Nationales Testinstitut für Cybersicherheit

Cybersicherheit von Peripheriegeräten

Versteckte Risiken im Büro: Sind kabellose Tastaturen, Headsets und Co. sicher genug für den Einsatz in kritischen Infrastrukturen?

Version	1.0
Datum	26. Februar 2026
Klassifikation	Öffentlich
Autoren	Tobias Castagna, Andreas Leisibach, Dilip Many, Fabio Zuber, Raphael M. Reischuk
Verantwortlich	Tobias Castagna

Inhaltsübersicht

1 Einleitung 3

2 Ausgangslage und Vorgehen 5

3 Zusammenfassende Einschätzung 8

4 Empfehlungen 10

4.1 Sichere Beschaffung und Standardisierung 10

4.1.1 Veraltete Protokolle und Standards 10

4.1.2 Supply-Chain-Risiken und Wildwuchs 10

4.1.3 Funksignale in Hochsicherheitsbereichen 11

4.2 Sicherer Betrieb und Konfiguration 11

4.2.1 Lifecycle-Management und Firmware 11

4.2.2 Systemhärtung und Schnittstellenkontrolle 12

4.2.3 Herstellersoftware 12

4.3 Sichere Gerätekopplung 12

4.3.1 «Schatten-Tastaturen» und Wanzen 12

4.4 Infrastruktur und Konferenzräume 13

4.4.1 Kritische Lücken in IoT-Geräten 13

4.5 Regulatorischer Ausblick 13

Danksagung

Ein besonderer Dank gilt allen Organisationen und Experten, die diese Untersuchung unterstützt haben, sei es durch die Bereitstellung von Testgeräten, durch Einblicke in die Verwendung solcher Geräte in unterschiedlichen Umgebungen oder durch eine Beteiligung an den Kosten. Ihr herausragendes Engagement im Bereich der Cybersicherheit hat massgeblich zum Gelingen dieser Sicherheitsanalyse beigetragen. Dazu gehören:

- Bundesamt für Cybersicherheit (BACS)
- Bundesamt für Kommunikation (BAKOM)
- Bundesamt für Zoll und Grenzsicherheit (BAZG)
- Digitec Galaxus
- Kanton Schwyz
- Redguard AG
- Zuger Kantonalbank
- weitere Schweizer Finanzinstitute (aus Diskretionsgründen ohne Namensnennung)

1 Einleitung

In der heutigen Arbeitswelt endet die IT-Sicherheit nicht an der Netzwerkgrenze. Während Organisationen erheblich in Schutzmassnahmen wie Firewalls und Endpoint-Protection investieren, wird eine naheliegende Angriffsfläche im Alltag häufig unterschätzt: Peripheriegeräte am digitalen Arbeitsplatz.

Ein reales Szenario verdeutlicht das Risiko: Eine vertrauliche Videokonferenz bei einem Betreiber einer kritischen Infrastruktur. Das Netzwerk ist abgesichert, die Verbindung Ende-zu-Ende verschlüsselt, der Server gehärtet und der Laptop geschützt. Doch der Angreifer zielt auf etwas anderes ab: Mit einer Antenne auf dem nahegelegenen Parkplatz fängt er den unverschlüsselten Funkverkehr des drahtlosen Tischmikrofons ab. Nach wenigen Sekunden wird das vertrauliche Gespräch abgehört – die IT-Sicherheit wurde durch ein unsicheres Peripheriegerät ausgehebelt.

Das Problem ist eine gefährliche Asymmetrie: Die Kosten für eine professionelle Sicherheitsanalyse, mit der sich solche Risiken erkennen lassen, übersteigen den Anschaffungspreis einer Webcam oder Tastatur um ein Vielfaches. In der Praxis verlassen sich IT-Abteilungen daher häufig auf die Versprechen der Hersteller.

Um das Sicherheitsniveau von in der Schweiz weit verbreiteten Peripheriegeräten systematisch zu beurteilen, hat das Nationale Testinstitut für Cybersicherheit NTC deshalb im Laufe eines Jahres rund 30 Geräte einer umfassenden technischen Sicherheitsanalyse unterzogen. In die Auswahl flossen gezielt Produkte etablierter Hersteller ein, die in Schweizer Organisationen und insbesondere in kritischen Infrastrukturen breit eingesetzt werden. Günstige Produkte unbekannter Herkunft wurden bewusst nicht berücksichtigt.

Insgesamt wurden über 60 Befunde unterschiedlicher Kritikalität identifiziert, darunter 13 schwerwiegende und drei mit der höchsten Kritikalitätsstufe.

Die Untersuchung zeigt, dass moderne, gut konzipierte Peripheriegeräte – einschliesslich kabelloser Lösungen – grundsätzlich ein hohes Sicherheitsniveau erreichen können. Dabei ist nicht nur die Sicherheit der einzelnen Komponenten entscheidend, sondern auch die Wahl einer sicheren Konfiguration sowie die Vorgaben, die den sicheren Einsatz der Geräte definieren. Dazu gehören auch organisatorische Prozesse, die den sicheren Betrieb gewährleisten, beispielsweise das regelmässige Einspielen von Firmware-Updates, sowie Klarheit über getroffene Annahmen.

Insbesondere Betreiber kritischer Infrastrukturen mit erhöhten Sicherheitsanforderungen müssen von besonders motivierten und ressourcenstarken Angreifern ausgehen. Diese können unkonventionelle Angriffsvektoren und Techniken verwenden, die anderorts untypisch sein mögen. So liessen sich beispielsweise mehrere getestete kabellose Headsets und Konferenzsysteme mit geringem Aufwand zu Abhörgeräten umfunktionieren. Diese und weitere Risiken werden im vorliegenden Bericht erläutert und durch konkrete Massnahmen und Empfehlungen adressiert.

Die detaillierten Befunde wurden den betroffenen Herstellern vertraulich übermittelt, um eine rasche Behebung der Schwachstellen zu ermöglichen. In diesem öffentlichen Bericht wird folglich bewusst auf die Nennung technischer Details verzichtet. Stattdessen werden typische Risikomuster und daraus abgeleitete Empfehlungen dargestellt.

Die Analyse erfolgte im Rahmen einer gemeinsamen Initiative des NTC mit Unterstützung von Behörden auf Bundes- und Kantonsebene sowie aus dem Finanzsektor. Um die Unabhängigkeit der Resultate zu gewährleisten, waren die Hersteller der getesteten Geräte weder in die Auswahl noch in die Durchführung der Tests eingebunden und wurden erst bei der Meldung der Schwachstellen kontaktiert.

5 empfohlene Massnahmen für mehr Sicherheit

Basierend auf der durchgeführten Sicherheitsanalyse lassen sich fünf grundlegende Handlungsfelder ableiten, um das Risiko beim Einsatz von Peripheriegeräten effektiv zu reduzieren:

Standardisierung und Beschaffung über vertrauenswürdige Kanäle
Es wird empfohlen, die Gerätevielfalt auf einen verbindlichen Katalog geprüfter Peripheriegeräte zu begrenzen. Die Beschaffung sollte ausschliesslich über vertrauenswürdige Kanäle erfolgen, um das Risiko manipulierter Hardware (Supply-Chain-Angriffe) zu reduzieren.

Integration in das Lifecycle-Management
Peripheriegeräte sollten nicht als reines Zubehör, sondern als vollwertige IT-Komponenten betrachtet werden. So sollten sicherheitsrelevante Geräte im Asset-Management erfasst und Prozesse etabliert werden, die beispielsweise sicherstellen, dass Firmware-Updates zeitnah eingespielt werden oder dass verwundbare Hardware rasch ersetzt wird.

Netzwerk-Segmentierung
Für netzwerkfähige Systeme, wie Konferenzlösungen oder IoT-Geräte, wird der Betrieb in isolierten Netzwerksegmenten empfohlen. So wird verhindert, dass diese Geräte als Einfallstor in das interne Firmennetzwerk dienen.

Physische Sicherheit und Sensibilisierung
Mitarbeitende sollten für den sicheren Umgang mit Peripheriegeräten sensibilisiert werden. Dies beinhaltet die ausschliessliche Nutzung freigegebener Hardware im Homeoffice sowie das Bewusstsein für Risiken durch unbeaufsichtigte Geräte wie USB-Dongles oder Funk-Headsets in öffentlichen Räumen.

Kabelgebundene Lösungen in Hochsicherheitsbereichen
In Bereichen mit maximalem Schutzbedarf sind kabelgebundene Peripheriegeräte zu bevorzugen. Kabel eliminieren die Risiken der drahtlosen Signalübertragung weitgehend.

Die aufgeführten Punkte fassen wichtige Empfehlungen zusammen. Eine detaillierte Ausführung der technischen Hintergründe und Massnahmen findet sich in *Kapitel 4 Empfehlungen* dieses Berichts.

2 Ausgangslage und Vorgehen

Peripheriegeräte sind weit mehr als nur Zubehör, denn sie bilden die physikalische Schnittstelle zwischen Mensch und Computer. Über sie fliessen sensible Informationen. So werden beispielsweise Passwörter über Tastaturen eingegeben und vertrauliche Gespräche werden über Webcams und Mikrofone geführt. Sind diese unsicher oder manipuliert, so können sie als Einfallstore dienen, um Sicherheitsmechanismen zu umgehen oder als Abhörwerkzeuge missbraucht werden. Während klassische Arbeitsrechner und Smartphones immer besser abgesichert werden, stellen die oft weniger gut geschützten Peripheriegeräte ein erhebliches, meist unüberwachtes Risiko dar.

Zwei aktuelle Vorfälle verdeutlichen die Relevanz dieses Themas: Im Jahr 2025 wurden eine Reihe von Schwachstellen[1] in weit verbreiteten Bluetooth-Chips des Herstellers Airoha bekannt. Dadurch können Angreifer die Bluetooth-Verbindung kapern und beispielsweise vertrauliche Gespräche unbemerkt mithören. Die verwundbaren Chips sind unter anderem in Geräten der Marken Bose, Jabra, JBL, Teufel, Sony und Marshall verbaut. Dass dieses Risiko permanent besteht, zeigte sich Anfang 2026 erneut: Forscher deckten unter dem Namen «WhisperPair»[2] gravierende Lücken in der Implementierung des «Google Fast Pair»-Protokolls auf. Diese erlauben es, Kopfhörer von Herstellern wie Google, Sony, Xiaomi und OnePlus ohne jegliche Nutzerinteraktion zu übernehmen und so Umgebungsgespräche abzuhören und den Standort via «Find My Device»-Netzwerk zu verfolgen. Solche Vorfälle zeigen, dass selbst Produkte namhafter Hersteller nicht immun gegen schwerwiegende Implementierungsfehler sind.

Trotz ihrer kritischen Rolle werden Schwachstellenanalysen von Peripheriegeräten nur selten durchgeführt. Die Gründe dafür sind vielfältig:

- **Fehlendes Risikobewusstsein:** Peripheriegeräte wie Tastaturen werden oft als primitive, nicht eigenständige Hardware wahrgenommen. Dabei verfügen sie inzwischen über eigene Prozessoren, Firmware und Funkschnittstellen und sind somit integraler Bestandteil der IT-Angriffsfläche.
- **Ökonomische Hürden:** Die Kosten für eine professionelle Sicherheitsanalyse übersteigen den Anschaffungspreis dieser Geräte oft um ein Vielfaches und stehen somit in einem ökonomischen Missverhältnis.
- **Verantwortungsdiffusion:** Die weite Verbreitung von Peripheriegeräten führt oft zu einem trügerischen Sicherheitsgefühl. Viele Unternehmen unterliegen der Fehlannahme, dass populäre Produkte aufgrund ihrer hohen Marktdurchdringung bereits durch Dritte geprüft wurden und gravierende Lücken längst behoben wären.
- **Kontrollverlust:** Die Zunahme von Homeoffice und «Bring Your Own Device» haben zu einer unüberschaubaren Gerätevielfalt geführt, die sich oft der zentralen Kontrolle der IT entzieht.

Das NTC hat aus oben genannten Gründen eine umfassende technische Sicherheits-überprüfung von rund 30 gängigen Peripheriegeräten durchgeführt. In die Auswahl flossen sowohl kabelgebundene als auch drahtlose Geräte etablierter Hersteller wie Logitech, Yealink, Jabra, HP, Eizo oder Cherry ein – also Geräte der folgenden

[1] CVE-Details: *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*

Kategorien, die in Schweizer Organisationen und insbesondere in kritischen Infrastrukturen breit eingesetzt werden:

- **Tastaturen und Mäuse**
- **Headsets**
- **Webcams**
- **Docking-Stationen**
- **Konferenzsysteme**

Die Tests und der anschliessende Responsible-Disclosure-Prozess mit den Herstellern erstreckten sich über einen Zeitraum von rund einem Jahr. Die Analyse wurde von vier Testexperten des NTC durchgeführt – in Zusammenarbeit mit mehreren Behörden auf Bundes- und Kantonsebene sowie mit Organisationen aus dem Finanzsektor.

Um die Unabhängigkeit der Ergebnisse zu gewährleisten, waren die Hersteller der überprüften Geräte weder an der Auswahl noch an der Beschaffung oder Durchführung der Tests beteiligt. Sie wurden erst bei der Meldung der Schwachstellen kontaktiert.

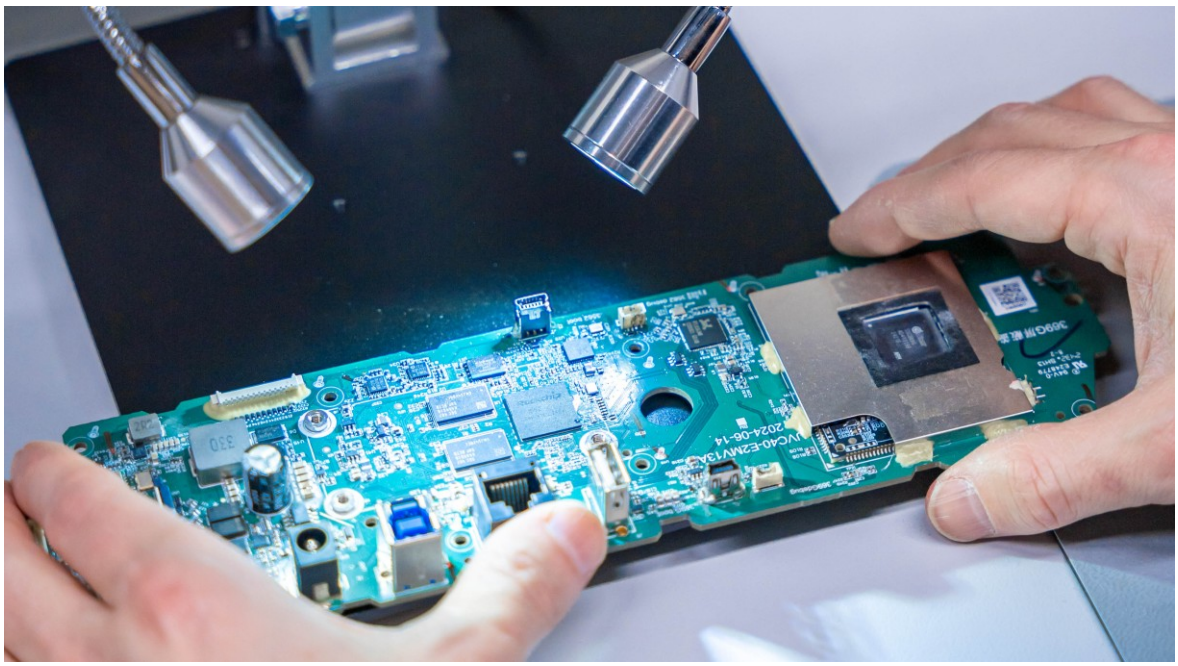

Abbildung 1: Optische Überprüfung der in den Peripheriegeräten verbauten Komponenten im Labor des NTC in Zug

Um fundierte Aussagen über die überprüften Geräte treffen zu können, gingen die Tests weit über reine Funktionsprüfungen hinaus. Die Analyse erfolgte mehrstufig. Dabei kamen unter anderem folgende Methoden zum Einsatz:

- **Hardware-Analyse:** Die Geräte wurden physisch geöffnet, um verbaute Chips zu identifizieren. Dabei wurde nach offenen Wartungsschnittstellen gesucht, die Angreifern Zugriff auf die Firmware ermöglichen könnten, sowie nach versteckten oder unerwarteten Bauteilen, die auf eine Manipulation in der Lieferkette (Supply Chain Attack) hindeuten könnten.
- **Firmware-Analyse:** Die Gerätesoftware wurde extrahiert und mittels Reverse Engineering untersucht. Ziel war es unter anderem, fest kodierte Passwörter (Hardcoded Credentials), versteckte Hintertüren (Backdoors), unsichere Verschlüsselungsverfahren oder fehlende Integritätsprüfungen aufzuspüren, die das

Einspielen manipulierter Updates ermöglichen würden.

- **Funk-Analyse:** Mittels Mitschneidens (Sniffing) und Analyse des Funkverkehrs wurde überprüft, ob die Kommunikation zwischen Peripheriegerät und seinem Gegenstück (Dongle/PC) verschlüsselt und gegen Manipulation geschützt ist.
- **Konfigurations- und Schnittstellenanalyse:** Es wurde geprüft, ob Management-Interfaces, Diagnoseschnittstellen oder zusätzliche Kommunikationsprotokolle die Angriffsfläche unnötig vergrössern und ob die Standardeinstellungen dem Security-by-Default-Prinzip folgen.

3 Zusammenfassende Einschätzung

Die meisten Produkte namhafter Hersteller weisen ein akzeptables bis gutes Sicherheitsniveau auf, sofern sie sicher konfiguriert sind und die Firmware aktuell gehalten wird. Dennoch wurden im Rahmen der Tests über 60 Befunde festgestellt, darunter 13 schwerwiegende und 3 der höchsten Kritikalitätsstufe. Die Schwachstellen wurden im Rahmen des Responsible-Disclosure-Prozesses vertraulich an die Hersteller gemeldet und grösstenteils von diesen behoben. Viele der identifizierten Schwachstellen setzen keine völlig neuen Angriffsmethoden voraus, sondern beruhen auf bekannten Angriffstechniken. Die Ausnutzbarkeit dieser Schwachstellen in realistischen Szenarien unterstreicht den Handlungsbedarf.

Während klassische Eingabegeräte wie Mäuse oder Tastaturen dank moderner Standards oft solide abgesichert sind, steigen die Risiken, sobald Geräte eine höhere Komplexität aufweisen, beispielsweise bei Konferenzsystemen und sonstigen IoT-Geräten, oder sobald veraltete Funktechnologie genutzt wird.

Relevante Beispiele von Befunden aus der Analyse sind:

Kritische Schwachstellen bei EZCast Pro II
Der schwerwiegendste Befund betrifft das drahtlose Präsentationssystem *EZCast Pro II*. Hier führen gravierende Designfehler zu kritischen Schwachstellen: Fest kodierte kryptografische Schlüssel erlauben den Zugriff auf die Admin-Oberfläche und WLAN-Passwörter lassen sich aus öffentlichen Kennungen berechnen. Ein Angreifer in Funkreichweite kann die komplette Kontrolle über das Gerät übernehmen und Bildschirminhalte unverschlüsselt mitschneiden. Da der Hersteller die Lücken nicht fristgerecht geschlossen hat, wurde der Fall an das Bundesamt für Cybersicherheit (BACS) übergeben, welches eine Warnung nach Informationssicherheitsgesetz (ISG) Art. 73c Abs. 2 veröffentlichte[3].

Scheinsicherheit bei Audio-Verschlüsselung
Ein überprüftes Konferenzsystem nutzt zwar eine verschlüsselte Funkübertragung für die Kommunikation mit den Mikrofonen. Die Verschlüsselung ist jedoch so schwach konzipiert, dass ein Angreifer sie innerhalb weniger Sekunden knacken und die Gespräche mithören kann.

Das Headset als Wanze
Bei mehreren kabellosen Headsets ist die simultane Kopplung mit mehr als einem Gerät, wie Smartphones oder Computern, eine gewünschte Funktion. Ein Angreifer, der kurzzeitig physischen Zugriff auf ein solches Headset hat, beispielsweise in einem unachtsamen Moment im Zug oder bei einem Bürobesuch, kann ein zweites, von ihm kontrolliertes Gerät koppeln. Anschliessend können alle Gespräche, die in der Nähe des Headsets geführt werden, unbemerkt mitgehört werden – sofern das Headset gerade nicht aktiv genutzt wird (z.B. im Standby-Modus oder in der Ladestation).
Dieses Beispiel zeigt, dass Schwachstellen nicht nur durch klassisches Hacking ausgenutzt werden können und dies nicht immer besonderes Know-how erfordert. Da es sich um eine gewünschte Funktion handelt, wird es keinen klassischen Patch geben. Die Risikominimierung muss hier durch organisatorische Massnahmen umgesetzt werden.

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

«Schatten-Tastaturen» und Injektion
Ähnlich wie beim oben erwähnten Headset-Angriff kann ein Angreifer eine zusätzliche, für den Anwender unsichtbare «Schatten-Tastatur» mit dem am Arbeitsrechner verbundenen USB-Dongle koppeln. Über diese «Schatten-Tastatur» können aus bis zu 100 Metern Entfernung Befehle an den Rechner gesendet werden, als würde man direkt davorsitzen. So können beispielsweise bösartige Befehle eingegeben oder Schadsoftware eingespielt und ausgeführt werden.

Firmware-Manipulation
Einige Geräte erlauben das Aufspielen von Firmware ohne gültige digitale Signatur. Ein Angreifer kann auf diese Weise manipulierte Firmware installieren und so eine dauerhafte Persistenz auf Hardware-Ebene erreichen. Selbst eine Neuinstallation des Betriebssystems auf dem angeschlossenen Arbeitsrechner oder Smartphone kann diese nicht beseitigen. Diese Schwachstelle ist z.B. auch für den «*BadCam*[4]»-Angriff verantwortlich, bei dem eine Webcam mit manipulierter Firmware sich gegenüber dem PC als Tastatur ausgibt.

Unsichere Standardeinstellungen
Ein übergeordnetes Problem stellt die Priorisierung von Komfort vor Sicherheit durch die Hersteller dar. Viele Geräte werden mit unsicheren Standardeinstellungen wie Standardpasswörtern oder unnötig aktivierten Schnittstellen ausgeliefert, um den Support zu erleichtern. Dies bietet Angreifern unnötige Angriffsflächen zugunsten von «Plug-and-Play».

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

4 Empfehlungen

Die Absicherung von Peripheriegeräten erfordert einen mehrschichtigen Ansatz, der von der Beschaffung über den Betrieb bis zur Sensibilisierung der Mitarbeitenden reicht. Die folgenden Empfehlungen sollen Organisationen dabei helfen, ihre Angriffsfläche mit angemessenem Aufwand erheblich zu reduzieren. Obwohl die Umsetzung dieser Massnahmen grundsätzlich für alle Organisationen empfohlen wird, um ein solides Basissicherheitsniveau zu gewährleisten, richten sie sich mit besonderer Dringlichkeit an Organisationen mit erhöhtem Schutzbedarf.

4.1 Sichere Beschaffung und Standardisierung

Sicherheitsrisiken, die durch unsichere Hardware entstehen, lassen sich nachträglich meist nicht «patchen». Sie müssen bei der Beschaffung gelöst werden:

4.1.1 Veraltete Protokolle und Standards

Während viele Hersteller auf bewährte Verschlüsselung setzen, finden sich immer wieder Implementierungsfehler. Bekannte Angriffe wie das Abfangen von Tastatureingaben (*KeySniffer*[5]) oder das Injizieren von Tastatur- und Mauseingaben (*MouseJack*[6]) bleiben eine Bedrohung, insbesondere bei älteren und günstigeren Geräten.

Massnahmen:

- **Bevorzugung von Standardprotokollen:** Grundsätzlich sind offene und gut etablierte Standardprotokolle wie Bluetooth in ihrer aktuellen Version proprietären, nicht dokumentierten Protokollen vorzuziehen. Standards werden von einer breiten Gemeinschaft von Sicherheitsexperten kontinuierlich überprüft, was die Wahrscheinlichkeit unentdeckter Schwachstellen reduziert.
- **Sicherheitsvorteile von Hersteller-Dongles:** Organisationen ohne tiefgreifendes Funk-Know-how sollten in der Regel auf Hersteller-Dongles setzen. Diese bieten oft eine robustere Sicherheitskonfiguration als die Standard-Einstellungen von Endgeräten, da kritische Parameter wie Verschlüsselung bereits werkseitig gehärtet sind. Organisationen mit hohen Sicherheitsanforderungen und entsprechender Expertise sollten hingegen prüfen, ob eine eigene Härtung der Endgeräte zielführender ist. Dies ermöglicht mehr Kontrolle über alle Parameter, setzt jedoch tiefes Fachwissen und etablierte Prozesse für Konfiguration und Monitoring voraus.

4.1.2 Supply-Chain-Risiken und Wildwuchs

Der unkontrollierte Einsatz verschiedenster Gerätemodelle («Wildwuchs») verunmöglicht ein effektives Sicherheitsmanagement. Zudem besteht das Risiko, dass Geräte bereits ab Werk oder auf dem Lieferweg manipuliert werden (Supply-Chain-Angriffe).

Massnahmen:

- **Standardisierung der Geräteauswahl:** Es wird empfohlen, einen verbindlichen Katalog von geprüften und freigegebenen Peripheriegeräten zu definieren. Dessen konsequente Einhaltung – auch im Homeoffice und unterwegs – reduziert die Komplexität und verhindert den Einsatz potenziell unsicherer No-Name-Produkte.

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

- **Auswahl vertrauenswürdiger Quellen:** Hardware sollte ausschliesslich über autorisierte Kanäle etablierter Hersteller bezogen werden («Chain of Trust»). Dies minimiert das Risiko von manipulierten Geräten zu einem gewissen Grad.
- **Einbindung der Informationssicherheit in den Beschaffungsprozess:** Sicherheitsanforderungen (z.B. signierte Firmware, Update-Garantien) sollten in Ausschreibungen und Verträgen als konkrete und verifizierbare Muss-Kriterien definiert werden. Diese sind konsequent aus dem eigenen Schutzbedarf abzuleiten und dürfen nicht durch eine lieferantenseitige Risikoeinschätzung ersetzt werden. Als technische Basis eignet sich z.B. der Standard ETSI EN 303 645. Er definiert Mindestanforderungen für vernetzte Geräte, deren Einhaltung vom Lieferanten transparent nachzuweisen ist (z.B. mittels Compliance-Matrix gemäss Annex B).

4.1.3 Funksignale in Hochsicherheitsbereichen

In Bereichen mit maximalem Schutzbedarf stellen Funkschnittstellen eine oft vermeidbare Erweiterung der Angriffsfläche dar.

Massnahmen:

- **Einsatz kabelgebundener Geräte:** Für Arbeitsplätze mit hohen Sicherheitsanforderungen sollte der Einsatz von kabelgebundenen Peripheriegeräten wie Tastaturen, Mäusen und Headsets als Standardvorgabe gelten. Kabel eliminieren die Risiken der drahtlosen Signalübertragung weitgehend.
- **Unabhängige Sicherheitsanalyse:** Für besonders kritische Einsatzbereiche wird empfohlen, die Geräte regelmässig einer unabhängigen Sicherheitsanalyse zu unterziehen. Um die Synergien der bereits durchgeführten Analyse zu nutzen, bietet das NTC Auskunft, ob die eigenen Geräte bereits Teil des Testumfangs waren.

4.2 Sicherer Betrieb und Konfiguration

Viele der gefundenen Schwachstellen sind technischer Natur, werden aber erst durch organisatorische Versäumnisse kritisch.

4.2.1 Lifecycle-Management und Firmware

Im Rahmen der Tests wurden zahlreiche Schwachstellen identifiziert, die von den Herstellern inzwischen behoben wurden. Da Peripheriegeräte jedoch oft nicht im zentralen IT-Patch-Management erfasst sind, erreichen diese Updates die Geräte nicht oder mit grosser Verzögerung.

Massnahmen:

- **Etablierung von Firmware-Updates:** Ein Prozess zur regelmässigen Aktualisierung der Firmware von Peripheriegeräten sollte etabliert werden – analog zum Vorgehen bei klassischen IT-Komponenten wie Server und Laptops.
  - **Wichtiger Hinweis:** Es wird empfohlen, permanent installierte Verwaltungssoftware der Hersteller auf jedem Arbeitsrechner kritisch zu hinterfragen, da diese selbst die Angriffsfläche vergrössern können. Mehr Details dazu finden sich in *Kapitel 4.2.3 Herstellersoftware.*
- **Inventarisierung:** Sicherheitsrelevante Peripheriegeräte sollten im Asset-Management erfasst werden. Nur was inventarisiert ist, dürfte am Ende des Lebenszyklus verlässlich sicher entsorgt und entkoppelt werden.

4.2.2 Systemhärtung und Schnittstellenkontrolle

Viele Geräte werden mit offenen Schnittstellen und aktivierten Komfortdiensten ausgeliefert («Plug-and-Play»), was unnötige Angriffsflächen bietet.

Massnahmen:

- **Deaktivierung ungenutzter Schnittstellen:** Es wird empfohlen, für den Betrieb nicht zwingend erforderliche Schnittstellen zu deaktivieren. Dies ist besonders bei komplexeren Geräten wie Konferenzsystemen mit ihrer Vielzahl von Anschlüssen relevant und betrifft sowohl physische Ports wie USB und Ethernet als auch Funkschnittstellen wie WLAN und Bluetooth. So wird die Angriffsfläche auf ein Minimum reduziert.
- **Deaktivierung unnötiger Dienste:** Komfortfunktionen wie Fernwartungszugänge, Telnet und Discovery-Protokolle sollten auf allen Geräten abgeschaltet werden, wenn diese nicht zwingend für den Betrieb erforderlich sind.

4.2.3 Herstellersoftware

Umfangreiche Management-Tools der Hersteller laufen oft permanent im Hintergrund und vergrössern die Angriffsfläche auf dem Client-PC.

Massnahme:

- **Minimalismus bei Herstellersoftware:** Es wird empfohlen, die Notwendigkeit der Installation von Herstellersoftware auf Endbenutzer-Systemen kritisch zu prüfen. Oft genügen Basistreiber des Betriebssystems für den Betrieb. Ist Zusatzsoftware unverzichtbar, sollte auf eine permanente Ausführung im Hintergrund verzichtet werden. Firmware-Updates sollten stattdessen beispielsweise über dedizierte Update-Stationen des IT-Supports erfolgen, sodass die Verwaltungssoftware auf den Endgeräten nicht erforderlich ist.

4.3 Sichere Gerätekopplung

Der Kopplungsprozess (Pairing) stellt eine kritische Phase dar, in der Angreifer versuchen können, eigene Geräte in die vertrauenswürdige Verbindung einzubinden.

4.3.1 «Schatten-Tastaturen» und Wanzen

Bei einigen Geräten ist es Angreifern möglich, sich mit dem Funk-Dongle eines Opfers zu verbinden. Dies setzt voraus, dass der Angreifer entweder kurzzeitig physischen Zugriff auf das Dongle hat oder eine potenziell vorhandene Sicherheitslücke im Kopplungsprotokoll ausnutzt. So kann eine unsichtbare «Schatten-Tastatur» Schadbefehle senden oder ein fremdes Headset als Abhörgerät («Wanze») fungieren.

Massnahmen:

- **Sensibilisierung:** Mitarbeitende sollten geschult werden, mobile Peripheriegeräte (wie z.B. USB-Dongles und Headsets) an öffentlichen Orten nicht unbeaufsichtigt zu lassen.
- **Einschränkung der Kopplungsmöglichkeiten**: Sofern technisch umsetzbar, sollten Dongles nach dem initialen Pairing softwareseitig «abgeschlossen» werden (Locking), um das nachträgliche Hinzufügen fremder Geräte zu verhindern. Es muss jedoch berücksichtigt werden, dass dies in der betrieblichen Praxis oft nur sehr schwer umzusetzen ist.

- **Nutzung in der Öffentlichkeit:** In unkontrollierten Umgebungen, wie beispielsweise im Zug oder im Café, wird empfohlen, ausschliesslich Geräte zu verwenden, die eine unbemerkte Fremdkopplung technisch ausschliessen (z.B. durch kabelgebundene Lösungen).

4.4 Infrastruktur und Konferenzräume

Da komplexe Multimedia-Geräte im Test besonders häufig kritische Mängel aufwiesen, sind die folgenden Zusatzempfehlungen für diese Gerätekategorie besonders wichtig.

4.4.1 Kritische Lücken in IoT-Geräten

Wie der Fall des Präsentationssystems EZCast zeigt, können Schwachstellen in Konferenzsystemen zum unbemerkten Mitschneiden von Bildschirminhalten oder zur vollständigen Systemübernahme führen.

Massnahme:

- **Netzwerktrennung:** Geräte mit eigenem Netzwerkanschluss wie IoT-Geräte, Videokonferenzsysteme und drahtlose Präsentationslösungen sollten in isolierten Netzwerken betrieben werden. Es sollte sichergestellt werden, dass diese Geräte keinen direkten Zugriff auf das interne Unternehmensnetzwerk haben.

4.5 Regulatorischer Ausblick

Während die neuen Cybersicherheitsanforderungen der **Radio Equipment Directive (RED)** bereits seit August 2025 in Kraft sind und Hersteller zu mehr Cybersicherheit verpflichten, wird der kommende **Cyber Resilience Act (CRA)** diese Pflichten weiter ausbauen. Er fordert unter anderem «Security by Design» und verpflichtende Sicherheitsupdates über den gesamten Lebenszyklus digitaler Produkte.

Es wird jedoch einige Zeit dauern, bis diese Regularien den Markt vollständig durchdrungen haben. Organisationen sollten daher nicht warten, sondern bereits heute von ihren Lieferanten Transparenz und vertraglich zugesichertes Engagement für Cybersicherheit einfordern.