

COMUNICATO STAMPA

Rapporto di sintesi sulla cibersecurity dei dispositivi periferici

Rischio sottovalutato: come tastiere, cuffie e altri dispositivi possono diventare una porta d'accesso ai sistemi critici

Zugo, 26 febbraio 2026 – Un'analisi tecnica approfondita condotta dall'Istituto nazionale di test per la cibersecurity NTC dimostra che i dispositivi periferici utilizzati sul posto di lavoro digitale rappresentano una superficie di attacco spesso sottovalutata. Sono state testate circa 30 tastiere, cuffie, webcam e sistemi di conferenza ampiamente diffusi in Svizzera, prodotti da fabbricanti affermati – dispositivi presenti praticamente su ogni scrivania in Svizzera. L'NTC ha identificato oltre 60 vulnerabilità, tra cui 13 gravi e tre critiche. Le vulnerabilità sono state segnalate ai fabbricanti e sono state in gran parte corrette.

Un esempio concreto illustra la natura di questi rischi: durante una videoconferenza riservata presso un gestore di infrastrutture critiche, la rete, il server e il laptop sono aggiornati secondo i più recenti standard di sicurezza e la connessione è cifrata end-to-end. Tuttavia, un attacco è comunque possibile. Con un'antenna posizionata in un parcheggio nelle vicinanze, un attaccante intercetta la comunicazione radio insufficientemente protetta di un microfono da tavolo senza fili. Nel giro di pochi secondi può ascoltare la conversazione riservata.

In questo modo, le misure di protezione esistenti possono essere aggirate attraverso un dispositivo periferico non sicuro. I dispositivi periferici costituiscono un'interfaccia critica attraverso la quale transitano informazioni sensibili: le tastiere elaborano password, mentre microfoni e webcam trasmettono conversazioni riservate. Emerge una pericolosa asimmetria: i costi delle analisi di sicurezza professionali superano spesso di gran lunga il prezzo di acquisto di tali dispositivi. «Nella pratica, i dispositivi periferici sono spesso considerati semplici accessori e, di conseguenza, non vengono sottoposti a verifiche sistematiche né integrati in modo coerente nei concetti di sicurezza esistenti», afferma Tobias Castagna, responsabile degli esperti di test presso l'NTC.

Risultati dell'analisi di sicurezza e principali schemi di rischio

Per valutare in modo sistematico il livello di sicurezza dei dispositivi periferici ampiamente utilizzati in Svizzera, l'NTC ha sottoposto circa 30 dispositivi cablati e wireless a un'analisi tecnica approfondita nell'arco di un anno. La selezione comprendeva prodotti di fabbricanti affermati quali Logitech, Yealink, Jabra, HP, Eizo o Cherry, largamente impiegati in Svizzera e in particolare nelle infrastrutture critiche.

Complessivamente sono stati individuati oltre 60 rilievi di diversa criticità, tra cui 13 gravi e tre con il livello di criticità più elevato. Diverse vulnerabilità possono essere sfruttate in scenari realistici mediante tecniche di attacco note. L'analisi mostra tuttavia che dispositivi periferici moderni, se configurati in modo sicuro e con firmware aggiornato, possono raggiungere un livello di sicurezza accettabile. I rischi aumentano però con la crescente complessità dei dispositivi, ad esempio nei sistemi di conferenza o in altri dispositivi di tipo IoT, nonché in caso di utilizzo di tecnologie radio obsolete.

Le vulnerabilità individuate sono state segnalate ai fabbricanti interessati e sono state in larga misura corrette tempestivamente. In un caso, tuttavia, un fabbricante non ha reagito: per un sistema di presentazione wireless, l'NTC ha trasmesso il caso all'Ufficio federale della cibersecurity (UFCS), che ha successivamente pubblicato un avviso pubblico.

Il rapporto pubblico rinuncia deliberatamente alla divulgazione di dettagli tecnici o vulnerabilità specifiche di prodotti. Vengono invece evidenziati schemi di rischio trasversali, tra cui impostazioni predefinite non sicure, debolezze nei processi di accoppiamento dei dispositivi, comunicazioni radio insufficientemente protette nonché carenze nella gestione del firmware e del ciclo di vita. L'analisi dimostra che la sicurezza dei dispositivi periferici non dipende esclusivamente dal prodotto in sé, ma in misura determinante dalla configurazione, dall'esercizio e da chiare disposizioni organizzative.

Raccomandazioni per la riduzione dei rischi

Sulla base dei risultati, l'NTC formula cinque raccomandazioni generali per ridurre i rischi connessi all'impiego dei dispositivi periferici, in particolare per gli operatori di infrastrutture critiche e le organizzazioni con requisiti di sicurezza elevati:

- Standardizzazione e approvvigionamento sicuro tramite canali affidabili
- Integrazione dei dispositivi periferici nella gestione del ciclo di vita e degli asset IT
- Segmentazione della rete per dispositivi connessi alla rete come i sistemi di conferenza
- Preferenza per soluzioni cablate in ambienti con esigenze di protezione elevate
- Sensibilizzazione del personale ai rischi fisici e organizzativi

L'attuazione di tali misure consente alle organizzazioni di ridurre in modo significativo la propria superficie di attacco con un impegno proporzionato.

L'analisi è stata condotta nell'ambito di un'iniziativa congiunta dell'Istituto nazionale di test per la cibersecurity NTC, con il sostegno di autorità federali e cantonali nonché di organizzazioni del settore finanziario. Per garantire l'indipendenza dei risultati, i fabbricanti dei dispositivi testati non sono stati coinvolti né nella selezione né nell'esecuzione dei test e sono stati contattati esclusivamente nell'ambito della segnalazione confidenziale delle vulnerabilità al fine di consentirne la tempestiva correzione.

[Rapporto di sintesi](#)

Contatto media:

Andreas W. Kaelin, Direttore Esecutivo
+41 41 317 00 11, andreas.kaelin@ntc.swiss

Informazioni sull'Istituto nazionale di test per la cibersecurity NTC

L'Istituto nazionale di test per la cibersecurity NTC contribuisce alla sicurezza e alla sovranità digitale della Svizzera, individuando in modo proattivo le vulnerabilità critiche dei prodotti digitali e i rischi delle nuove tecnologie digitali e sostenendo la loro mitigazione. In qualità di associazione senza scopo di lucro con sede a Zugo, l'NTC si basa sui principi di indipendenza e obiettività. L'NTC esegue autonomamente test su prodotti e applicazioni digitali che non sono stati sottoposti a sufficienti controlli in Svizzera, ma che rivestono un'importanza cruciale per l'economia e la società. L'NTC esegue inoltre controlli di cibersecurity per conto di gestori di infrastrutture critiche e autorità. <https://it.ntc.swiss>