Institut national de test pour la cybersécurité

Cybersécurité des périphériques

Risques cachés au bureau: les claviers sans fil, casques et autres périphériques similaires sont-ils suffisamment sûrs pour être utilisés dans les infrastructures critiques?

Version	1.0
Date	26 février 2026
Classification	Public
Auteurs	Tobias Castagna, Andreas Leisibach, Dilip Many, Fabio Zuber, Raphael M. Reischuk
Responsable	Tobias Castagna

Sommaire

Remerciements

Nous adressons nos remerciements particuliers à toutes les organisations et à tous les experts qui ont soutenu cette étude, que ce soit par la mise à disposition d'appareils de test, par le partage d'expériences concernant l'utilisation de ce type d'appareils dans différents environnements ou par une participation aux coûts. Leur engagement remarquable en matière de cybersécurité a contribué de manière décisive à la réussite de cette analyse de sécurité. Il s'agit notamment des partenaires suivants:

- Office fédéral de la cybersécurité (OFCS)
- Office fédéral de la communication (OFCOM)
- Office fédéral de la douane et de la sécurité des frontières (OFDF)
- Canton de Schwytz
- Digitec Galaxus
- Redguard AG
- Banque cantonale de Zoug
- d'autres établissements financiers suisses (non cités pour des raisons de discrétion)

1 Introduction

Dans l'environnement de travail actuel, la sécurité informatique ne s'arrête pas au périmètre du réseau. Alors que les organisations investissent massivement dans des mesures de protection telles que les pare-feu et la protection des terminaux, une surface d'attaque pourtant facilement accessible est souvent sous-estimée dans la pratique quotidienne: les périphériques du poste de travail numérique.

Voici un scénario réaliste qui illustre ce risque: une visioconférence confidentielle chez un exploitant d'infrastructures critiques. Le réseau est sécurisé, la connexion est chiffrée de bout en bout, le serveur est durci et l'ordinateur portable est protégé. Pourtant, l'attaquant vise un autre élément. À l'aide d'une antenne depuis un parking à proximité, il intercepte le trafic radio non chiffré d'un microphone de table sans fil. En quelques secondes, la conversation confidentielle est écoutée clandestinement – la sécurité informatique a été compromise par un périphérique insuffisamment sécurisé.

Le problème repose sur une asymétrie dangereuse: le coût d'une analyse de sécurité professionnelle permettant d'identifier de tels risques dépasse de plusieurs fois le prix d'achat d'une webcam ou d'un clavier. Dans la pratique, les services informatiques s'en remettent donc souvent aux promesses de sécurité des fabricants.

Afin d'évaluer de manière systématique le niveau de sécurité des périphériques largement utilisés en Suisse, l'Institut national de test pour la cybersécurité NTC a mené, sur une période d'un an, une analyse technique approfondie de la sécurité d'environ 30 appareils. La sélection s'est volontairement concentrée sur des produits de fabricants établis, largement déployés dans les organisations suisses et en particulier dans les infrastructures critiques. Les produits à bas coût d'origine inconnue ont été délibérément exclus.

Au total, plus de 60 constats de niveaux de criticité variables ont été dressés, dont 13 jugés graves et trois classés au niveau de criticité le plus élevé.

L'analyse montre que des périphériques modernes et bien conçus – y compris des solutions sans fil – peuvent en principe atteindre un niveau de sécurité élevé. Toutefois, la sécurité ne dépend pas uniquement des composants individuels, mais aussi du choix d'une configuration sécurisée et de règles clairement définies encadrant l'utilisation sûre de ces appareils. Cela inclut des processus organisationnels garantissant une exploitation sécurisée, tels que l'application régulière des mises à jour de micrologiciel, ainsi qu'une clarification des hypothèses sous-jacentes.

Les exploitants d'infrastructures critiques présentant des exigences de sécurité accrues doivent en particulier s'attendre à faire face à des assaillants très motivés et disposant de ressources importantes. Ceux-ci peuvent recourir à des vecteurs et techniques d'attaque non conventionnels, peu courants dans d'autres contextes. Ainsi, plusieurs casques sans fil et systèmes de conférence testés ont pu être transformés en dispositifs d'écoute avec un effort minime. Ces risques et d'autres sont expliqués dans le présent rapport et traités au moyen de mesures et de recommandations concrètes.

Les constats détaillés ont été transmis de manière confidentielle aux fabricants concernés dans le cadre d'un processus de divulgation responsable, afin de permettre une correction rapide des vulnérabilités. En conséquence, le présent rapport public renonce délibérément à la divulgation de détails techniques et se concentre sur des schémas de risques récurrents ainsi que sur les recommandations qui en découlent.

L'analyse a été réalisée 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 n'ont été contactés qu'au moment de la communication des vulnérabilités.

Cinq mesures recommandées pour renforcer la sécurité

Sur la base de l'analyse de sécurité réalisée, cinq axes d'action fondamentaux peuvent être identifiés afin de réduire efficacement les risques liés à l'utilisation de périphériques:

Standardisation et approvisionnement via des canaux de confiance
Il est recommandé de limiter la diversité des appareils en définissant un catalogue contraignant de périphériques testés et approuvés. L'approvisionnement devrait s'effectuer exclusivement via des canaux de confiance et autorisés, afin de réduire le risque de manipulation des appareils et d'attaques sur la chaîne d'approvisionnement.

Intégration dans la gestion du cycle de vie
Les périphériques ne doivent pas être considérés comme de simples accessoires, mais comme des composants informatiques à part entière. Les appareils pertinents pour la sécurité devraient dès lors être enregistrés dans la gestion des actifs, et des processus devraient être mis en place afin de garantir, par exemple, l'application rapide des mises à jour de micrologiciel et le remplacement des matériels vulnérables ou en fin de vie.

Segmentation du réseau
Pour les systèmes disposant d'une connectivité réseau, tels que les solutions de conférence ou les appareils IoT, il est recommandé de les exploiter dans des segments de réseau isolés. Cela empêche que ces appareils ne servent de point d'entrée vers le réseau interne de l'organisation en cas de compromission.

Sécurité physique et sensibilisation
Le personnel doit être sensibilisé à la gestion sécurisée des périphériques. Cela inclut l'utilisation exclusive de matériel approuvé en télétravail ainsi qu'une prise de conscience des risques liés aux appareils laissés sans surveillance, tels que les dongles USB ou les casques sans fil, dans les espaces publics ou semi-publics.

Solutions filaires dans les zones à haute sécurité
Dans les environnements présentant des exigences de protection maximales, les périphériques filaires doivent être privilégiés. Les connexions physiques éliminent en grande partie les risques liés à la transmission de signaux sans fil et réduisent significativement la surface d'attaque.

Ces points résument les principales recommandations. Une analyse détaillée des aspects techniques et des mesures spécifiques figure au *chapitre 4, Recommandations*, du présent rapport.

2 Contexte et méthodologie

Les périphériques sont bien plus que de simples accessoires: ils constituent l'interface physique entre l'être humain et l'ordinateur, et des informations sensibles transitent par leur intermédiaire. Les claviers servent à saisir des mots de passe, tandis que les microphones et webcams permettent de transmettre des conversations confidentielles. Lorsqu'ils sont insuffisamment sécurisés ou manipulés, ces appareils peuvent servir de points d'entrée pour contourner des mécanismes de sécurité ou être détournés à des fins d'écoute clandestine. Alors que les postes de travail classiques et les smartphones bénéficient d'une protection croissante, les périphériques – souvent moins bien sécurisés – représentent un risque significatif et fréquemment non surveillé.

Deux incidents récents illustrent la pertinence de cette problématique. En 2025, une série de vulnérabilités[1] a été rendue publique dans des puces Bluetooth largement utilisées, fabriquées par Airoha. Ces failles permettent à des attaquants de détourner des connexions Bluetooth et, par exemple, d'écouter discrètement des conversations confidentielles. Les puces concernées sont intégrées à des appareils de marques telles que Bose, Jabra, JBL, Teufel, Sony et Marshall. Le caractère persistant de ce risque est apparu de nouveau début 2026, lorsque des chercheurs ont mis au jour, sous le nom de «WhisperPair»[2], de graves failles dans l'implémentation du protocole «Google Fast Pair». Celles-ci permettent de prendre le contrôle de casques de fabricants tels que Google, Sony, Xiaomi et OnePlus sans aucune interaction de l'utilisateur, rendant possible l'écoute de conversations ambiantes et le suivi de la localisation via le réseau «Find My Device». Ces incidents montrent que même des produits de fabricants renommés ne sont pas à l'abri d'erreurs d'implémentation critiques.

Malgré leur rôle central, les analyses de vulnérabilités portant sur les périphériques sont rares. Les raisons en sont multiples:

- **Manque de sensibilisation aux risques:** les périphériques tels que les claviers sont souvent perçus comme du matériel simple et non autonome. En réalité, ils intègrent aujourd'hui leurs propres processeurs, micrologiciels et interfaces sans fil, et font donc partie intégrante de la surface d'attaque informatique.
- **Contraintes économiques:** le coût d'une analyse de sécurité professionnelle dépasse souvent de plusieurs fois le prix d'achat de ces appareils, créant un déséquilibre économique important.
- **Dilution des responsabilités:** la large diffusion des périphériques engendre fréquemment un faux sentiment de sécurité. De nombreuses organisations partent du principe erroné que les produits populaires, en raison de leur forte pénétration du marché, ont déjà été examinés par des tiers et que les failles graves auraient été corrigées depuis longtemps.
- **Perte de contrôle:** l'essor du télétravail et des pratiques de type «bring your own device» (BYOD) a conduit à une diversité d'appareils difficilement maîtrisable, échappant souvent au contrôle centralisé des services informatiques.

Pour ces raisons, l'Institut national de test pour la cybersécurité NTC a mené une évaluation technique approfondie de la sécurité d'environ 30 périphériques couramment utilisés. La sélection comprenait aussi bien des appareils filaires que sans fil de fabricants établis tels que Logitech, Yealink, Jabra, HP, Eizo ou Cherry – des dispositifs largement

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

déployés dans les organisations suisses, en particulier dans les infrastructures critiques. Les appareils testés relevaient des catégories suivantes:

- **Claviers et souris**
- **Casques**
- **Webcams**
- **Stations d'accueil**
- **Systèmes de conférence**

Les tests ainsi que le processus de divulgation responsable mené avec les fabricants se sont étendus sur une période d'environ un an. L'analyse a été réalisée par quatre experts en test de l'Institut national de test pour la cybersécurité NTC, en collaboration avec plusieurs autorités fédérales et cantonales ainsi qu'avec des organisations du secteur financier.

Afin de garantir l'indépendance des résultats, les fabricants des appareils évalués n'ont été impliqués ni dans la sélection, ni dans l'acquisition, ni dans la réalisation des tests. Ils n'ont été contactés qu'au moment de la communication des vulnérabilités identifiées.

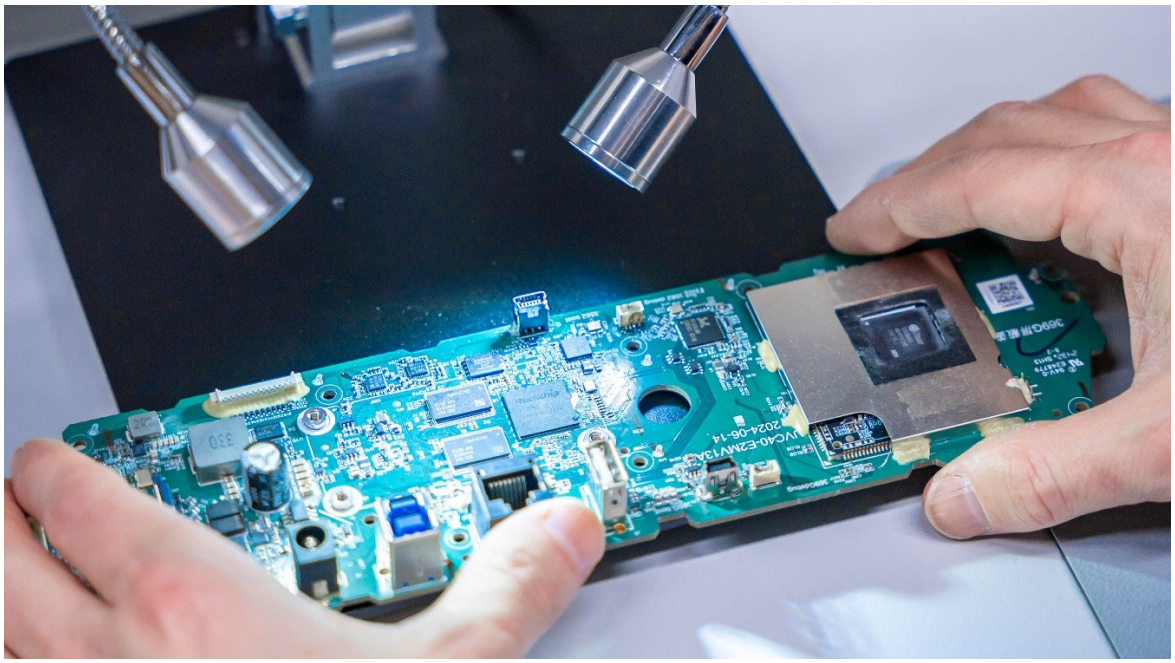

Figure 1: Inspection visuelle des composants intégrés dans les périphériques au laboratoire de l'Institut national de test pour la cybersécurité NTC à Zoug

Pour pouvoir formuler des conclusions solides concernant les appareils évalués, les tests sont allés bien au-delà de simples vérifications fonctionnelles. L'analyse s'est déroulée en plusieurs étapes et a notamment fait appel aux méthodes suivantes:

- **Analyse hardware:** les appareils ont été ouverts physiquement afin d'identifier les puces intégrées. Les experts ont recherché des interfaces de maintenance ouvertes susceptibles de permettre un accès non autorisé au micrologiciel, ainsi que des composants cachés ou inattendus pouvant indiquer une manipulation au niveau de la chaîne d'approvisionnement.

- **Analyse du micrologiciel:** le logiciel embarqué a été extrait et examiné au moyen de techniques de rétro-ingénierie. L'objectif était notamment d'identifier des mots de passe codés en dur, des portes dérobées, des mécanismes de chiffrement faibles ou l'absence de contrôles d'intégrité permettant l'installation de mises à jour manipulées.
- **Analyse des communications radio:** une interception et une analyse du trafic radio ont permis de déterminer si la communication entre le périphérique et sa contrepartie (dongle ou PC) était chiffrée et protégée contre les manipulations.
- **Analyse de la configuration et des interfaces:** l'analyse a porté sur les interfaces de gestion, les ports de diagnostic et les protocoles de communication supplémentaires, afin de déterminer s'ils augmentaient inutilement la surface d'attaque et si les paramètres par défaut respectaient le principe de la sécurité par défaut (security by default).

3 Évaluation globale

La majorité des produits de fabricants reconnus présentent un niveau de sécurité acceptable à bon, pour autant qu'ils soient configurés de manière sécurisée et que leur micrologiciel soit maintenu à jour. Néanmoins, plus de 60 constats ont été dressés dans le cadre des tests, dont 13 jugés graves et trois classés au niveau de criticité le plus élevé. Les vulnérabilités ont été communiquées de manière confidentielle aux fabricants dans le cadre du processus de divulgation responsable et ont, pour la plupart, été corrigées par ces derniers. Un grand nombre des failles identifiées ne reposent pas sur des méthodes d'attaque inédites, mais sur des techniques bien connues. Leur exploitabilité dans des scénarios réalistes souligne la nécessité d'agir.

Alors que les périphériques d'entrée classiques tels que les souris ou les claviers sont souvent correctement sécurisés grâce à des normes modernes, les risques augmentent sensiblement dès que les appareils gagnent en complexité – par exemple dans le cas des systèmes de conférence et d'autres appareils IoT – ou lorsque des technologies radio obsolètes sont utilisées.

Voici quelques exemples représentatifs de constats issus de l'analyse:

Vulnérabilités critiques dans EZCast Pro II
Le constat le plus grave concerne le système de présentation sans fil *EZCast Pro II*. De graves erreurs de conception entraînent des vulnérabilités critiques: des clés cryptographiques codées en dur permettent l'accès à l'interface d'administration et les mots de passe Wi-Fi peuvent être déduits à partir d'identifiants observables publiquement. Un attaquant se trouvant à portée radio peut ainsi prendre le contrôle complet de l'appareil et intercepter le contenu de l'écran sans chiffrement. Le fabricant n'ayant pas corrigé ces failles dans les délais impartis, le cas a été transmis à l'Office fédéral de la cybersécurité (OFCS), qui a publié une alerte conformément à l'article 73c, alinéa 2, de la loi sur la sécurité de l'information (LSI)[3].

Faux sentiment de sécurité lié au chiffrement audio
Un système de conférence évalué utilise certes une transmission radio chiffrée pour la communication avec ses microphones. Toutefois, le chiffrement est implémenté de manière si faible qu'un attaquant peut le compromettre en quelques secondes et écouter les conversations.

Les casques comme dispositifs d'écoute
Plusieurs casques sans fil permettent un appairage simultané avec plusieurs appareils, tels que des smartphones ou des ordinateurs, fonctionnalité souhaitée par les utilisateurs. Un attaquant disposant brièvement d'un accès physique à un tel casque – par exemple lors d'un moment d'inattention dans un train ou lors d'une visite dans des locaux – peut y appairer un second appareil dont il a le contrôle. Par la suite, toutes les conversations à proximité du casque peuvent être écoutées à l'insu des personnes concernées, à condition que le casque ne soit pas activement utilisé (par exemple en mode veille ou lorsqu'il est placé dans sa station de charge).

Cet exemple montre que les vulnérabilités ne nécessitent pas toujours des techniques de piratage sophistiquées ni des compétences techniques avancées. Étant donné qu'il

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

s'agit ici d'une fonctionnalité prévue, aucun correctif logiciel classique n'est envisageable. La réduction du risque doit donc être assurée par des mesures organisationnelles.

«Claviers fantômes» et attaques par injection
De manière analogue au scénario des casques, un attaquant peut appairer un «clavier fantôme» supplémentaire, invisible de l'utilisateur, avec le dongle USB connecté à un poste de travail. À l'aide de ce clavier fantôme, des commandes peuvent être envoyées à l'ordinateur depuis une distance allant jusqu'à 100 mètres, comme si le attaquant se trouvait physiquement devant l'écran. Cela permet notamment l'injection de commandes malveillantes ou l'installation et l'exécution de logiciels malveillants.

Manipulation du micrologiciel
Certains appareils autorisent l'installation de micrologiciels sans signature numérique valide. Un attaquant peut ainsi déployer un micrologiciel manipulé et établir une persistance durable au niveau matériel. Même une réinstallation du système d'exploitation sur le poste de travail ou le smartphone connecté ne permet pas d'éliminer cette compromission. Ce type de vulnérabilité est également à l'origine de l'attaque dite «*BadCam*[4]», dans laquelle une webcam dotée d'un micrologiciel modifié se présente au PC comme un clavier.

Paramètres par défaut non sécurisés
Un problème transversal récurrent réside dans la priorité accordée par les fabricants au confort d'utilisation au détriment de la sécurité. De nombreux appareils sont livrés avec des paramètres par défaut peu sûrs, tels que des mots de passe standards ou des interfaces inutilement activées, afin de simplifier le support et de favoriser le fonctionnement «plug and play». Cela crée des surfaces d'attaque évitables pour les attaquants.

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

4 Recommandations

La sécurisation des périphériques requiert une approche à plusieurs niveaux, couvrant l'approvisionnement, l'exploitation et la sensibilisation du personnel. Les recommandations suivantes visent à aider les organisations à réduire de manière significative leur surface d'attaque avec un effort raisonnable. Bien que la mise en œuvre de ces mesures soit recommandée de manière générale pour toutes les organisations afin d'établir un niveau de sécurité de base solide, elles revêtent une importance particulière pour les organisations présentant des exigences de protection accrues.

4.1 Approvisionnement sécurisé et standardisation

Les risques de sécurité liés à du matériel non sécurisé peuvent rarement être corrigés a posteriori par des mises à jour. Ils doivent être traités dès la phase d'acquisition:

4.1.1 Protocoles et normes obsolètes

Alors que de nombreux fabricants s'appuient sur des mécanismes de chiffrement éprouvés, des erreurs d'implémentation continuent de survenir. Des attaques bien connues, telles que l'interception de frappes clavier (*KeySniffer*[5]) ou l'injection de commandes clavier et souris (*MouseJack*[6]), demeurent une menace, en particulier pour les appareils plus anciens ou à bas coût.

Mesures:

- **Préférence pour les protocoles standards**: en règle générale, les protocoles standards ouverts et largement établis, tels que Bluetooth dans ses versions actuelles, devraient être privilégiés par rapport à des protocoles propriétaires non documentés. Les standards font l'objet d'un examen continu par une vaste communauté d'experts en sécurité, ce qui réduit la probabilité de vulnérabilités non détectées.
- **Avantages de sécurité des dongles des fabricants:** les organisations ne disposant pas d'une expertise approfondie en matière de communications radio devraient en principe recourir aux dongles fournis par les fabricants. Ceux-ci offrent souvent une configuration de sécurité plus robuste que les paramètres par défaut des terminaux, car des paramètres critiques tels que le chiffrement sont durcis dès la production. Les organisations ayant des exigences de sécurité élevées et une expertise suffisante devraient toutefois évaluer si un durcissement personnalisé des terminaux est plus approprié, ce qui offre un contrôle accru mais nécessite des connaissances techniques approfondies et des processus établis de configuration et de surveillance.

4.1.2 Risques liés à la chaîne d'approvisionnement et prolifération des appareils

L'utilisation non contrôlée d'une grande variété de modèles d'appareils («prolifération des appareils») rend une gestion efficace de la sécurité quasiment impossible. Par ailleurs, il existe un risque que des appareils soient déjà manipulés en usine ou lors du transport (attaques sur la chaîne d'approvisionnement).

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

Mesures:

- **Standardisation du choix des appareils:** il est recommandé de définir un catalogue contraignant de périphériques testés et approuvés. Le respect systématique de ce catalogue – y compris en télétravail et lors des déplacements – réduit la complexité et empêche l'utilisation de produits génériques potentiellement peu sûrs.
- **Sélection de sources fiables:** le matériel devrait être acquis exclusivement via des canaux autorisés de fabricants établis («chaîne de confiance»), ce qui réduit dans une certaine mesure le risque de manipulation des appareils.
- **Intégration de la sécurité de l'information dans les processus d'achat:** les exigences de sécurité (par exemple micrologiciel signé, garanties de mise à jour) devraient être définies comme des critères obligatoires concrets et vérifiables dans les appels d'offres et les contrats. Ces exigences doivent découler des besoins de protection propres à l'organisation et ne doivent pas être remplacées par des évaluations de risques effectuées par les fournisseurs.

  À titre de base technique, la norme ETSI EN 303 645 est particulièrement adaptée. Elle définit des exigences minimales de sécurité pour les appareils connectés, dont le respect doit être démontré de manière transparente par les fournisseurs (par exemple au moyen d'une matrice de conformité conformément à l'annexe B).

4.1.3 Signaux sans fil dans les zones à haute sécurité

Dans les environnements présentant des exigences de protection maximales, les interfaces sans fil constituent souvent une extension évitable de la surface d'attaque.

Mesures:

- **Utilisation de périphériques filaires:** pour les postes de travail soumis à des exigences de sécurité élevées, l'utilisation de périphériques filaires tels que claviers, souris et casques devrait être définie comme norme. Les connexions physiques éliminent en grande partie les risques liés à la transmission de signaux sans fil.
- **Analyses de sécurité indépendantes:** pour les cas d'utilisation particulièrement critiques, il est recommandé de soumettre régulièrement les appareils à des analyses de sécurité indépendantes. Afin de tirer parti des synergies avec l'analyse déjà réalisée, l'Institut national de test pour la cybersécurité NTC peut indiquer si certains appareils faisaient partie du périmètre de test.

4.2 Exploitation et configuration sécurisées

Nombre des vulnérabilités identifiées sont de nature technique, mais ne deviennent critiques qu'en raison de lacunes organisationnelles.

4.2.1 Gestion du cycle de vie et micrologiciel

Au cours des tests, de nombreuses vulnérabilités ont été identifiées et ont depuis été corrigées par les fabricants. Toutefois, comme les périphériques ne sont souvent pas intégrés à la gestion centralisée des correctifs informatiques, les mises à jour n'atteignent pas les appareils ou seulement avec un retard considérable.

Mesures:

- **Mise en place de processus de mise à jour du micrologiciel:** un processus régulier de mise à jour des micrologiciels des périphériques devrait être établi, à l'instar de ce

qui est pratiqué pour les composants informatiques classiques tels que les serveurs et les ordinateurs portables.
  - **Remarque importante:** il est recommandé d'examiner de manière critique l'installation permanente de logiciels de gestion des fabricants sur les systèmes des utilisateurs finaux, car ces logiciels peuvent eux-mêmes accroître la surface d'attaque. De plus amples informations figurent au point *4.2.3 Logiciels des fabricants*.
- **Inventaire des actifs:** les périphériques pertinents pour la sécurité devraient être enregistrés dans la gestion des actifs. Seuls les appareils inventoriés peuvent être mis hors service de manière fiable, éliminés en toute sécurité et correctement déconnectés en fin de cycle de vie.

4.2.2 Durcissement des systèmes et contrôle des interfaces

De nombreux appareils sont livrés avec des interfaces ouvertes et des services de confort activés («plug and play»), ce qui crée des surfaces d'attaque inutiles.

Mesures:

- **Désactivation des interfaces inutilisées:** il est recommandé de désactiver les interfaces qui ne sont pas strictement nécessaires au fonctionnement. Cela concerne en particulier les appareils plus complexes tels que les systèmes de conférence avec leurs nombreux ports, et concerne aussi bien les ports physiques comme l'USB et l'Ethernet que les interfaces sans fil comme le WLAN et le Bluetooth. Cela permet de réduire la surface d'attaque au minimum.
- **Désactivation des services non nécessaires:** les fonctions de confort telles que les accès de maintenance à distance, Telnet et les protocoles de découverte devraient être désactivées sur tous les appareils, sauf si elles sont strictement requises pour l'exploitation.

4.2.3 Logiciels des fabricants

Les outils de gestion complets fournis par les fabricants fonctionnent souvent en permanence en arrière-plan et augmentent la surface d'attaque sur les systèmes clients.

Mesure:

- **Principe de sobriété pour les logiciels des fabricants:** il est recommandé d'évaluer de manière critique la nécessité d'installer des logiciels de fabricants sur les systèmes des utilisateurs finaux. Dans de nombreux cas, les pilotes de base du système d'exploitation suffisent. Si des logiciels supplémentaires sont indispensables, leur exécution permanente en arrière-plan devrait être évitée. Les mises à jour de micrologiciel devraient plutôt être effectuées via des stations de mise à jour dédiées, exploitées par le support informatique, ce qui rendrait inutile l'installation de logiciels de gestion sur les postes des utilisateurs.

4.3 Appairage sécurisé des appareils

Le processus d'appairage constitue une phase critique durant laquelle des attaquants peuvent tenter d'intégrer leurs propres appareils dans une relation de confiance.

4.3.1 «Claviers fantômes» et dispositifs d'écoute

Pour certains appareils, des attaquants peuvent se connecter au dongle sans fil d'une victime. Cela suppose soit un accès physique temporaire au dongle, soit l'exploitation d'une vulnérabilité dans le protocole d'appairage. Un «clavier fantôme» invisible peut alors injecter des commandes malveillantes, ou un casque non autorisé peut fonctionner comme dispositif d'écoute.

Mesures:

- **Sensibilisation et formation:** le personnel devrait être formé à ne pas laisser sans surveillance des périphériques mobiles (par exemple dongles USB et casques) dans des lieux publics.
- **Restriction des possibilités d'appairage:** lorsque cela est techniquement possible, les dongles devraient être verrouillés par logiciel après l'appairage initial afin d'empêcher l'ajout ultérieur d'appareils non autorisés. Il convient toutefois de reconnaître que cette mesure est souvent difficile à mettre en œuvre dans la pratique.
- **Utilisation dans les environnements publics:** dans les environnements non contrôlés tels que les trains ou les cafés, il est recommandé d'utiliser exclusivement des appareils empêchant techniquement tout appairage clandestin par des tiers, par exemple au moyen de solutions filaires.

4.4 Infrastructures et salles de conférence

Étant donné que les appareils multimédias complexes ont présenté une fréquence de lacunes critiques particulièrement élevée lors des tests, les recommandations complémentaires suivantes revêtent une importance particulière pour cette catégorie d'équipements.

4.4.1 Vulnérabilités critiques dans les appareils IoT

Comme l'illustre le cas du système de présentation EZCast, des vulnérabilités dans les systèmes de conférence peuvent permettre l'interception clandestine de contenus d'écran ou une compromission complète du système.

Mesure:

- **Séparation des réseaux:** les appareils disposant de leur propre connectivité réseau, tels que les appareils IoT, les systèmes de visioconférence et les solutions de présentation sans fil, devraient être exploités dans des segments de réseau isolés. Il doit être garanti que ces appareils n'aient pas d'accès direct au réseau interne de l'organisation.

4.5 Perspectives réglementaires

Si les nouvelles exigences en matière de cybersécurité de **la directive sur les équipements radioélectriques (RED)** sont en vigueur depuis août 2025 et obligent les fabricants à renforcer la sécurité de leurs produits, le futur **Cyber Resilience Act (CRA)** étendra encore ces obligations. Il impose notamment le principe de la sécurité dès la conception (security by design) ainsi que des mises à jour de sécurité obligatoires sur l'ensemble du cycle de vie des produits numériques.

Il faudra toutefois du temps pour que ces réglementations s'imposent pleinement sur le

marché. Les organisations ne devraient donc pas attendre, mais exiger dès aujourd'hui de leurs fournisseurs une transparence accrue et des engagements contractuels clairs en matière de cybersécurité.