Checklist: Is my company ready for passkeys?

Technical requirements

☐ Our identity and access management (IAM) solution supports FIDO2 / WebAuthn.

☐ Our device fleet (e.g., notebooks, smartphones) supports biometric unlocking or secure PIN.

☐ Our applications and platforms can be integrated with modern authentication methods (e.g., SSO, OAuth, OpenID Connect).

☐ Our authentication infrastructure (e.g., Microsoft Entra ID, Okta, Ping Identity) is passkey-compatible or expandable.

☐ Our employees use devices on which private keys can be stored securely (e.g., TPM, Secure Enclave).

Security & Compliance

☐ We have an up-to-date IT security strategy that takes zero trust and passwordless authentication into account.

☐ We can document how passkeys support our compliance requirements (e.g., GDPR, ISO 27001).

☐ We have processes in place for secure recovery in the event of device loss.

☐ We have policies for device security and user identification in mobile environments.

User acceptance & change management

☐ We have a concept for employee training and awareness that communicates the benefits of passkeys.

☐ We consider use cases with different user groups (e.g., internal employees, external parties, partners).

☐ We plan pilot projects to gain experience and insights for the rollout.

☐ We ensure that existing multi-factor authentication (MFA) strategies can be combined with or replaced by passkeys in a meaningful way.

Strategic considerations

☐ The introduction of passkeys is part of our digitalization or IT strategy.

☐ We regularly analyze security incidents and support costs to quantify added value.

☐ We are prepared to gradually replace traditional methods without overwhelming users.

☐ We actively follow technological developments related to passkeys, FIDO2, and identity management.

Recommendation: If you can answer more than 10-12 points with ‘x’, your company is well prepared. Otherwise, we recommend starting with a targeted evaluation or pilot project.