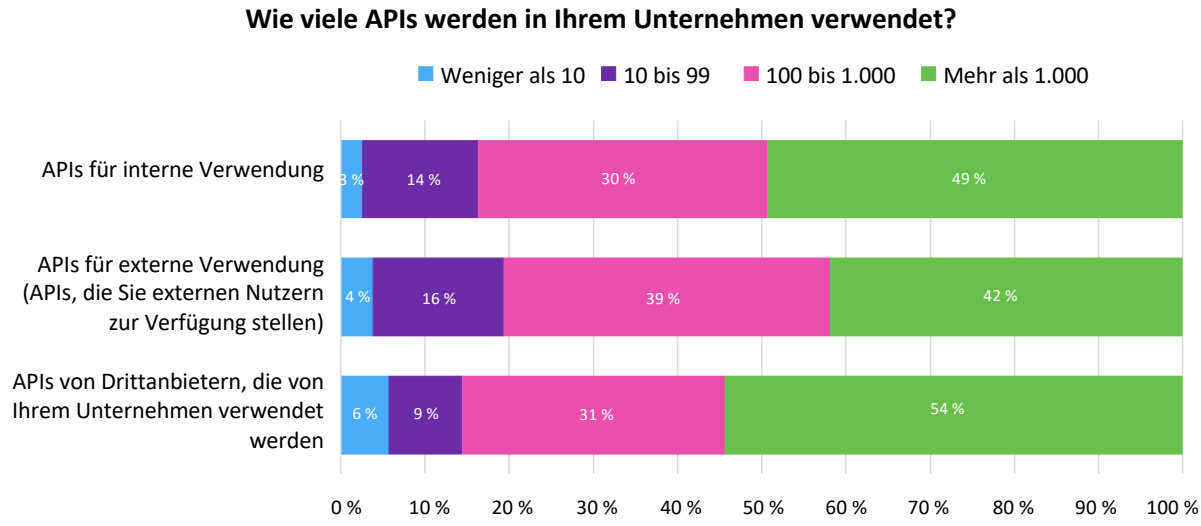
Abbildung 1: Anzahl der verwendeten APIs



Hinweis: n=160
Quelle: Omdia

Die Verwendung von APIs nimmt zu. Gleichzeitig berichteten viele unserer Befragten von API-Sicherheitsvorfällen – mit spezifischen Problemen wie der Extraktion interner Datensätze oder umfangreichem Daten-Scraping.

Dieses Szenario bedeutet, dass Unternehmen ihre API-Sicherheitsbemühungen jetzt verbessern sollten. Denn die Zunahme von APIs wird anhalten und die Sicherheitsprobleme werden noch weiter verschärft, wenn nicht die richtigen Maßnahmen ergriffen werden. Mit zunehmender Anzahl von APIs wird sich die Angriffsfläche weiter vergrößern, was zu mehr potenziellen Angriffen führt.

Eine kurze Einführung zur API-Sicherheit

Der übliche Ablauf der API-Sicherheit konzentriert sich auf vier Hauptanwendungsfälle, die in einer Endlosschleife arbeiten – ähnlich wie beim DevOps-Zyklus „Entwickeln, Bereitstellen, Ausführen, Überwachen“:

- **Erkennung von APIs, die in verschiedenen Umgebungen verwendet werden:** Dies kann auf viele verschiedene Arten geschehen, darunter die Erfassung von OpenAPI-Definitionen (Swagger), das Scannen von Code-Repositorys oder aktive Scans von Umgebungen. Die meisten APIs werden durch Analyse des Traffics erkannt. Das Hochladen von API-Spezifikationsdateien ist eine weniger genutzte Taktik und ist nur möglich, wenn das Unternehmen bereits weiß, welche APIs es hat. Außerdem reicht ein Ansatz allein nicht aus: Die Kombination aus kontinuierlichen Traffic- und Repository-Scans liefert mit hoher Wahrscheinlichkeit einen umfassenden Überblick über die API-Nutzung in Unternehmen.

  Unternehmen müssen die API-Sicherheit in ihrer gesamten Technologieumgebung berücksichtigen, nicht nur in bestimmten API-freundlichen Umgebungen. In vielen Fällen erfordert der Einsatz von Legacy-APIs einen anderen Ansatz.