Wie sicher sind Smartwatches für Kinder?

Katarina Kühn
Referat K 12 – Technischer Verbraucherschutz

Bundesamt
für Sicherheit in der
Informationstechnik

Bild: © AdobeStock/Nirut

Agenda

1. Gesetzlicher Auftrag
2. Untersuchungsreihe „IT-Sicherheit auf dem digitalen Verbrauchermarkt“ im Überblick
3. SiKiWa (IT-**Si**cherheit von **Ki**nder-Smart**wa**tches)
   i. Hintergründe und Ausgangslage
   ii. Vorgehen
   iii. Ergebnisse und Empfehlungen
4. Fragen

Bild: © AdobeStock/Liudmyla

Unsere Stakeholder

Staat

Wirtschaft

Gesellschaft

Wissenschaft

Stellen 2025

1.791

36 %* **Frauen**

64 % **Männer**

*Anteil in Leitungsfunktion: 28 %

Stand: 31.12.2025

Bundesamt für Sicherheit in der Informationstechnik

Gründung

01. Januar 1991

Bundesministerium des Innern

Bundesamt für Sicherheit in der Informationstechnik

Standorte

Stützpunkte

Verbindungsstellen

Prävention

Detektion

Reaktion

- Übernahme technischer Schutzmaßnahmen
- Nationales IT-Lagezentrum
- Technische Unterstützung und Dienstleistungen
- CERT-Bund und MIRTs
- Beratung und Service-Center
- Kooperation
- Allianz für Cybersicherheit
- UP KRITIS
- Begleitung in der Aus- und Fortbildung
- Technische Richtlinien
- Zertifizierung
- IT-Sicherheitskennzeichen

379 Mio. Euro

Haushalt 2026

Gesetzlicher Auftrag

§§ 3 Abs. 1 S. 2 Nr. 21 iVm 14 BSIG

§ 3 Aufgaben des Bundesamtes

„Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen“

§ 14 Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen

(1) „Das Bundesamt kann zur Erfüllung seiner Aufgaben nach **§ 3 Absatz 1 Satz 2 Nummer** 1, 20, **21**, 24 oder 25 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.“

(2) „Soweit erforderlich, kann das Bundesamt für Untersuchungen nach Absatz 1 Satz 1 von Herstellern informationstechnischer Produkte und Systeme alle notwendigen Auskünfte, insbesondere auch zu technischen Details, verlangen…“

IT-Sicherheit auf dem digitalen Verbrauchermarkt

Bild: © AdobeStock/Azazul

Untersuchungsreihe im Überblick

Einordnung

- Eine von drei **priorisierten Säulen** des Digitalen Verbraucherschutz im BSI
- **Hauptziel:** Wirkung nach außen erzielen, die zu sichereren Verbraucherprodukten und -diensten führt
- Primäre **Akteure**:
  - Referat K 12 als Projektleitung
  - Fachexpertise im Haus
  - Hersteller im Herstellerdialog
  - Interne Kommunikatoren
  - Optionale Zusammenarbeit mit externen Projekt-/Kooperationspartnern

Untersuchungsreihe im Überblick

Grundsätzlicher Ablauf

- Themenfindung mit „Pitch“/Begründung aus einer **qualifizierten Marktbeobachtung**
- Definition von **Untersuchungsgegenstand und Marktabgrenzung**
- *optional: Beauftragung externer Dienstleister*
- *optional: Aufteilung der APs intern/extern*
- **Marktsichtung**, Festlegung der **Auswahlmethode** und **Auswahl** der Untersuchungsgegenstände
- Durchführung und begleitender **Herstellerdialog**
- **Abschlussbericht** i.S.v. „Ross & Reiter“ und Ergebnisverwertung
  → *optionale Elemente*: aktive Pressearbeit inkl. Interviews, Fachartikel, Vorträge und Konferenzteilnahmen, Gremienarbeit

Untersuchungsreihe im Überblick

Von der ersten Studie zur etablierten Untersuchungsreihe

Publikation	Software	Hardware
-2021	Gesundheits-Apps	
	Moderne Messenger	
-2023	Onlineshopping-Plattformen	
-2024	Steuererklärungs-Apps	
	Heizkörperthermostate	
-2025	Passwortmanager	
	E-Mail-Programme	
-2026	Kinder-Smartwatches	
	Missbrauch von Smarthome im sozialen Nahraum	
	VPN-Clients	
	Sichere Heimnetzwerke	

Im Rahmen der Marktbeobachtung untersucht das BSI regelmäßig einzelne **Segmente des digitalen Verbrauchermarktes** mittels einer tiefergehenden Analyse.

Auf Basis der gewonnenen Erkenntnisse identifizieren wir **Handlungsbedarfe**, um eine Grundlage für weitere **Zusammenarbeit** zwischen Staat, Wirtschaft und Gesellschaft zu legen.

Landing Page:

https://www.bsi.bund.de/dok/132496

„Ross und Reiter“ nennen

Der neue Umgang mit den Ergebnissen nach § 14 BSIG

- **Ansatz: Wandel der Veröffentlichungspraxis**
  - Wir benennen die konkret untersuchten Produkte zusammen mit den Prüffeststellungen
  - Wir führen einen obligatorischen, vertraulichen Herstellerdialog
- **Wirksamkeit erhöhen**
  - Verbraucher bekommen konkretere Vorschläge für ihre digitale Absicherung
  - Öffentliche Ressourcen werden effizienter eingesetzt
  - „Tue Gutes und sprich darüber“: Berichterstattung und öffentliche Resonanz
- **Rechtsklarheit schaffen**

„Ross und Reiter“ nennen

Wirksamkeit und öffentliche Resonanz

- *"Logins stored in the Firefox Password Manager are now encrypted on disk using a modern encryption scheme (AES-256-CBC), replacing the older 3DES-CBC. This change **improves local data protection**.“* (Mozilla)
- *"We're happy to be one of only few to receive a very positive review without major security concerns. We're also mentioned explicitly for being particularly privacy-friendly. (...) Based on early feedback provided from the BSI (...), version 2.7.11 **changed the default auto-lock setting** after inactivity to "on" with a timeout of 15 minutes."* (keepassxc)
- *„Die Ergebnisse des BSI fliessen konsequent in unsere Verbesserungsmassnahmen ein. [Es wurden] Updates für die mobilen Apps ausgeliefert, die mehrere der im Bericht genannten Punkte adressieren. (…) Falls Sie (…)dennoch beschliessen, unsere Lösung nicht weiter zu verwenden, zeigen wir Verständnis und **akzeptieren (…) eine ausserordentliche Kündigung**.“* (PassSecurium)
- *"S-Trust wird zum 31. März 2026 eingestellt“* (Sparkassen)

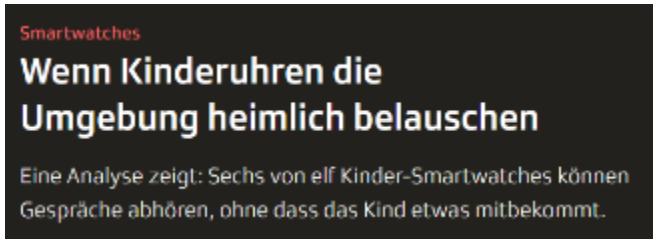
Kinder-Smartwatches

Bild: © AdobeStock/Azazul

Projekt SiKiWa

Hintergründe und Ausgangslage

- Erfassung sensorbasierter Daten, wie z. B. Standort- und Bewegungsdaten und Kombination mit Cloud-Diensten, mobiler App-Steuerung
- oft undurchsichtiger Datenverarbeitung durch internationale Anbieter
- erhebliche Risiken: insbesondere mangelhafte IT-Sicherheit, Sicherheitslücken in den zugehörigen Apps oder Cloud-Diensten sowie fehlende Transparenz hinsichtlich der Datenverarbeitung
- Besonders kritisch: Verarbeitung personenbezogener Daten von Kindern → besonders vulnerable Verbrauchergruppe


Smartwatches

Wenn Kinderuhren die Umgebung heimlich belauschen

Eine Analyse zeigt: Sechs von elf Kinder-Smartwatches können Gespräche abhören, ohne dass das Kind etwas mitbekommt.

Von wegen sicher

So einfach konnten Hacker auf Kinder-Smartwatches zugreifen

Eigentlich sollen Spezial-Smartwatches die Sicherheit von Kindern verbessern. Doch Forscher aus Darmstadt konnten sich problemlos in deren Kommunikation einklinken. Der Hersteller reagiert nur zögerlich.

Projekt SiKiWa

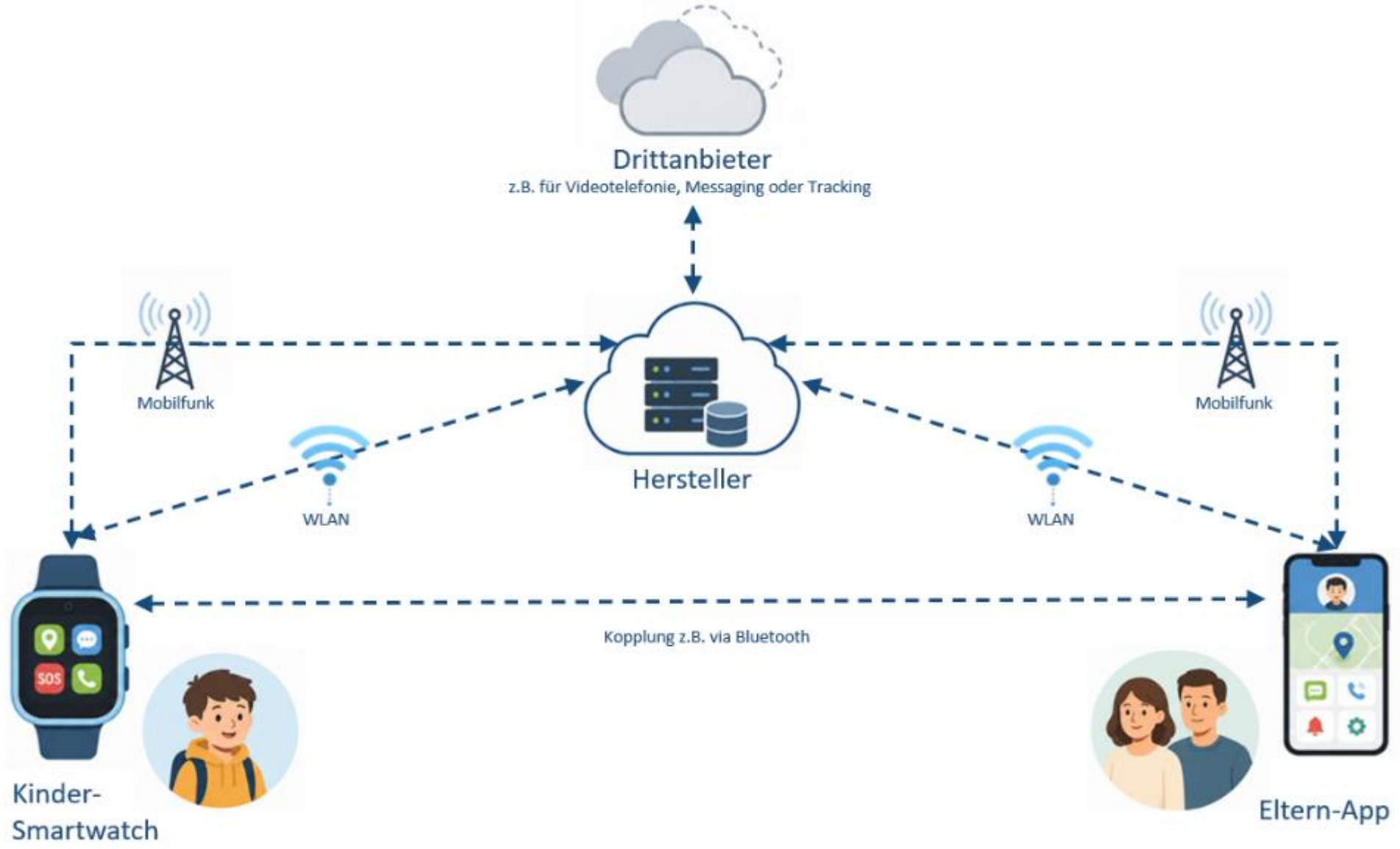
Projektverlauf und Testprodukte

- 3 Kinder-Smartwatches im Test
- Prüfung anhand ausgewählter Kriterien
  - ETSI EN 303 645
  - ETSI TS 103 701
  - OWASP Mobile Application Security Testing Guide (MASTG)
- sowie ausgewählte Fragen zu Parental Control Funktionen der Geräte

Schwachstellenanalyse → Herstellerdialog → Veröffentlichung Abschlussbericht

Projekt SiKiWa

Funktionsweise von Kinder-Smartwatches



Projekt SiKiWa

Zentrale Ergebnisse

- Bei keinem der drei untersuchten Produkte war eine sichere Standardkonfiguration vollständig umgesetzt.
- Zwei der drei untersuchten Kinder-Smartwatches übermittelten Daten teilweise unverschlüsselt.
- Bei allen drei untersuchten Produkten zeigten sich Defizite bei der sicheren Außerbetriebnahme. Insbesondere die Löschung personenbezogener Daten und die Rücksetzung auf einen sicheren Ausgangszustand war nicht zuverlässig möglich.
- Nur bei einem der untersuchten Produkte gab der Hersteller an, wie lange Sicherheitsupdates bereitgestellt werden.
- Nach der Untersuchung der drei Produkte wurden alle Hersteller über die bestehenden Sicherheitsmängel informiert und arbeiteten gemeinsam mit dem BSI an der Behebung.

Projekt SiKiWa

Ergebnisse Garmin Bounce

- Fehlerhafter Löschvorgang:
  - Namen, Nachrichten und weitere Daten bleiben nach dem Löschen des Familienkontos lokal auf der Uhr gespeichert
  - Eine Fehlermeldung statt einer Bestätigung lässt unklar, ob das Familienkonto erfolgreich gelöscht wurde
  - Datenschutzrisiko beim Weiterverkauf
- Uneingeschränkter USB-Zugriff: Über die Garmin-Express-App ist der Zugriff auf die Uhr per USB uneingeschränkt möglich

Projekt SiKiWa

Ergebnisse: Imoo Z3

- Eingeschränkte Kindersicherung: Kinder können standardmäßig Geräteeinstellungen ändern und beliebige Telefonnummern anrufen
- Verbindung mit unsicheren WLAN-Zugangspunkten möglich
- Chat-Nachrichten sowie Bilder und Videos werden teilweise unverschlüsselt übertragen
- Übertragene Informationen zu WLAN-Zugangspunkten können Rückschlüsse auf den Aufenthaltsort des Kindes ermöglichen
- Ein Vorbesitzer kann unter bestimmten Voraussetzungen erneut Zugriff auf die Uhr und den Familienchat erhalten
- Nach dem Löschen eines Kontos verbleiben Daten im App-Speicher

Projekt SiKiWa

Ergebnisse: One2Track Connect Neo

- Datenströme von Videoanrufen werden unverschlüsselt übertragen
- Die Uhr kann keine Sicherheitsupdates empfangen; Informationen zum Supportzeitraum fehlen
- Nach der Löschung des Kontos bleiben Nutzungsdaten auf der Uhr gespeichert
- Unverschlüsselte Daten bleiben auch nach der Kontolöschung im App-Speicher erhalten
- Gespeicherte Daten lassen sich über ein modifiziertes USB-Kabel auslesen

Projekt SiKiWa

Empfehlungen

Auch die Privatsphäre von Kindern sollte bei der Nutzung berücksichtigt werden. Standort- und Kommunikationsfunktionen sollten entsprechend dem Alter des Kindes und dem konkreten Anwendungszweck bewusst eingesetzt werden.

Prüfen Sie, wie lange der Hersteller die Smartwatch mit Sicherheitsupdates versorgen wird und wie diese installiert werden. Erhält eine Smartwatch keine Sicherheitsupdates mehr, sollte sie nicht mehr genutzt werden.

Auf eine kindersichere Konfiguration achten: Nur vorher ausgewählte Kontakte sollten ein Kind über die Smartwatch anrufen können.

Zugänge absichern: Starke, einzigartige Passwörter für Nutzerkonten verwenden und – sofern angeboten – Zwei-Faktor-Authentisierung aktivieren.

Außerbetriebnahme beachten: Vor der Entsorgung oder Weitergabe prüfen, ob sich persönliche Daten sicher löschen und das Gerät auf Werkseinstellungen zurücksetzen lässt.

Projekt SiKiWa

Ergebnisse

- VÖ am 19.10.2026 – siehe Berichterstattungen
- **Primärquellen Untersuchungsbericht:**

DE

https://www.bsi.bund.de/dok/1210076

EN

https://www.bsi.bund.de/dok/1210026

Coming soon

Volle CRAft voraus

- Cyber Resilience Act (CRA) → erste europäische Verordnung, die ein Mindestmaß an Cybersicherheit für alle vernetzten Produkte festlegt, die auf dem EU-Markt erhältlich sind.
  - Vorschriften gelten in allen EU-Mitgliedstaaten und werden schrittweise umgesetzt
  - Ab dem 11. Dezember 2027 gelten alle CRA-Anforderungen
- MissSims (Missbrauch von Smarthome im sozialen Nahraum) → 3. Dezember 2026
- Untersuchung von smarten TV-Boxen und -Sticks
- Untersuchung von VPN-Clients
- Untersuchung von KI-Clients
- (…)

Vielen Dank für Ihre Aufmerksamkeit

Katarina Kühn

Referat K 12 – Technischer Verbraucherschutz

E-Mail: katarina.kuehn@bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

Bild: © AdobeStock/Nirut