WHITEPAPER

Shared Responsibility Model

sure[secure]

Shared Responsibility Model

Die Einführung von Cloud-Technologien in Unternehmen hat zu einem grundlegenden Wandel in der Art und Weise geführt, wie IT-Sicherheit betrachtet und bewertet werden muss. Ein zentrales Element der Cloud Security ist das Shared Responsibility Model, das die Sicherheitsverantwortung zwischen dem jeweiligen Cloud Service Provider wie z.B. Microsoft, AWS, Adobe, Salesforce und dem Kunden aufteilt.

Für die Verantwortlichen ist es wichtig, das Shared Responsibility Model bestmöglich zu verstehen, um nicht nur die Sicherheitsrisiken in der Cloud bei verschiedenen Anbietern bewerten zu können, sondern auch das inhärente Risiko dieses Modells selbst zu erkennen und darauf aufbauend die richtigen Entscheidungen für die Cybersecurity-Strategie des eigenen Unternehmens treffen zu können, mit dem Ziel, die Cyberresilienz in diesem Kontext zu gewährleisten und/oder zu erhöhen.

Detaillierte Betrachtung der Verantwortungsteilung

Das Shared Responsibility Model basiert auf einer Trennung der Verantwortlichkeiten:

Anbieter-Verantwortlichkeiten:

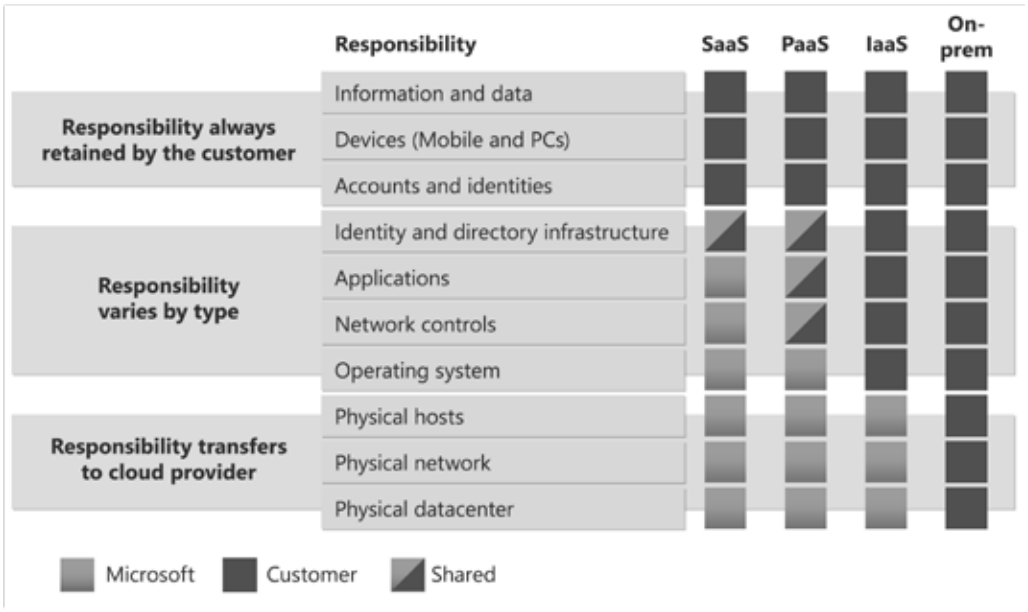
Der Cloud-Service-Anbieter sichert bspw. die Infrastruktur der Cloud, einschließlich Hardware, Software, Netzwerkbetrieb und physische Sicherheit der Datenzentren. Dies umfasst auch den Schutz vor externen Bedrohungen und die Bereitstellung einer sicheren Betriebsumgebung.

Kunden-Verantwortlichkeiten:

Kunden sind für den Schutz ihrer Daten, Anwendungen und Betriebssysteme in der Cloud verantwortlich. Dies kann bspw. die Verschlüsselung von Daten, die Sicherstellung der Anwendungssicherheit und die Verwaltung von Identitäts- und Zugriffsrechten umfassen.

Betrachtung am Beispiel Microsoft 365

Die detaillierte Betrachtung der Verantwortungsteilung im Shared Responsibility Model wird am Beispiel von Microsoft Cloud-Lösungen besonders deutlich. Die folgende Grafik zeigt auf, wo die Verantwortlichkeiten zwischen Anbieter und Kunde liegen und in welchen Bereichen diese fließend sind. Dies hilft, ein besseres Verständnis für die spezifischen Sicherheitsaufgaben beider Parteien zu entwickeln.



Quelle: https://learn.microsoft.com/de-de/azure/security/fundamentals/shared-responsibility

Spezifische Herausforderungen und Lösungsansätze

Die Umsetzung des Shared Responsibility Model in der Praxis bringt spezifische Herausforderungen mit sich:

Klare Grenzen der Verantwortlichkeit:

Oft herrscht Unsicherheit über die genauen Zuständigkeiten, da diese je nach Cloud-Anbieter und Modell (wie IaaS, SaaS etc.) variieren können. Insbesondere bei großen Hyperscalern ist eine direkte Abstimmung meist nicht möglich. Daher ist es entscheidend, relevante Informationen über andere Kanäle, wie online zugängliche Ressourcen, Dokumentationen und spezialisierte Dienstleister zu erhalten. Dies hilft, Missverständnisse zu vermeiden, die im schlimmsten Fall die Angriffsfläche Ihres Unternehmens vergrößern könnten.

Anpassung an verschiedene Cloud-Modelle:

Die Verantwortlichkeiten variieren je nach Cloud-Dienstmodell (IaaS, PaaS, SaaS). Eine genaue Kenntnis der Unterschiede und Anforderungen dieser Modelle ist entscheidend für die richtige Implementierung von Sicherheitsmaßnahmen mit dem Ziel, das Sicherheitsniveau kontinuierlich auf gleichem oder höherem Niveau zu halten.

Management von Multi-Cloud-Umgebungen:

In Multi-Cloud-Umgebungen müssen Sicherheitsstrategien an die verschiedenen Anbieter und Dienste angepasst werden. Dies erfordert ein flexibles und dynamisches Sicherheitsmanagement, um konsistente Sicherheitsstandards über alle Cloud-Plattformen hinweg zu gewährleisten. Hinzu kommt, dass viele Anbieter für ihre Umgebungen das Evergreen-Modell verfolgen, bei dem kontinuierliche Updates durchgeführt werden. Dies bedeutet, dass es nur teilweise oder gar nicht möglich ist, bestimmte Umgebungen auf festen Versionsständen „einzufrieren“, was eine kontinuierliche Anpassung und Überprüfung der Sicherheitsmaßnahmen erfordert.

Best Practices für die effektive Implementierung

Um das Shared Responsibility Model erfolgreich umzusetzen, sollten folgende Best Practices berücksichtigt werden:

Umfassendes Verständnis:

Eine gründliche Kenntnis der Shared Responsibility Models und damit der Verteilung der Verantwortlichkeiten, insbesondere in Bereichen, die nicht direkt mit dem jeweiligen Cloud-Anbieter abgegrenzt werden können, ist von entscheidender Bedeutung. Es ist wichtig, genau zu verstehen, welche Sicherheitsaspekte vom Anbieter abgedeckt werden und wofür er verantwortlich ist.

Risikobewertung und -management:

Es ist wichtig, regelmäßige Risikobewertungen durchzuführen, um potenzielle Sicherheitslücken zu identifizieren und zu schließen. Dies beinhaltet auch die Beurteilung von Compliance-Anforderungen und regulatorischen Rahmenbedingungen. Darüber hinaus sollten Sie die regelmäßigen Informationen und Updates, die Cloud-Anbieter – oft im Rahmen des Evergreen-Modells – per E-Mail oder direkt auf der Plattform bereitstellen, aktiv berücksichtigen und in Ihre Sicherheitsstrategien integrieren. Dies gewährleistet, dass Ihre Sicherheitsmaßnahmen stets aktuell sind und sich an die kontinuierlichen Entwicklungen der Cloud-Umgebungen anpassen.

Fortlaufende Weiterbildung:

Stellen Sie sicher, dass Ihr Team regelmäßig zu den neuesten Cloud-Sicherheitspraktiken geschult wird. In einer sich ständig weiterentwickelnden Landschaft, gekennzeichnet durch das Evergreen-Modell vieler Cloud-Lösungen, sind Bewusstsein und Wissen entscheidend für den proaktiven Umgang mit Sicherheitsrisiken. Kontinuierliche Schulungen stellen sicher, dass Ihr Team mit den neuesten Entwicklungen und Best Practices Schritt hält und effektiv auf die sich verändernde Bedrohungslandschaft reagieren kann.

Einsatz zusätzlicher Sicherheitstechnologien:

Überprüfen Sie regelmäßig, ob die Sicherheitsfunktionen der Cloud-Anbieter ausreichend sind. Da viele Cloud-basierte Lösungen nicht ‚secure by default' sind, ist es entscheidend, in regelmäßigen Abständen zu evaluieren, ob die standardmäßig bereitgestellten Sicherheitsfeatures Ihren Anforderungen genügen. Dies ist besonders wichtig, da im Rahmen des Evergreen-Modells oder durch kontinuierliche Weiterentwicklungen häufig neue Features hinzukommen, die bestehende Lösungen von Drittanbietern möglicherweise überflüssig machen und das Sicherheitsniveau Ihrer Cloud-Ressourcen signifikant erhöhen können.

Regelmäßige Überprüfung und Anpassung der Sicherheitsstrategien:

Die Cloud-Umgebung und die Bedrohungslandschaft entwickeln sich ständig weiter. Eine kontinuierliche Überprüfung und Anpassung der Sicherheitsstrategien ist notwendig, um den aktuellen und zukünftigen Herausforderungen gerecht zu werden...

Management von Multi-Cloud-Umgebungen:

In Multi-Cloud-Umgebungen müssen Sicherheitsstrategien an die verschiedenen Anbieter und Dienste angepasst werden. Dies erfordert ein flexibles und dynamisches Sicherheitsmanagement, um konsistente Sicherheitsstandards über alle Cloud-Plattformen hinweg zu gewährleisten. Hinzu kommt, dass viele Anbieter für ihre Umgebungen das Evergreen-Modell verfolgen, bei dem kontinuierliche Updates durchgeführt werden. Dies bedeutet, dass es nur teilweise oder gar nicht möglich ist, bestimmte Umgebungen auf festen Versionsständen „einzufrieren", was eine kontinuierliche Anpassung und Überprüfung der Sicherheitsmaßnahmen erfordert.

Fazit

Das Shared Responsibility Model ist ein zentraler Aspekt der Cloud-Sicherheit, bei dem eine klare Trennung und gleichzeitig ein Bewusstsein für fließende Verantwortlichkeiten zwischen Cloud-Providern und Kunden notwendig sind. Für Entscheidungsträger ist es unerlässlich, das Modell umfassend zu verstehen, um sowohl die Sicherheitsrisiken als auch die unscharfen Grenzen der Zuständigkeiten richtig einschätzen zu können. Dieses Verständnis ist entscheidend, um die Cyberresilienz zu stärken und eine effektive Cybersecurity-Strategie zu entwickeln. Angesichts der ständigen Weiterentwicklung der Technologie ist eine kontinuierliche Anpassung und ein proaktives Management der Sicherheitsstrategie erforderlich, um mit den Veränderungen der Cloud-Technologie Schritt zu halten.

Thino Ullmann
Business Development & Go-to-Market Manager

Tel.: +49 (2156) 959 45 90
Mail: thino.ullmann@suresecure.de

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de