



Cloud Security Assessment von Controlware

Erfahren Sie den aktuellen Sicherheits-/Compliance-Status Ihrer Cloud-Umgebung und schützen Sie sich kontinuierlich vor möglichen Bedrohungen

Die meisten Sicherheitsvorfälle im Zusammenhang mit Cloud Umgebungen resultieren durch Fehlkonfigurationen von Anwendern.

Durch die Nutzung von Cloud Services ergeben sich für Unternehmen viele Chancen um im Rahmen der Digitalisierung an Schnelligkeit und Agilität zu gewinnen. Gleichzeitig nehmen Schlagzeilen über Sicherheitsvorfälle in Bezug auf Cloud Umgebungen (z. B. Datenpannen durch öffentlich zugängliche AWS S3 Buckets) zu. Ist die Cloud deshalb unsicher?

In den meisten Fällen sind diese Sicherheitsvorfälle auf Fehlkonfigurationen und mangelndes Sicherheitsbewusstsein zurückzuführen, nicht auf Nachlässigkeiten durch Cloud Provider. Diese propagieren seit Jahren ein Shared Responsibility Modell in dem, je nach Servicemodell, unterschiedliche Verantwortlichkeiten beim Cloud Provider, aber auch beim Cloud Nutzer verortet werden. Die letztendliche Pflicht zur Compliance gegenüber Kunden und die regulatorischen Pflichten bleiben beim Service Owner der Cloud Services!

Aber wie können Unternehmen die Vorteile von Cloud Umgebungen nutzen, gleichzeitig den Überblick über ihren Sicherheitsstatus behalten, sowie Compliance Vorgaben erfüllen? Das Controlware Cloud Security Assessment wird Ihnen diese Frage beantworten und Ihnen einen möglichen Rahmen aufzeigen.

Was bietet Ihnen das Cloud Security Assessment?

- Erkennung von potentiellen Sicherheitsmängeln und Fehlkonfigurationen
- Sichtbarkeit Ihrer (Multi-)Cloud Umgebung/en
- Reduktion des Risikos durch Datenpannen und Sicherheitsvorfällen
- Stärken Ihrer Wettbewerbsposition gegenüber der Konkurrenz
- Einhaltung von gesetzlichen Vorgaben und Regularien (z. B. ISO 27001)

Was bietet Ihnen das Cloud Security Assessment?

- Professionelles Assessment Ihrer aktuellen Konfiguration
- Umfangreiche Handlungsempfehlung als Grundlage, um die Sicherheit in Ihrem Unternehmen zu steigern
- Kosteneffiziente und zeitnahe Durchführung durch etablierte Verfahren
- Controlware als Partner bietet mehrjährige Erfahrung im Bereich Security und unterstützt Sie auch bei der Umsetzung.



Warum sollte ein Cloud Security Assessment durchgeführt werden?

Durch die im Cloud Security Assessment festgestellten Findings, wird Ihnen eine zuvor nicht gegebene Sichtbarkeit auf Ihre Cloud Workloads und deren Sicherheitsstatus gegeben. Sie erhalten Maßnahmenempfehlungen um Fehlkonfigurationen zu vermeiden, Best Practices umzusetzen, das Sicherheitsniveau zu erhöhen und die Compliance gegenüber Aufsichtsbehörden und Auditoren nachzuweisen.

Auf Basis der gesammelten Erkenntnisse bietet die Controlware weiterführende Workshops und Beratung im Rahmen des Business Consulting an.



CSPM – Die Methodik hinter dem Cloud Security Assessment

Um die Sicherheit und Compliance in einer Single-, Hybrid-, oder Multi-Cloud Umgebung zu überwachen ist ein kontinuierlicher Prozess nötig. In diesem Prozess werden bestehende und neue Deployments überwacht, bewertet und die Ergebnisse werden schnellstmöglich an Entwickler, Dev(Sec)Ops-Team oder Betriebseinheiten zurückgegeben. Es reicht daher nicht mehr aus, diese Überwachung nur sporadisch im Rahmen von Assessments oder Audits durchzuführen und nachzuweisen, sondern es muss ein kontinuierlicher, wiederholbarer und automatisierter Prozess eingeführt werden.

Das Marktforschungsunternehmen Gartner hat hierzu den Begriff Cloud Security Posture Management definiert. Hier werden Prozesse, Tools und Methoden zusammengefasst, die ein kontinuierliches Risikomanagement und Business Continuity Management in Cloud Umgebungen sicherstellen. Unterstützt wird dies durch Hersteller wie z. B. Check Point oder Palo Alto Networks. Diese Lösungen kommen im Rahmen des Cloud Security Assessments zum Einsatz.



Die Ziele des Cloud Security Assessments

Im Rahmen eines mehrtägigen Cloud Security Assessment wollen wir Ihre Cloud Umgebungen in einem kontinuierlichen Prozess überwachen. So können Fehlkonfigurationen, Risiken, aber auch Verstöße gegen interne Compliance-Vorgaben aufgedeckt werden. Der Fokus liegt auf einer automatisierten, dokumentierten, sowie wiederholbaren Überprüfung von Cloud Services, unterschiedlichen Compliance Vorgaben (bspw. nach ISO 27001, PCI-DSS) oder speziellen, kunden-spezifischen Regularien und Anforderungen.

Welche Bereiche deckt das Cloud Security Assessment ab?

Die Überprüfung von Infrastructure-as-a-Service (IaaS) und Platform-as-a-Service (PaaS) Diensten der führenden Cloud Anbieter:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

Im Rahmen des Assessments werden auch Quick-Wins aufgezeigt, leicht zu behebbende Fehlkonfigurationen und Risiken, die im Falle einer Datenpanne oder eines Sicherheitsvorfalls einen Schaden für Ihr Unternehmen nach sich ziehen könnten. Sie erhalten konkrete Empfehlungen welche Änderungen notwendig sind um erkannte Sicherheitslücken zu schließen.

Security Assessments können den Grundstein legen für eine weiterführende Zusammenarbeit mit der Controlware, einem der führenden deutschen Systemintegratoren, in den Themenbereichen:

- Netzwerk-Infrastruktur
- IT-Security und
- Datacenter/Cloud

Zentrale

Controlware GmbH

Waldstraße 92
63128 Dietzenbach

Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de