Definition von Shadow-IT

- Shadow-IT bezeichnet die Nutzung von IT-Systemen, Geräten, Software, Anwendungen und Diensten ohne ausdrückliche Genehmigung der IT-Abteilung oder Geschäftsleitung.
- Shadow-IT kann zwar die Produktivität der Mitarbeiter verbessern und zur Innovation beitragen, aber auch ernstzunehmende Sicherheitsrisiken für Ihr Unternehmen mit sich bringen, z. B. durch Datenlecks und potenzielle Compliance-Verstöße.

Warum nutzen Mitarbeiter Shadow-IT?

- Einer der Hauptgründe, warum Mitarbeiter auf Shadow-IT zurückgreifen, ist schlichtweg (aus Sicht des Mitarbeiters) ein effizienteres Arbeiten.
- So kann ein Mitarbeiter beispielsweise eine bessere File-Sharing-Anwendung entdecken als die offiziell genehmigte.
- Ist dies böse Absicht des Mitarbeiters? Nein nicht unbedingt!
- Und die Shadow-IT erstreckt sich nicht nur auf die Unternehmensgeräte, sondern auch auf die persönlichen Geräte der Mitarbeiter wie Smartphones oder Notebooks, was als Bring Your Own Device (BYOD) bezeichnet wird.

Sicherheitsrisiken und Herausforderungen von Shadow-IT

- Das Entscheidende ist, dass wenn die IT-Abteilung von einer Anwendung nichts weiss, sie diese weder unterstützen noch ihre Sicherheit gewährleisten kann.
- Shadow-IT ist nicht per se gefährlich, aber bestimmte Funktionen wie File-Sharing/Speicherung und Zusammenarbeit (z. B. Google Docs) können zu sensiblen Datenlecks führen.
- Neben Sicherheitsrisiken kann Shadow-IT auch unnötige Kosten verursachen, wenn verschiedene Abteilungen unwissentlich die gleichen Lösungen kaufen.

Gibt es auch Vorteile von Shadow-IT?

- Für Mitarbeiter ist oft schwierig eine Genehmigung von der IT für eine neue Software zu erhalten.
- Die Suche nach einem Mittelweg kann es Mitarbeitern ermöglichen, die für sie geeignetsten Lösungen zu finden, während die IT-Abteilung die Daten und Benutzerberechtigungen für die Anwendungen kontrollieren kann.