



COMMUNIQUÉ DE PRESSE

Rapport de synthèse sur la cybersécurité des appareils connectés au regard de la nouvelle directive RED

De nombreux appareils connectés ne sont pas conformes à la nouvelle directive de sécurité – des interdictions de commercialisation risquent d’être imposées à partir d’août 2025

Zoug, le 22 mai 2025 – Le 1^{er} août 2025, des dispositions plus strictes de la Radio Equipment Directive (RED), également applicables en Suisse, entreront en vigueur. Celles-ci définissent de nouvelles exigences en matière de cybersécurité pour les appareils connectés dotés d’une interface radio, tels que les montres connectées, les routeurs WLAN et les babyphones avec caméra. Un rapport récent de l’Institut national de test pour la cybersécurité NTC révèle qu’un nombre important des produits testés ne répond actuellement pas aux nouvelles exigences. Le NTC préconise donc des mesures d’urgence sur toute la chaîne d’approvisionnement.

L’étude portait sur des appareils largement répandus dans le commerce suisse, notamment des montres connectées pour enfants, des babyphones avec caméra, des systèmes d’alarme, des routeurs WLAN et des adaptateurs de prises intelligents. Dans le cadre de cette analyse, les appareils ont été testés à titre d’exemple eu égard à certaines exigences de la directive RED. L’accent a été mis sur les aspects particulièrement importants pour la sécurité et la résilience des appareils: l’authentification et le contrôle d’accès, la communication protégée des données, les mises à jour sécurisées des logiciels ainsi que la protection contre la manipulation et les accès non autorisés. L’objectif était de déterminer si les produits testés répondaient aux exigences de cybersécurité applicables à partir d’août 2025.

Résultats de l’échantillon

L’analyse technique met en évidence des vulnérabilités courantes, telles que des mots de passe par défaut non sécurisés, un cryptage inexistant ou insuffisant lors de la transmission des données, ainsi que des mécanismes défaillants ou inexistantes pour les mises à jour logicielles. Ces failles ont été constatées non seulement sur des produits d’importation à bas prix, mais aussi sur des appareils de fabricants de marques bien implantées. Les vulnérabilités identifiées révèlent une surface d’attaque nettement plus importante, le fait que certaines de ces failles de sécurité puissent être exploitées sans connaissances techniques approfondies soulevant notamment de vives inquiétudes. Les appareils présentant de tels défauts seront à l’avenir considérés comme non conformes à la norme RED et ne pourront plus être mis sur le marché à partir d’août 2025.

Les nouvelles exigences permettront de disposer de produits plus sûrs à long terme. Toutefois, les résultats de cette analyse soulèvent des doutes quant à la possibilité que la directive soit mise en œuvre de manière généralisée et en temps utile.

Recommandations aux acteurs du marché

Le NTC recommande aux fabricants de mettre en œuvre les exigences applicables de la directive RED en matière de cybersécurité de manière systématique et le plus tôt possible. La cybersécurité doit faire partie intégrante du processus de développement, selon le principe de la «Security by Design». Il est recommandé aux importateurs et aux distributeurs d’exiger systématiquement des preuves de conformité auprès de leurs fournisseurs et de sélectionner les produits avec soin. Les consommatrices et consommateurs peuvent eux aussi contribuer à leur propre sécurité en faisant leurs achats chez des distributeurs bien établis en Suisse, en faisant preuve de prudence lors d’importations directes, en changeant immédiatement les mots de passe par défaut et en installant régulièrement les mises à jour.

[Management Summary](#)

[Rapport de synthèse \(en anglais\)](#)

[Rapport de synthèse \(en allemand\)](#)

Contact presse:

Andreas W. Kaelin, Directeur général

+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://www.ntc.swiss>