swissbit®

Beyond the Buzz · it-sa 2026

Sichere Zugänge: Was jetzt zählt

Die wichtigsten Erkenntnisse der it-sa 2026 für Unternehmen

Sicherheit endet nicht bei der Anmeldung

Phishing-resistente Authentifizierung, digitale und physische Zugänge sowie Post-Quantum-Kryptografie stellen Unternehmen vor neue Anforderungen. Entscheidend sind nicht nur sichere Technologien, sondern auch deren Integration in bestehende Systeme und die zuverlässige Verwaltung von Identitäten und Berechtigungen. Dieser Bericht zeigt, welche Entwicklungen die it-sa 2026 geprägt haben, welche Herausforderungen daraus entstehen und welche Lösungen sich bereits umsetzen lassen.



Alexander Summerer
Head of Authentication



Fünf Entwicklungen, die Sicherheit neu definieren

01 Phishing-Resistenz wird zum Maßstab
FIDO2 und Passkeys schützen vor Angriffen über gefälschte Anmeldeseiten. Entscheidend ist, dass Unternehmen unsichere Ausweichverfahren vermeiden.

02 Ein Schlüssel für digitale und physische Zugänge
Gemeinsame Zugangsmedien können getrennte Verfahren vereinfachen. Ihr Nutzen hängt jedoch von der Integration in vorhandene Systeme ab.

03 Die Verwaltung wird zur Sicherheitsfrage
Ausgabe, Registrierung, Ersatz und Sperrung sind bei großen Nutzerzahlen genauso wichtig wie die eigentliche Anmeldung.

04 Post-Quantum-Kryptografie verlangt Vorbereitung
Kryptografische Abhängigkeiten und spätere Umstellungswege müssen frühzeitig bekannt sein, auch wenn der technologische Wandel schrittweise erfolgt.

05 Vertrauen umfasst auch die Lieferkette
Herkunft, Qualitätssicherung und die verlässliche Zuordnung von Sicherheitsschlüsseln zu berechtigten Personen bleiben entscheidend.

Fortschritte bei der Anmeldung – Herausforderungen bei der Verwaltung

35%

Probleme beim Entzug von Zugängen

der Befragten berichteten von Verzögerungen oder Fehlern beim Entzug digitaler und physischer Zugangsberechtigungen in den vergangenen zwei Jahren.

68%

Passkeys gewinnen an Bedeutung

der befragten Organisationen befinden sich in der Einführung, Erprobung oder Bereitstellung von Passkeys für Mitarbeitende.



Quellen: 35%: FIDO Alliance/HID, Untersuchung zur Verwaltung physischer und digitaler Identitäten, 2026; 68%: FIDO Alliance, The State of Passkeys 2026

Warum eine sichere Anmeldung allein nicht reicht

Phishing-resistent ist nicht gleich vollständig geschützt
FIDO2 bindet die Anmeldung kryptografisch an den jeweiligen Dienst. Bei hardware-gebundenen Passkeys verbleiben die privaten Schlüssel auf dem Sicherheitsschlüssel. Gestohlene Sitzungscookies oder kompromittierte Endgeräte bleiben jedoch Risiken. Deshalb gehören Schutzmaßnahmen für Endgeräte und laufende Sitzungen weiterhin zur Sicherheitsstrategie.



Zwei Zugangsbereiche – eine gemeinsame Verantwortung
Der iShield Key 2 kombiniert FIDO2-basierte Authentifizierung mit Technologien für die physische Zutrittskontrolle, je nach Ausführung etwa MIFARE DESFire, HID Seos und LEGIC. Die Verbindung schafft vor allem dann Vorteile, wenn digitale und physische Berechtigungen über abgestimmte Prozesse verwaltet werden. Die Zusammenarbeit von Swissbit und Pointsharp adressiert diese Einbindung.

> Ein Sicherheitsschlüssel für digitale und physische Zugänge ist der technische Ausgangspunkt. Entscheidend ist, dass sich die zugehörigen Berechtigungen im Unternehmen zuverlässig verwalten lassen.

Travis Dunn
Senior Product Manager




Aus der Praxis: Beim gemeinsamen Fachvortrag von Swissbit und Pointsharp ging es um die Verbindung digitaler Authentifizierung mit physischer Zutrittskontrolle. Ein Schwerpunkt lag auf der Einbindung in bestehende Systeme und der Verwaltung von Berechtigungen.

Was Unternehmen erwarten – und wie Swissbit darauf antwortet

Die Gespräche auf der it-sa 2026 zeigten, dass Unternehmen nicht allein nach stärkeren Authentifizierungsverfahren suchen. Ebenso wichtig sind die Integration in bestehende IT- und Zutrittssysteme, die zuverlässige Verwaltung von Berechtigungen und langfristige Investitionssicherheit.



01 Schutz vor Phishing ohne zusätzliche Hürden
Anforderung: Eine robuste, alltagstaugliche Anmeldung.
Swissbit: Der iShield Key 2 unterstützt hardwarebasierte, phishing-resistente Authentifizierung nach FIDO2.

02 Weniger getrennte Zugangsmedien
Anforderung: Digitale und physische Zugänge möglichst einfach nutzen.
Swissbit: Ein Sicherheitsschlüssel kombiniert beide Funktionen, sofern die eingesetzten Zutrittssysteme unterstützt werden.

03 Verwaltung für große Nutzerzahlen
Anforderung: Ausgabe, Ersatz und Entzug von Berechtigungen zuverlässig steuern.
Swissbit: Integrationen mit Partnern wie Pointsharp unterstützen die Einbindung in bestehende Identitäts- und Zugriffsprozesse.

04 Zukunftsfähigkeit ohne vorschnelle Festlegung
Anforderung: Auf kryptografischen Wandel vorbereitet sein und Investitionen schützen.
Swissbit: Angekündigte FIDO- und PKI-Demonstratoren zur Post-Quantum-Kryptografie zeigen Entwicklungsansätze – keine allgemein verfügbare Serienfunktion.

> Unternehmen brauchen heute mehr als eine sichere Anmeldung. Sie benötigen Lösungen, die digitale und physische Zugänge verbinden und sich über den gesamten Lebenszyklus zuverlässig verwalten lassen.



Hendrik Flierman
Sales Director Security Solutions



Sieben Fragen für die nächste Sicherheitsentscheidung

1. **Phishing-Resistenz**
   Welche kritischen Zugänge nutzen noch angreifbare Anmeldeverfahren?
2. **Identitätsprüfung**
   Wie werden Ausgabe, Registrierung und Wiederherstellung abgesichert?
3. **Berechtigungen**
   Wo bestehen getrennte Abläufe für digitalen und physischen Zugang?
4. **Verwaltung**
   Sind Ersatz, Verlust und Entzug auch bei hohen Nutzerzahlen geregelt?
5. **Kryptografie**
   Welche Abhängigkeiten erschweren einen späteren Verfahrenswechsel?
6. **Vertrauenswürdigkeit der Hardware**
   Wie werden Fertigung, Herkunft, Qualität und Lieferfähigkeit geprüft?
7. **Wirksamkeit**
   Wird neben dem Einführungsstand auch die Sicherheit im Betrieb gemessen?

Fazit

Nicht die Anzahl eingesetzter Sicherheitstechnologien entscheidet über eine belastbare Zugriffsstrategie, sondern ihr Zusammenspiel: phishing-resistente Authentifizierung, eine nachvollziehbare Berechtigungsverwaltung, vertrauenswürdige Hardware und die Vorbereitung auf zukünftige kryptografische Anforderungen.



Sichere Zugänge gezielt weiterentwickeln

Erfahren Sie, wie sich phishing-resistente Authentifizierung und physische Zutrittskontrolle mit dem iShield Key 2 verbinden lassen.

Mehr zum iShield Key 2

sales@swissbit.com

© Swissbit AG 2026 – All rights reserved.