

MEDIENMITTEILUNG

Summarischer Bericht zur Cybersicherheit von Peripheriegeräten

Unterschätztes Risiko: Wie Tastaturen, Headsets und Co. zum Einfallstor für kritische Systeme werden

Zug, 26. Februar 2026 – Eine umfassende technische Analyse des Nationalen Testinstituts für Cybersicherheit NTC zeigt, dass Peripheriegeräte am digitalen Arbeitsplatz eine oft unterschätzte Angriffsfläche darstellen. Getestet wurden rund 30 in der Schweiz weit verbreitete Tastaturen, Headsets, Webcams und Konferenzsysteme etablierter Hersteller – Geräte, wie sie auf jedem Schweizer Schreibtisch zu finden sind. Das NTC identifizierte über 60 Schwachstellen, darunter 13 schwerwiegende und 3 kritische Befunde. Die Schwachstellen wurden den Herstellern gemeldet und grösstenteils behoben.

Wie konkret diese Risiken sind, zeigt ein reales Szenario: Eine vertrauliche Videokonferenz bei einem Betreiber einer kritischen Infrastruktur ist gut gegen Hackerangriffe geschützt – Netzwerk, Server und Laptop sind auf dem neuesten Sicherheitsstand, die Verbindung ist Ende-zu-Ende verschlüsselt. Ein Angriff ist dennoch möglich: Mit einer Antenne auf dem nahegelegenen Parkplatz fängt ein Angreifer den unzureichend abgesicherten Funkverkehr des drahtlosen Tischmikrofons ab. Innerhalb weniger Sekunden kann er das vertrauliche Gespräch mithören.

Auf diese Weise werden bestehende Schutzmassnahmen über ein unsicheres Peripheriegerät umgangen. Peripheriegeräte bilden die kritische Schnittstelle, über die sensible Informationen fliessen. So werden über Tastaturen Passwörter eingegeben und über Mikrofone und Webcams vertrauliche Gespräche übertragen. Es zeigt sich eine gefährliche Asymmetrie: Die Kosten für professionelle Sicherheitsanalysen übersteigen den Anschaffungspreis solcher Geräte oft um ein Vielfaches. «Peripheriegeräte werden in der Praxis oft als reines Zubehör betrachtet und entsprechend nicht systematisch geprüft sowie nicht konsequent in bestehende Sicherheitskonzepte integriert», sagt Tobias Castagna, Leiter Testexperten beim NTC.

Ergebnisse der Sicherheitsanalyse und zentrale Risikomuster

Um das Sicherheitsniveau weit verbreiteter Peripheriegeräte in der Schweiz systematisch zu beurteilen, hat das NTC im Laufe eines Jahres rund 30 kabelgebundene und drahtlose Geräte einer umfassenden technischen Sicherheitsanalyse unterzogen. In die Auswahl flossen Produkte etablierter Hersteller ein, darunter Geräte von Logitech, Yealink, Jabra, HP, Eizo oder Cherry, die weit verbreitet in der Schweiz und insbesondere auch in kritischen Infrastrukturen eingesetzt werden.

Insgesamt wurden über 60 Befunde unterschiedlicher Kritikalität identifiziert, darunter 13 schwerwiegende und 3 mit höchster Kritikalitätsstufe. Mehrere der Schwachstellen lassen sich in alltäglichen Szenarien durch bekannte Angriffsmethoden ausnutzen. Die Analyse zeigt zugleich, dass moderne Peripheriegeräte bei sicherer Konfiguration und aktueller Firmware ein akzeptables Sicherheitsniveau erreichen können. Die Risiken steigen jedoch mit zunehmender Gerätekomplexität, etwa bei Konferenzsystemen oder sonstigen IoT-Geräten, sowie beim Einsatz veralteter Funktechnologien.

Die identifizierten Schwachstellen wurden den betroffenen Herstellern gemeldet und mehrheitlich rasch behoben. In einem Einzelfall reagierte ein Hersteller jedoch nicht: Bei einem drahtlosen Präsentationssystem übergab das NTC den Fall an das Bundesamt für Cybersicherheit (BACS), das daraufhin eine öffentliche Warnung veröffentlichte.

Der öffentliche Bericht verzichtet bewusst auf technische Details und produktbezogene Schwachstellen. Stattdessen werden übergreifende Risikomuster aufgezeigt, darunter unsichere Standardeinstellungen, Schwächen bei der Gerätekopplung, unzureichend abgesicherte Funkkommunikation sowie Defizite im Firmware- und Lifecycle-Management. Die Untersuchung verdeutlicht, dass Sicherheit bei Peripheriegeräten nicht allein eine Produkteigenschaft ist, sondern wesentlich von Konfiguration, Betrieb und klaren organisatorischen Vorgaben abhängt.

Empfehlungen zur Risikominimierung

Basierend auf den Ergebnissen formuliert das NTC fünf allgemeine Empfehlungen zur Reduktion der Risiken beim Einsatz von Peripheriegeräten insbesondere für Betreiber kritischer Infrastrukturen und Organisationen mit erhöhten Sicherheitsanforderungen:

- Standardisierung und sichere Beschaffung über vertrauenswürdige Kanäle
- Aufnahme von Peripheriegeräten in das IT-Lifecycle- und Asset-Management
- Netzwerksegmentierung für netzwerkfähige Geräte wie Konferenzsysteme
- Bevorzugung kabelgebundener Lösungen in Bereichen mit erhöhtem Schutzbedarf

- Sensibilisierung der Mitarbeitenden für physische und organisatorische Risiken

Die Umsetzung dieser Massnahmen erlaubt es Organisationen, ihre Angriffsfläche mit angemessenem Aufwand deutlich zu reduzieren.

Die Untersuchung erfolgte im Rahmen einer gemeinsamen Initiative des Nationalen Testinstituts für Cybersicherheit NTC mit Unterstützung von Behörden auf Bundes- und Kantonsebene sowie Organisationen aus dem Finanzsektor. Das NTC dankt den beteiligten Organisationen für ihre Unterstützung bei der Durchführung der Analyse. Um die Unabhängigkeit der Resultate zu gewährleisten, waren die Hersteller der getesteten Geräte weder an der Auswahl noch an der Durchführung der Tests beteiligt und wurden erst im Rahmen der vertraulichen Meldung zur Behebung der Schwachstellen kontaktiert.

[Summarischer Bericht Peripheriegeräte](#)

Medienkontakt:

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

Über das Nationale Testinstitut für Cybersicherheit NTC

Das Nationale Testinstitut für Cybersicherheit NTC trägt zur Sicherheit und zur digitalen Souveränität der Schweiz bei, indem es kritische Schwachstellen von digitalen Produkten und Risiken neuer Digitaltechnologien vorausschauend erkennt und deren Mitigation unterstützt. Als gemeinnütziger Verein mit Sitz in Zug folgt das NTC den Prinzipien der Unabhängigkeit und Objektivität. Das NTC testet auf eigene Initiative digitale Produkte und Anwendungen, die in der Schweiz nicht hinreichend getestet werden, jedoch für Wirtschaft und Gesellschaft von grosser Bedeutung sind. Ebenso führt das NTC Cybersicherheitsprüfungen im Auftrag von Betreibern kritischer Infrastrukturen und Behörden durch. <https://www.ntc.swiss>