Abhilfe bei Fachkräftemangel und knappen Budgets

Für viele Unternehmen ist IT-Security ein Balanceakt zwischen der sorgfältigen Priorisierung von Sicherheitsanforderungen und Budget-Restriktionen. Einige Organisationen konzentrieren sich auf Advanced Threat Protection, um die Flut an Cyberangriffen zu bekämpfen, für andere sind Applikationssicherheit und das Testen von Anwendungen gesetzliche Anforderung und daher kaum verhandelbar. Zudem hat der Anstieg von Bring-Your-Own-Device (BYOD) die Angriffsfläche für Cyberkriminelle enorm vergrößert, und der Schutz vor Datenlecks ist stets ein Hauptanliegen von Unternehmen und muss angemessen berücksichtigt werden.
Eine Option, die deshalb immer beliebter wird, ist die partielle oder vollständige Auslagerung der Security. Durch die Entscheidung für einen Managed Security Service können Unternehmen von externem Spezialwissen profitieren und zugleich die Bereitstellung, Verwaltung und Überwachung von Sicherheitsanwendungen an eine vertrauenswürdige dritte Partei weitergeben. Dieser Ansatz kann die Rentabilität von Security-Investitionen beschleunigen, die Sicherheitseffektivität optimieren und gleichzeitig Kosten reduzieren. Security-as-a-Service-Modelle sind zwar nicht neu auf dem Markt, doch die Ausgereiftheit der verfügbaren Optionen und das immer günstigere Schutz-zu-Kosten-Verhältnis unterstreichen ihren Wert für ein breites Spektrum an Unternehmen.

Interne Bereitstellung versus Managed Security Services

Obwohl sich Managed Services nicht zwangsläufig für jede Organisation oder Branche eignen, sind viele Unternehmen, die diese Dienstleistungen in Anspruch nehmen, der Ansicht, dass sie dadurch für einen Bruchteil der Investitionen, die für eine interne Bereitstellung derselben Lösung erforderlich wäre, Security auf Enterprise-Niveau realisieren können. Im Folgenden drei strategische Vorteile, die Managed Security Services bieten:

1. Zugang zu externen Sicherheitsexperten: Entschärfung des Fachkräftemangels

In der gesamten Cyber-Security-Branche sind erfahrene Fachkräfte das knappste Gut, selbst für Unternehmen mit größeren Budgets. Dies macht Sicherheitsexperten zu einer seltenen und oft teuren Ressource. Die Zusammenarbeit mit einem Managed Services Provider gibt Unternehmen Zugang zu externem Fachwissen, wie es in jedem Service Level Agreement festgelegt ist. Dies bietet große Vorteile, insbesondere für Organisationen mit geringeren Budgets, die sich keine eigenen internen Sicherheitsressourcen leisten können.

2. Flexibler Einsatz durch hybride Modelle: Sensible Daten bleiben on-Premises

Bei einigen Unternehmen erfordert die Sorge um die Sensibilität von Security-Reporting-Daten, dass ihre Infrastruktur on-Premises bleiben muss. Doch für Situationen, in denen der interne Betrieb von Software nicht praktikabel, die Auslagerung der Verantwortung jedoch nicht wünschenswert ist, hat sich ein hybrides Modell herausgebildet: das Hosting von Managed Security Services vor Ort. Bei diesem Ansatz liefert und verwaltet der Provider die im Rahmen des Managed-Security-Programms verwendete Software, während das Unternehmen die Infrastruktur in seiner eigenen IT-Umgebung verwaltet. Alle Daten verbleiben beim Unternehmen, während die Verantwortlichkeiten für die Programmverwaltung vom Managed Security Service Provider übernommen werden. Auf diese Weise können Unternehmen den Security-Betrieb sicher an ihre(n) Managed-Service-Partner auslagern. Dabei werden die Investitionskosten im Vorfeld minimiert, und die Bedenken, dass Daten jeglicher Art das Haus verlassen könnten, ausgeräumt.

3. Schnellere Wertschöpfung von Security-Investitionen

Trotz des allgegenwärtigen Drucks, die Zeit bis zur Wertschöpfung zu minimieren, ist es nicht immer einfach, neue Softwarelösungen intern einzusetzen. Denn interne Teams müssen lernen, mit neuer Software zu arbeiten, die Implementierung erfolgreich zu managen sowie Kollegen zu schulen – neben vielen weiteren Prioritäten. Darüber hinaus können auch die Auswirkungen unerwarteter Verzögerungen aufgrund mangelnder Vertrautheit mit den Tools die Zeit bis zur Wertschöpfung verlangsamen. Durch den Einsatz eines Managed Security Service Providers kann jedoch ein Großteil der Einrichtungszeit und Kosten, die mit der Einführung verbunden sind, entfallen. Darüber hinaus werden Änderungen an der Infrastruktur minimiert oder gänzlich eliminiert, und externe Sicherheitsexperten übernehmen die Verantwortung für Installation, Einführung sowie Schulung aller relevanten Mitarbeiter. Dies führt zu einer schnelleren Implementierung und einer schnelleren Wertschöpfung.

Der Einsatz eines Managed Security Service Providers erfordert eine sorgfältige Abwägung, und die Entscheidung, ob es sich um die richtige Wahl handelt, hängt von einigen Variablen ab. Unternehmen, die über die Zeit, Ressourcen, das Budget oder eine bereits umfangreiche Infrastruktur verfügen, finden die Bereitstellung on-Premises möglicherweise

immer noch am sinnvollsten. Wenn jedoch eine schnellere Wertschöpfung, niedrigere IT-Overheads und zusätzliche Sicherheitsexpertise dringendere Prioritäten sind, kann ein Managed-Security-Service- oder Hybrid-Modell eine äußerst effektive Möglichkeit zur Optimierung der Unternehmenssicherheit sein.