



Hardware Authentifizierung für die Fertigungsindustrie



Der universelle Security Key für digitalen und physischen Zugang

Cyberangriffe zielen zunehmend auf die Fertigungsindustrie ab. Auf diese entfielen 2024 mehr als 25% der weltweiten Cybervorfälle – damit war sie das dritte Jahr in Folge das Hauptziel. Phishing-Angriffe haben zwischen September 2023 und September 2024 um 80% zugenommen. In Deutschland sehen 53% der Unternehmen Phishing als die größte Cyber-Bedrohung.

Um Industrie-4.0-Technologien wie IIoT-Geräte, cloudbasierte Systeme und eingebettete Lieferketten zu schützen, muss der Sektor strenge Sicherheitsmaßnahmen ergreifen und seine Resilienz stärken. Außerdem muss er globale Vorschriften wie FDA, OSHA Standards (USA), EPA Richtlinien (USA), ISO 9001, GMP Richtlinien, NIS2 und KRITIS (EU & Deutschland) einhalten.



Herausforderungen

- **Phishing:** In der Fertigungsindustrie wird Ransomware in der Regel über Phishing-Mails in IT- & OT-Systeme von Unternehmen eingeschleust, was zu Produktionsausfällen führen kann.
- **Use Cases:** Absicherung von branchenrelevanten Daten, vernetzten Arbeitsprozessen, zentralen IT-Netzwerken, OT-Systemen & Zugang zu Gebäuden, Büros und Produktionsstätten.
- **Vorschriften:** FDA, OSHA-Standards (USA), EPA-Richtlinien (USA), ISO 9001, GMP-Richtlinien sowie NIS2 & KRITIS (EU und Deutschland).

Die Zahl der Email-Angriffe auf Unternehmen, die Hersteller ins Visier nehmen, ist um 56 % im Vergleich zum Vorjahr gestiegen.

Source: CSO Online, 2024

Lösung

FIDO Passkeys und Security Keys werden bis 2027 der Goldstandard für die Authentifizierung.

Source: 2025 HYPR State of Passwordless Identity Assurance

- **Digitaler & physischer Zugang mit einem Gerät:** Unterstützung aller wichtigen Zugangssysteme (MIFARE, HID, LEGIC), um jede Fertigungsumgebung nahtlos zu integrieren.
- **Zertifizierte Sicherheit:** Der Smartcard-Chip garantiert mit FIPS 140-3 Level 3 & CC EAL6+ Zertifizierung höchste Sicherheit.
- **Remote-Update-Fähigkeit:** Hält alle Protokolle aktuell, um höchste Sicherheitsanforderungen zu erfüllen.

Benefits

- **Einheitliche Authentifizierung über Systeme hinweg:** Der iShield Key 2 unterstützt nicht nur FIDO2, sondern kann aufgrund der Unterstützung von PKI- und OTP-Anwendungen flexibel & nahtlos in heterogenen Systemen eingesetzt werden.
- **Geringere Komplexität und Kosteneffizienz:** Der iShield Key 2 reduziert Sicherheitsvorfälle, Support-Aufwand und Kosten für das Gerätemanagement, indem er den digitalen und physischen Zugang in einem Gerät vereint.
- **Perfekt für den robusten Einsatz:** Der äußerst robuste iShield Key 2 ist ideal für Produktionsumgebungen geeignet. Er kann dort eingesetzt werden, wo Smartphones nicht erlaubt sind.

Sie haben Fragen?
Kontaktieren Sie uns!

sales@swissbit.com
www.swissbit.com



Feature	iShield Key 2 FIDO2	iShield Key 2 Pro	iShield Key 2 FIDO2 MIFARE	iShield Key 2 Pro MIFARE	iShield Key 2 FIDO2 FIPS	iShield Key 2 Pro FIPS
FIDO2	✓	✓	✓	✓	✓	✓
PIV (Smartcard)		✓		✓		✓
OTP (HOTP, TOTP)		✓		✓		✓
300 Passkeys	✓	✓	✓	✓	✓	✓
MIFARE			✓	✓		
FIPS					✓	✓

About Swissbit

Die Swissbit AG ist das führende europäische Technologieunternehmen für Speicherprodukte und Sicherheitslösungen. Unsere Vision ist eine vernetzte Welt, in der Daten und Identitäten jederzeit vertrauenswürdig sind, um die digitale Souveränität zu gewährleisten.