Sicherheit in einer hybrid Multi-Cloud Umgebung

Martin Runde | Marketing Manager Security DACH | 17. September , 2020

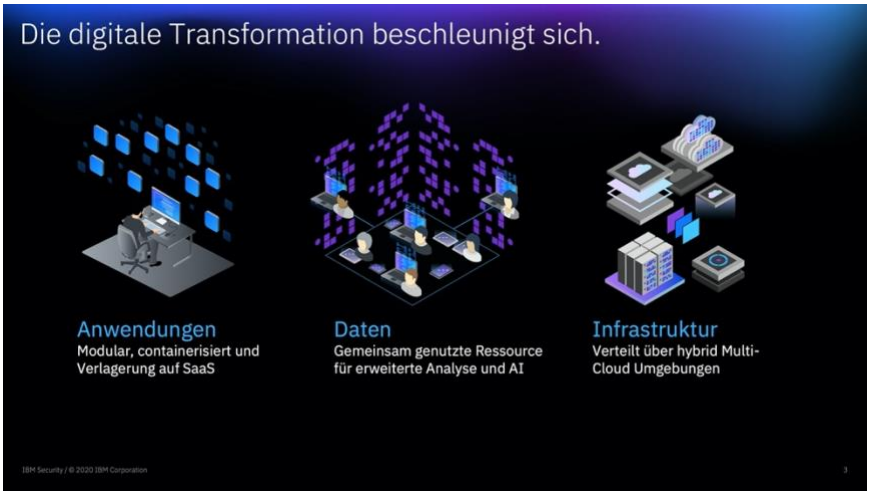
IBM Security

Der Einsatz von Cloud Technologien ist die wohl größte Herausforderung der IT-Sicherheit. Wie gelingt es Sicherheitsteams mit dieser Herausforderung umzugehen?

Die Arbeit in einem Sicherheitsteam kann frustrierend sein. Sie haben es nicht nur mit sich stetig verändernden Angriffsmustern zu tun, sondern sind auch gezwungen ihre Sicherheitsstrategie kontinuierlich, an die sich schnell ändernden Geschäftsanforderungen anzupassen. Dabei ist die in den vergangenen Jahren zunehmende Adaption von Cloud Technologien die wohl größte Veränderungen in der Geschäftswelt und gleichermaßen die größte Herausforderung für die Sicherheitsteams. Mit dem stetigen Bestreben die Sicherheitsanforderungen, die der Weg zur Cloud- und Anwendungsmodernisierung mit sich bringt, zu bewältigen, haben viele Unternehmen Ihre Situation jedoch möglicherweise noch verschlimmert.

Lassen Sie uns dies etwas genauer betrachten.

Wenn Unternehmen ihre Geschäftsprozesse in die Cloud verlagern, werden die Daten zwischen einzelnen Standorten und mehreren Cloud-Ökosystemen fragmentiert. Für Sicherheitsteams kann es herausfordernd sein, in solchen Infrastrukturen einen Überblick über die Risiken und Bedrohungen zu erhalten. Im Laufe der Jahre haben viele Unternehmen deshalb begonnen neue, spezialisierte Tools einzusetzen, um dieses Problem zu lösen.



Dies hat zu einer Fülle von Sicherheitswerkzeugen geführt. Eine von Forrester Consulting im Auftrag der IBM durchgeführte Studie ergab, dass 91 Prozent der Organisationen mit sich mit der zunehmenden Komplexität ihrer Sicherheitsinfrastruktur zu kämpfen haben. Im Durchschnitt verwalten Organisationen 25 verschiedene Sicherheitsprodukte oder -Dienstleistungen von 13 Anbietern. Der aktuelle „Cost of a Data Breach Report" identifiziert die Komplexität der Sicherheitsinfrastruktur folgerichtig als den größten Kostentreiber im Falle einer Datenschutzverletzung.

Zusätzlich führen verteilte Dienste zu einer explosionsartigen Zunahme von Sicherheits-Daten. Viele Organisationen führen diese Daten zur Erkennung und Analyse von Bedrohungen und Risiken zusammen. Die resultierenden Datenspeicher sind allerdings mit eigenen Herausforderungen verbunden.

Schließlich verstärkt die Vielzahl der eingesetzten Tools ein weiteres Problem: jedes verfügt über unterschiedliche Datenbestände, Benutzeroberflächen und Arbeitsabläufe. Dies kostet Sicherheitsteams zusätzlichen Zeit-, Integrations- und Wissensaufwand.

Sind Unternehmen mit zu vielen unzusammenhängenden Tools und zu vielen unzusammenhängenden Daten konfrontiert, so steigt das Risiko eine Bedrohung zu übersehen oder die Durchführung einer gründlichen Untersuchung und die Koordinierung einer Reaktion nicht zeitnahe durchzuführen, wodurch die Auswirkungen eines Angriffs möglicherweise noch verstärkt werden können.

Moderne Sicherheitssysteme sind keine Inseln; sie müssen miteinander verbunden werden, um sie so effektiv zu gestalten, wie Organisationen sie brauchen. Dies bedeutet zum einen die Verbindung vorhandener Tools und Datenbestände, um Details über Bedrohungen und Risiken zu gewinnen, die das Unternehmen gefährden. Zum anderen, die Verbindung und Automatisierung von Arbeitsabläufen, um die Reaktion auf einen Sicherheitsvorfall unternehmensweit auf allen Ebenen zu koordinieren und Reaktionszeiten zu verbessern.

Wir unterstützen Organisationen, diese Herausforderungen zu bewältigen. Mit IBM Cloud Pak for Security bieten wir eine Plattform, die vorhandenen Sicherheitstools unterschiedlicher Hersteller integriert, um tiefere Einblicke in Bedrohungen in hybriden Multi-Cloud-Umgebungen zu gewinnen. Hierbei verwenden wir eine infrastrukturunabhängige gemeinsame Betriebsumgebung, die überall ausgeführt werden kann. Sicherheitsteams können schnell nach Bedrohungen suchen diese analysieren und die Reaktion mit automatisierten Aktionen orchestrieren - ohne die zugrunde liegenden Daten zu verschieben.

Mit IBM Cloud Pak for Security sind Sie in der Lage die bestehende Sicherheitslandschaft eines Unternehmens auf die vielschichtigen Anforderungen einer modernen hybrid Multi Cloud Umgebung anzupassen.