

Projekt „Windows seziert“: BSI veröffentlicht Sicherheitsanalysen von Windows Hello for Business

Datum 14.10.2026
Subjekt Bundesamt für Sicherheit in der Informationstechnik
Region Deutschland
Kategorie IT und Kommunikation, Technologie, Sicherheit

Unternehmen, Verwaltung und die Bevölkerung sind auf sichere Betriebssysteme angewiesen. Sicherheitslücken in Betriebssystemen sind daher ein bedeutendes Cybersicherheitsrisiko für Staat, Wirtschaft und Gesellschaft. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den Auftrag, Bewertungen von IT-Systemen und -Komponenten vorzunehmen und Empfehlungen zu deren Einsatz und sicheren Konfiguration auszusprechen.

Um tiefgreifende Analysen verschiedener sicherheitsbezogener Komponenten in den Betriebssystemen Microsoft Windows 10 und Windows 11 durchzuführen, hat das BSI das Projekt „Windows seziert“ gestartet. Als erstes Ergebnis des Projekts wurden heute Analysen zu "Windows Hello for Business" (WHfB) veröffentlicht.

Das BSI analysiert in „Windows seziert“, wie der Authentifizierungsablauf mit Windows Hello for Business technisch funktioniert: Die Analyse beschreibt den Ablauf der Identitätsprüfung, den Windows-Biometriedienst sowie die Schnittstelle „Windows Biometric Framework“ (Nutzung von Fingerabdruck- oder Gesichtserkennung). Zudem wird die Verwaltung und Aufbau der Biometrie-Datenbank und die erweiterte Anmeldesicherheit „Enhanced Sign-in Security“ (ESS) erläutert. Außerdem zeigt die Analyse, wie WHfB in Unternehmen eingeführt wird, welche Konfigurationsmöglichkeiten es für Administratoren gibt und wie Sicherheitsvorfälle erkannt und protokolliert werden können. Ergänzend werden mögliche Angriffsszenarien und passende Gegenmaßnahmen aufgezeigt.

Auf Grundlage der Analysen kann das BSI mehrere Empfehlungen zur Absicherung von Windows Hello for Business ableiten: So sollte unter anderem zur Risikominimierung der ESS-Modus (Sicherheitsmodus Enhanced Sign-in Security) aktiviert werden. Dieser erfordert spezielle, kompatible Hardware („sichere Sensoren“). Des Weiteren sollte, um die Gefahr der gegenseitigen Identitätsübernahme zu verringern, pro Gerät nur eine Person registriert werden. Darüber hinaus werden Härtingsmaßnahmen wie der Einsatz von Trusted Platform Module (TPM) mit Brute-Force-Schutz und eine Festplattenverschlüsselung empfohlen.

Basierend auf diesen Analysen sind IT-Sicherheitsbeauftragte und Administratorinnen und Administratoren in der Lage, zu bewerten, ob Windows Hello for Business für den Einsatz in ihren Szenarien geeignet ist und wie eine sichere Konfiguration vorgenommen werden kann. In den kommenden Monaten werden zahlreiche weitere Veröffentlichungen, z. B. Analysen zu „Protected Process Light“ (PPL) und „Control Flow Guard“ (CFG), mit Ergebnissen aus dem Projekt „Windows seziert“ folgen.

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260715_Projekt_Wi

[ndows_seziert.html](#)