6 Wege zu mehr Sicherheit mit Cloud Computing

Die Einführung von Cloud Computing zwingt Unternehmen dazu, sich zwischen der Kosteneffizienz, Skalierbarkeit und Benutzerfreundlichkeit einer Cloud-Umgebung und dem Komfort des sicheren Hostings von Daten und Anwendungen auf ihren eigenen Servern zu entscheiden. Aber ist On-Premise wirklich sicherer als Cloud Computing? Viele Fachleute antworten hier mit nein. Die folgenden 6 Aspekte zeigen Ihnen, warum Sie ohne Bedenken auf Cloud Computing umsteigen können.

1 Sicherheit ist teuer

Sicherheit kostet Geld. Fragen Sie sich: Was kann sich mein Unternehmen wirklich leisten? Das Deployment der erforderlichen Sicherheitsmaßnahmen für ein On-Premise-Rechenzentrum ist in der Tat kostspielig, insbesondere für kleine und mittlere Unternehmen. Ein Sicherheitsniveau zu erreichen, wie es Hyperscaler ihren Kunden bieten können, ist nicht praktikabel.

2 Sicherheit erfordert erhebliche Personalressourcen

Sicherheit erfordert auch einen höheren Personalaufwand. Große Cloud-Anbieter beschäftigen rund um die Uhr Sicherheitsteams und ein umfassendes Security Operations Center, das die IT-Infrastruktur und die physische Hardware kontinuierlich überwacht. So ist beispielsweise ein Team aus mehr als 3.500 Fachleuten für Cybersicherheit für den Schutz von Microsoft Azure verantwortlich. Die meisten Unternehmen verfügen nicht über die personellen Kapazitäten, um das gleiche Maß an Sicherheit wie Hyperscaler zu gewährleisten.

3 Cloud-Anbieter sind im Sicherheitssektor tätig

Sicherheit ist Ihnen wichtig, aber sie ist nicht Ihr Geschäft. Sicherheit ist zwar eines Ihrer zahlreichen Anliegen, aber auch eine der höchsten Prioritäten für Cloud-Anbieter. Um im Geschäft und wettbewerbsfähig zu bleiben, müssen Cloud-Anbieter ihren Kunden ein Höchstmaß an Sicherheit bereitstellen. Google Cloud bietet zum Beispiel eine „Secure by Design-Infrastruktur" mit integriertem Schutz und standardmäßiger Verschlüsselung.[1]

Microsoft Azure hilft bei der Identifizierung von Bedrohungen „durch das Analysieren umfangreicher Quellen, darunter 18 Milliarden Bing-Webseiten, 400 Milliarden E-Mails, 1 Milliarde Windows-Geräte-Updates und 450 Milliarden monatliche Authentifizierungen mithilfe von maschinellem Lernen, Verhaltensanalysen und anwendungsbasierter Intelligenz als Teil des Microsoft Intelligent Security Graph".[2]

Cloud-Anbieter müssen hohe Standards erfüllen, einschließlich unabhängiger, international anerkannter Zertifizierungen und Audits von Sicherheitspersonal, -prozessen und -technologien durch eine Reihe strenger Programme. Amazon Web Services (AWS) erhält beispielsweise regelmäßig eine Validierung durch Dritte für Tausende von globalen Compliance-Anforderungen. Den meisten Unternehmen fehlen Zeit, Ressourcen oder Budget zum Erreichen dieses Sicherheitsniveaus.[3]

1 *„Vertrauen und Sicherheit". Google, Zugriff am 29. April 2022.*

2 *„Strengthen your security posture with Azure". Azure, Zugriff am 29. April 2022.*

3 *„AWS Cloud Security". Amazon, Zugriff am 29. April 2022.*

4 Fortschrittliche Sicherheitstools

Cloud-Anbieter setzen eine Reihe fortschrittlicher Sicherheitstools zum Schutz der Anwendungen und Daten ihrer Kunden ein. AWS bietet präzise Identitäts- und Zugriffskontrollen, kontinuierliche Überwachung, Bedrohungserkennung, Netzwerk- und Anwendungsschutz, mehrere Verschlüsselungsebenen, automatisierte Wiederherstellung und Reaktion auf Vorfälle und vieles mehr. Hyperscaler ermöglichen den Zugang zu Hunderten von zusätzlichen Sicherheitslösungen, die auf den Marktplätzen ihrer Partner verfügbar sind. Es ist praktisch unmöglich, dieses breite Spektrum an fortschrittlichen Sicherheitstools in Ihrem eigenen Netzwerk und Rechenzentrum zu duplizieren. Die Kosten, der Personal-, Zeit- und Arbeitsaufwand sind für ein nicht auf Sicherheit spezialisiertes Unternehmen zu hoch.

5 Netzwerksegmentierung

Ein Vorteil für die Sicherheit in einer Cloud-Umgebung ist die Segmentierung der Workstations von Nutzenden. Eine gängige Methode bei Cyberangriffen besteht darin, bestimmte Nutzende des Systems über E-Mails und Websites anzugreifen. In diesen Fällen erfolgt der Zugang zum System über die Workstations der Nutzenden. In einer Cloud-Umgebung sind die Workstations der Nutzenden nur so weit vernetzt, wie es die Nutzenden zur Erledigung ihrer Aufgaben benötigen. Die Workstations haben keinen direkten Zugang zum Unternehmensnetzwerk. Selbst wenn also eine Workstation kompromittiert wird, erhält der Angreifer so keinen Zugriff auf das Unternehmen und seine Anwendungen und Daten.

6 Physische Sicherheit

Die physische Sicherheit ist immer noch ein entscheidender Faktor. Personen mit direktem physischen Zugang zu Hardware können ein erhebliches potenzielles Sicherheitsrisiko darstellen. Wenn sich Daten und Anwendungen jedoch in einer Cloud-Umgebung befinden, haben unzufriedene Beschäftigte – und andere Personen, die vor Ort arbeiten und versehentlich Schaden anrichten können – keinen unmittelbaren Zugriff mehr auf diese Assets. Für sie ist es viel schwieriger, die Daten in einer Cloud-Umgebung zu finden.

Darüber hinaus verfügen Hyperscaler über die erforderlichen Ressourcen, um physischen Datendiebstahl zu verhindern, wie z. B. Sicherheitspersonal, verschlossene Serverschränke und andere moderne physische Sicherheitskontrollen, die bei den meisten Unternehmen nicht vorhanden sind.

Weiterlesen

Im Whitepaper „Unterstützung von Entwicklungsteams durch Cloud Services“ gewinnen Sie weitere Insights dazu, wie Red Hat® Cloud Services Sie bei der Umstellung auf cloudnative Anwendungen unterstützen kann.

EUROPA, NAHOST UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

de.redhat.com
#F31540_0522