Mit Security as a Service gegen den Fachkräftemangel - Managed Services als Unterstützung interner IT-Teams

Security as a Service wird bei Grossunternehmen und KMUs immer beliebter: Die sich ständig erweiternde Bedrohungslandschaft und der Mangel an Fachkräften führt zur zunehmenden Akzeptanz von IT-Sicherheit als Dienstleistung. Denn der Arbeitsmarkt bleibt angespannt, in Deutschland gibt es laut Bitkom 82.000 offene Stellen für IT-Spezialisten, und die Nachfrage nach Sicherheitsexperten steigt branchenübergreifend. Für viele Unternehmen ist deshalb eine Auslagerung von Management, Implementierung und Äœberwachung des komplexen Security-Bereichs eine sinnvolle und kosteneffiziente Investition, um ihre internen IT-Ressourcen zu entlasten und zugleich ihr Sicherheitsprofil zu schärfen.

Grundlegende Funktionsweise von Security as a Service

Beim traditionellen Security-Modell verwaltet die interne IT-Abteilung Sicherheitslösungen lokal, installiert Anti-Viren-Schutz, Spam-Filter-Software und andere Sicherheitswerkzeuge auf jeder Maschine, im Netzwerk oder auf dem Server und hält die Systeme auf dem neuesten Stand. Beim Security-as-a-Service-Modell (SECaaS) übernimmt ein externer Security-Dienstleister das Management der Cyber-Sicherheit eines Unternehmens. Im Grunde ist die Verwendung einer Antivirensoftware via Internet das simpelste Beispiel für SECaaS. Im Gegensatz zum traditionellen Ansatz, bei dem Unternehmen Vorlaufkosten für Hardware haben, ermöglicht SECaaS die Verwendung der gleichen Tools einfach per Webbrowser.

Vorteile von Security as a Service im Äœberblick - 1. Konsistenter Schutz durch neueste und aktuellste Sicherheitstools

Programme und Systeme auf dem neuesten Update-Stand zu halten, ist ein entscheidender Baustein für die Unternehmenssicherheit, da veraltete Software ein Einfallstor für Angreifer bietet. Durch Security as a Service arbeiten Unternehmen stets mit den neuesten und aktuellsten Sicherheitstools. Interne IT-Teams müssen sich nicht mehr darum kümmern, dass Benutzer die Antiviren- und andere Software updaten und aktuelle Sicherheitspatches und Virendefinitionen verwenden. Das gleiche gilt für die Aktualisierung und Wartung von Spamfiltern.

2. Externe Sicherheitsexperten als Unterstützung des internen IT-Teams

Durch SECaaS erhalten Unternehmen rund um die Uhr Zugriff auf externe Sicherheitsexperten, die häufig mehr Spezialwissen und Erfahrung als interne IT-Teams mitbringen. Dank der Unterstützung durch externe Fachkräfte können sich interne Security-Spezialisten zudem auf hochwertige Sicherheitsaufgaben konzentrieren, statt Zeit auf administrative Tätigkeiten wie die Wartung der eingesetzten Lösungen zu verwenden. Die Nutzung einer Webschnittstelle oder der Zugriff auf ein SECaaS-Management-Dashboard erleichtert es darüber hinaus dem internen Team, alle Sicherheitsprozesse des Unternehmens im Blick zu behalten.

3. Schnelle Bereitstellung und einfache Skalierbarkeit

Ein weiterer Vorteil von As-as-Service-Angeboten ist, dass IT-Teams Benutzern sofortigen Zugriff auf die eingesetzten Tools geben können. SECaaS-Angebote werden nach Bedarf bereitgestellt und bieten dadurch eine einfache, schnelle und flexible Skalierbarkeit, zugeschnitten auf die Anforderung eines Unternehmens.

4. Kostenersparnis

Durch SECaaS haben Unternehmen keine Vorlaufkosten für Hardware oder Lizenzen. Stattdessen können sie diese durch variable Betriebskosten für die Managed Security-Lösung ersetzen. Dies ist in der Regel günstiger als eine traditionelle In-House-Lösung.

Worauf Unternehmen bei SECaaS-Anbietern achten sollten

Erwägt ein Unternehmen, die Dienste eines SECaaS-Anbieters zu nutzen, gibt es drei Punkte, auf die es zu achten gilt. Unternehmen sollten auf Flexibilität wertlegen, um sicherzustellen, dass die von ihnen gewählten Lösungen keine Interoperabilitätsprobleme aufweisen. Weiterhin ist die Total Cost of Ownership (TCO, Gesamtkosten des Betriebs) ein gutes Kriterium bei der Auswahl eines SECaaS-Anbieters. Man sollte das jeweilige Angebot genau prüfen, sonst bezahlt man am Ende vielleicht mehr für das ausgewählte Paket als bei einem ähnlichen, das nur nominal einen höheren Preis aufweist. Die Lösungen sollten zudem über eine Reporting-Funktion verfügen, die es IT-Teams ermöglicht, wichtige Sicherheitsereignisse, Angriffsprotokolle und andere relevante Daten einzusehen. Der Hauptvorteil von SECaaS besteht

zwar darin, dass ein Drittanbieter die gesamte Sicherheit verwaltet, aber die Transparenz sollte dennoch gegeben sein.
Mit dem Aufkommen der Cloud gibt es heutzutage nahezu keinen Bereich der IT-Infrastruktur, in dem Dienstleister Unternehmen nicht unterstützen könnten. Die gesamte as-a-Service-Umgebung hat es für Unternehmen schneller, einfacher und kostengünstiger gemacht, ihre IT-Anforderungen zu erfüllen, ohne dass sie eine eigene Infrastruktur aufbauen oder in die Entwicklung, Wartung und Erstellung dieser Ressourcen investieren müssen. In Anbetracht des anhaltenden IT-Fachkräftemangels bieten speziell Security-as-a-Service-Angebote daher einen sinnvollen Weg, um interne IT-Teams zu entlasten und zugleich ein hohes Sicherheitsprofil des Unternehmens zu gewährleisten.