



COMMUNIQUÉ DE PRESSE

Rapport de synthèse sur la cybersécurité des périphériques

Un risque sous-estimé: comment claviers, casques et autres périphériques peuvent devenir une porte d'entrée vers des systèmes critiques

Zoug, le 26 février 2026 – Une analyse technique approfondie menée par l'Institut national de test pour la cybersécurité NTC montre que les périphériques utilisés sur les postes de travail numériques constituent une surface d'attaque souvent sous-estimée. Environ 30 claviers, casques, webcams et systèmes de conférence largement répandus en Suisse ont été testés – des appareils que l'on retrouve sur chaque bureau en Suisse ou presque. Le NTC a identifié plus de 60 vulnérabilités, dont 13 graves et 3 critiques. Après signalement aux fabricants, ces vulnérabilités ont été en grande partie corrigées.

Un scénario concret illustre ces risques: lors d'une visioconférence confidentielle chez un exploitant d'infrastructure critique, le réseau, le serveur et l'ordinateur portable sont à jour sur le plan de la sécurité et la connexion est chiffrée de bout en bout. Une attaque reste néanmoins possible: à l'aide d'une antenne depuis un parking voisin, un attaquant intercepte la communication radio insuffisamment protégée d'un micro de table sans fil. En quelques secondes, la conversation confidentielle peut être écoutée.

Ainsi, les mesures de protection existantes peuvent être contournées via un périphérique non sécurisé. Les périphériques constituent une interface critique par laquelle transitent des informations sensibles: les claviers traitent des mots de passe, les micros et webcams transmettent des conversations confidentielles. Une asymétrie préoccupante apparaît alors: les coûts d'analyses de sécurité professionnelles dépassent souvent largement le prix d'achat de ces appareils. «Dans la pratique, les périphériques sont souvent considérés comme de simples accessoires et, par conséquent, ne sont ni systématiquement testés ni intégrés de manière cohérente aux concepts de sécurité existants», déclare Tobias Castagna, responsable des experts en tests au sein du NTC.

Résultats de l'analyse de sécurité et principaux schémas de risques

Afin d'évaluer de manière systématique le niveau de sécurité des périphériques largement utilisés en Suisse, le NTC a soumis environ 30 appareils filaires et sans fil à une analyse technique approfondie pendant une année. La sélection comprenait des produits de fabricants établis tels que Logitech, Yealink, Jabra, HP, Eizo ou Cherry, largement utilisés en Suisse et notamment dans les infrastructures critiques.

Au total, plus de 60 constats de différents niveaux de criticité ont été identifiés, dont 13 graves et 3 du niveau de criticité le plus élevé. Plusieurs vulnérabilités peuvent être exploitées dans des scénarios réalistes à l'aide de méthodes d'attaque connues. L'analyse montre toutefois que des périphériques modernes, correctement configurés et dotés d'un firmware à jour, peuvent atteindre un niveau de sécurité acceptable. Les risques augmentent néanmoins avec la complexité des appareils, notamment pour les systèmes de conférence ou autres dispositifs de type IoT, ainsi qu'en cas d'utilisation de technologies radio obsolètes.

Les vulnérabilités identifiées ont été signalées aux fabricants concernés et ont été majoritairement corrigées rapidement. Dans un cas, un fabricant n'a toutefois pas réagi: pour un système de présentation sans fil, le NTC a transmis le cas à l'Office fédéral de la cybersécurité (OFCS), qui a ensuite publié un avertissement public.

Il a délibérément été décidé de ne pas publier dans le rapport public de détails techniques ni de vulnérabilités spécifiques à des produits. Le rapport met en évidence des schémas de risques transversaux, notamment des paramètres par défaut non sécurisés, des faiblesses dans les processus d'appairage, des communications radio insuffisamment protégées ainsi que des lacunes dans la gestion du firmware et du cycle de vie. L'analyse montre que la sécurité des périphériques dépend non seulement du produit lui-même, mais aussi de sa configuration, de son exploitation et de cadres organisationnels clairs.

Recommandations pour réduire les risques

Sur la base des résultats, le NTC formule cinq recommandations générales pour réduire les risques liés à l'utilisation des périphériques, en particulier pour les exploitants d'infrastructures critiques et les organisations ayant des exigences de sécurité élevées:

- Standardisation et approvisionnement sécurisé via des canaux fiables
- Intégration des périphériques dans la gestion du cycle de vie et des actifs IT
- Segmentation réseau pour les appareils connectés tels que les systèmes de conférence
- Priorité aux solutions filaires dans les environnements à besoins de protection élevés
- Sensibilisation du personnel aux risques physiques et organisationnels

La mise en œuvre de ces mesures permet aux organisations de réduire significativement leur surface d'attaque avec des moyens proportionnés.

L'analyse a été menée dans le cadre d'une initiative conjointe de l'Institut national de test pour la cybersécurité NTC avec le soutien d'autorités fédérales et cantonales ainsi que d'organisations du secteur financier. Afin de garantir l'indépendance des résultats, les fabricants des appareils testés n'ont été impliqués ni dans la sélection ni dans la réalisation des tests et ont été contactés uniquement dans le cadre du signalement confidentiel des vulnérabilités en vue de leur correction.

[Rapport de synthèse](#)

Contact médias:

Andreas W. Kaelin, Directeur

+41 41 317 00 11, andreas.kaelin@ntc.swiss

À propos de l'Institut national de test pour la cybersécurité NTC

L'Institut national de test pour la cybersécurité NTC contribue à la sécurité et à la souveraineté numérique de la Suisse en identifiant de manière anticipée les vulnérabilités critiques des produits numériques et les risques des nouvelles technologies numériques et en soutenant leur atténuation. En tant qu'association à but non lucratif dont le siège est à Zoug, le NTC repose sur des principes d'indépendance et d'objectivité. Le NTC vérifie, de sa propre initiative, la conformité des produits et applications numériques qui n'ont pas été suffisamment testés en Suisse, mais qui revêtent une grande importance pour l'économie et la société. Le NTC réalise également des audits de cybersécurité pour le compte d'exploitants d'infrastructures critiques et d'autorités publiques.

<https://fr.ntc.swiss>