavoro. Mediante questa tastiera fantasma è possibile inviare comandi al computer da distanze fino a 100 metri, come se l'attaccante fosse fisicamente presente. Ciò consente, ad esempio, l'iniezione di comandi malevoli o l'installazione e l'esecuzione di malware.

Manipolazione del firmware
Alcuni dispositivi consentono l'installazione di firmware privi di una firma digitale valida. Ciò permette agli attaccanti di distribuire firmware manipolati e di stabilire una persistenza duratura a livello hardware. Anche una reinstallazione del sistema operativo sul computer o sullo smartphone collegato non è in grado di eliminare tale compromissione. Questa categoria di vulnerabilità è inoltre responsabile del cosiddetto attacco «*BadCam*[4]», in cui una webcam con firmware modificato si presenta al PC come una tastiera.

Impostazioni predefinite non sicure
Un problema di ordine superiore è rappresentato dalla priorità data dai produttori alla comodità rispetto alla sicurezza. Molti dispositivi vengono forniti con impostazioni predefinite non sicure, come password standard o interfacce attivate inutilmente, per facilitare l'assistenza. Ciò offre agli aggressori inutili punti di attacco a favore del «plug-and-play».

[4] *https://eclypsium.com/blog/badcam-now-weaponizing-linux-webcams/*

4 Raccomandazioni

La protezione dei dispositivi periferici richiede un approccio multilivello che copra l'intero ciclo di vita, dall'approvvigionamento all'esercizio operativo fino alla sensibilizzazione del personale. Le seguenti raccomandazioni hanno lo scopo di aiutare le organizzazioni a ridurre in modo significativo la loro superficie di attacco con uno sforzo adeguato. Sebbene l'attuazione di queste misure sia generalmente consigliata a tutte le organizzazioni per garantire un solido livello di sicurezza di base, esse sono rivolte con particolare urgenza alle organizzazioni con esigenze di protezione elevate.

4.1 Approvvigionamento sicuro e standardizzazione

I rischi per la sicurezza causati da hardware non sicuro non possono solitamente essere risolti a posteriori con una «patch». Devono essere risolti al momento dell'approvvigionamento:

4.1.1 Protocolli e standard obsoleti

Sebbene molti produttori puntino su una crittografia collaudata, si riscontrano ripetutamente errori di implementazione. Attacchi noti come l'intercettazione dei comandi da tastiera (*KeySniffer*[5]) o l'iniezione di comandi da tastiera e mouse (*MouseJack*[6]) rappresentano ancora una minaccia, in particolare per dispositivi più vecchi ed economici.

Misure:

- **Preferenza per protocolli standard:** in linea generale, dovrebbero essere privilegiati protocolli standard aperti e ampiamente affermati, come Bluetooth nelle versioni più recenti, rispetto a protocolli proprietari non documentati. Gli standard vengono esaminati continuamente da una vasta comunità di esperti di sicurezza, riducendo la probabilità di vulnerabilità non individuate.
- **Vantaggi di sicurezza dei dongle dei produttori**: le organizzazioni prive di competenze approfondite nel campo delle comunicazioni radio dovrebbero generalmente fare affidamento sui dongle forniti dai produttori. Questi offrono spesso una configurazione di sicurezza più robusta rispetto alle impostazioni predefinite dei dispositivi periferici, poiché parametri critici come la cifratura vengono rafforzati già in fase di produzione. Le organizzazioni con requisiti di sicurezza elevati e competenze adeguate dovrebbero invece valutare se un rafforzamento personalizzato dei dispositivi periferici sia più appropriato, consapevoli che ciò richiede conoscenze tecniche approfondite e processi consolidati di configurazione e monitoraggio.

4.1.2 Rischi della catena di approvvigionamento e proliferazione dei dispositivi

L'uso non controllato di una vasta gamma di modelli di dispositivi («proliferazione dei dispositivi») rende praticamente impossibile una gestione efficace della sicurezza. Inoltre, sussiste il rischio che i dispositivi vengano manipolati già in fabbrica o durante il trasporto (attacchi alla catena di approvvigionamento).

[5] *https://keysniffer.net*
[6] *https://bastille.net/research/vulnerabilities-mousejack*

Misure:

- **Standardizzazione della selezione dei dispositivi:** si raccomanda di definire un catalogo vincolante di dispositivi periferici testati e approvati. Il rispetto coerente di tale catalogo – anche in contesti di telelavoro e mobilità – riduce la complessità e previene l'impiego di prodotti generici potenzialmente insicuri.
- **Selezione di fonti affidabili:** l'hardware dovrebbe essere acquistato esclusivamente tramite canali autorizzati di produttori affermati («Chain of Trust»). Ciò riduce in una certa misura il rischio di dispositivi manipolati.
- **Integrazione della sicurezza informatica nei processi di acquisto:** i requisiti di sicurezza (ad es. firmware firmato digitalmente, garanzie di aggiornamento) dovrebbero essere definiti come criteri obbligatori concreti e verificabili nei bandi di gara e nei contratti. Tali requisiti devono derivare dalle esigenze di protezione proprie dell'organizzazione e non devono essere sostituiti da valutazioni del rischio effettuate dai fornitori.

Come base tecnica è particolarmente indicato lo standard ETSI EN 303 645, che definisce requisiti minimi di sicurezza per i dispositivi connessi. La conformità dovrebbe essere dimostrata in modo trasparente dal fornitore (ad esempio mediante una matrice di conformità secondo l'allegato B).

4.1.3 Segnali wireless in aree ad alta sicurezza

Negli ambienti con requisiti di protezione massimi, le interfacce wireless rappresentano spesso un'estensione evitabile della superficie di attacco.

Misure:

- **Impiego di dispositivi cablati:** per le postazioni di lavoro con requisiti di sicurezza elevati, l'utilizzo di dispositivi periferici cablati quali tastiere, mouse e cuffie dovrebbe essere definito come standard. Le connessioni fisiche eliminano in larga misura i rischi legati alla trasmissione di segnali wireless.
- **Analisi di sicurezza indipendenti:** per ambiti di impiego particolarmente critici, si raccomanda di sottoporre regolarmente i dispositivi ad analisi di sicurezza indipendenti. Al fine di sfruttare le sinergie con l'analisi già condotta, l'Istituto nazionale di test per la cibersicurezza NTC può fornire indicazioni sull'eventuale inclusione di specifici dispositivi nel perimetro di test.

4.2 Esercizio e configurazione sicuri

Molte delle vulnerabilità individuate sono di natura tecnica, ma diventano critiche solo a causa di carenze organizzative.

4.2.1 Gestione del ciclo di vita e firmware

Nel corso dei test sono state individuate numerose vulnerabilità che nel frattempo sono state corrette dai produttori. Tuttavia, poiché i dispositivi periferici spesso non sono inclusi nella gestione centralizzata delle patch IT, gli aggiornamenti non raggiungono i dispositivi o lo fanno con notevole ritardo.

Misure:

- **Istituzione di processi di aggiornamento del firmware:** dovrebbe essere definito un processo per l'aggiornamento regolare del firmware dei dispositivi periferici,

analogo a quello adottato per i componenti IT tradizionali come server e computer portatili.
  - **Nota importante:** si raccomanda di valutare criticamente l'installazione permanente dei software di gestione dei produttori sui sistemi degli utenti finali, poiché tali software possono a loro volta aumentare la superficie di attacco. Ulteriori dettagli sono riportati nella sezione *4.2.3 Software dei produttori*.
- **Inventario degli asset:** i dispositivi periferici rilevanti ai fini della sicurezza dovrebbero essere registrati nei sistemi di gestione degli asset. Solo i dispositivi inventariati possono essere dismessi in modo affidabile, smaltiti in sicurezza e correttamente disaccoppiati al termine del ciclo di vita.

4.2.2 Rafforzamento dei sistemi e controllo delle interfacce

Molti dispositivi vengono forniti con interfacce aperte e servizi di comodità attivati («plug-and-play»), creando superfici di attacco inutili.

Misure:

- **Disattivazione delle interfacce non utilizzate**: si raccomanda di disattivare le interfacce non strettamente necessarie al funzionamento. Ciò è particolarmente rilevante per dispositivi più complessi come i sistemi di conferenza, dotati di numerose opzioni di connessione, e riguarda sia le porte fisiche (ad es. USB, Ethernet) sia le interfacce wireless (Wi-Fi, Bluetooth).
- **Disattivazione dei servizi non necessari:** funzioni di comodità come accessi di manutenzione remota, Telnet e protocolli di discovery dovrebbero essere disattivate su tutti i dispositivi, salvo che siano indispensabili per l'esercizio.

4.2.3 Software dei produttori

Gli strumenti di gestione completi forniti dai produttori vengono spesso eseguiti in modo permanente in background e aumentano la superficie di attacco sui sistemi client.

Misura:

- **Principio di minimalismo per il software dei produttori:** si raccomanda di valutare criticamente la necessità di installare software dei produttori sui sistemi degli utenti finali. In molti casi sono sufficienti i driver di base del sistema operativo. Qualora software aggiuntivo sia indispensabile, dovrebbe essere evitata l'esecuzione continua in background. Gli aggiornamenti del firmware dovrebbero invece essere effettuati tramite stazioni di aggiornamento dedicate gestite dal supporto IT, rendendo superflua l'installazione di software di gestione sui dispositivi degli utenti.

4.3 Associazione sicura dei dispositivi

Il processo di associazione (pairing) rappresenta una fase critica durante la quale gli attaccanti possono tentare di integrare i propri dispositivi in una connessione affidabile.

4.3.1 «Tastiere fantasma» e dispositivi di intercettazione

Per alcuni dispositivi è possibile che un attaccante si colleghi al dongle wireless di una vittima. Ciò richiede o un breve accesso fisico al dongle o lo sfruttamento di una vulnerabilità nel protocollo di associazione. In tal modo, una «tastiera fantasma» invisibile può iniettare comandi malevoli, oppure una cuffia non autorizzata può fungere

da dispositivo di intercettazione.

Misure:

- **Sensibilizzazione:** i collaboratori dovrebbero essere sensibilizzati a non lasciare incustoditi dispositivi periferici mobili (ad es. dongle USB e cuffie) in luoghi pubblici.
- **Limitazione delle possibilità di associazione:** laddove tecnicamente possibile, i dongle dovrebbero essere bloccati via software dopo l'associazione iniziale, al fine di impedire l'aggiunta successiva di dispositivi non autorizzati. Va tuttavia considerato che questa misura è spesso difficile da implementare nella pratica.
- **Utilizzo in ambienti pubblici:** in contesti non controllati, come treni o caffè, si raccomanda di utilizzare esclusivamente dispositivi che escludano tecnicamente associazioni non autorizzate (ad esempio tramite soluzioni cablate).

4.4 Infrastrutture e sale conferenze

Poiché durante i test i dispositivi multimediali complessi hanno mostrato con particolare frequenza carenze critiche, le seguenti raccomandazioni aggiuntive rivestono un'importanza speciale per questa categoria di dispositivi.

4.4.1 Vulnerabilità critiche nei dispositivi IoT

Come dimostrato dal caso del sistema di presentazione EZCast, le vulnerabilità nei sistemi di conferenza possono consentire l'intercettazione occulta dei contenuti dello schermo o la compromissione completa del sistema.

Misura:

- **Separazione delle reti:** i dispositivi dotati di una propria connettività di rete, come i dispositivi IoT, i sistemi di videoconferenza e le soluzioni di presentazione wireless, dovrebbero essere utilizzati in segmenti di rete isolati. Deve essere garantito che tali dispositivi non abbiano accesso diretto alla rete interna dell'organizzazione.

4.5 Prospettive normative

Mentre i nuovi requisiti di cibersicurezza della **Radio Equipment Directive (RED)** sono in vigore dall'agosto 2025 e impongono ai produttori un rafforzamento delle misure di sicurezza, il futuro **Cyber Resilience Act (CRA)** rafforzerà ulteriormente tali obblighi. Esso prevede, tra l'altro, il principio della sicurezza fin dalla progettazione (security by design) e l'obbligo di fornire aggiornamenti di sicurezza per l'intero ciclo di vita dei prodotti digitali.

Tuttavia, sarà necessario del tempo affinché queste normative si affermino pienamente sul mercato. Le organizzazioni non dovrebbero quindi attendere, ma già oggi esigere dai propri fornitori trasparenza e impegni contrattuali vincolanti in materia di cibersicurezza.