Orange
Cyberdefense

Cloud Security

Klare Sicht – auch bei dichten Wolken.

Kaum ein modernes Unternehmen kommt noch an Cloud-Diensten vorbei. Die Vorteile der Cloud-Nutzung sind einfach zu vielfältig. Die Cloud macht vieles schneller und einfacher. Nur nicht die Security. Aber dafür sind ja auch wir zuständig!

Sie sind überall.

Cloud-Dienste schießen wie Pilze aus dem Boden und erfreuen sich unter kreativen Mitarbeitern großer Beliebtheit, ermöglichen sie doch oft schnelle und unkomplizierte Lösungen. Allerdings nur auf den ersten Blick, denn der mitunter sorglose Umgang mit vertraulichen Daten verursacht für das Unternehmen erhebliche Risiken. Oft fehlt den Anwendern das nötige Wissen, um zu beurteilen, ob ein Cloud Service für Kommunikation oder Datentransfer in Bezug auf Sicherheitsfragen geeignet ist.

Wie IT-Abteilungen die Kontrolle zurückerlangen

Interne IT-Abteilungen haben hier Probleme. Besonders dann, wenn im Unternehmen keine offizielle Richtlinie zur Nutzung von Cloud Services eingeführt wurde, herrscht gefährlicher Wildwuchs. Um diesen einzudämmen, müssen die Verantwortlichen die Kontrolle zurückerlangen. Im ersten Schritt heißt das, sich einen Überblick über die genutzten Cloud Services zu verschaffen, diese nach wirtschaftlicher Notwendigkeit, Sicherheit, Kosten, Alternativen etc. zu bewerten und nachfolgend die notwendigen Dienste für das Unternehmen in geeigneter Weise anzubieten z.B. über einen zentralen Cloud Access Security Broker Service (CASB).

» Im Nebel herumstochern bringt nichts. Wer die Cloud sicher nutzen will, braucht in erster Linie Durchblick: eine zuverlässige Navigationshilfe. «

David Kühner // Senior Consultant IT-Security, Orange Cyberdefense Germany GmbH

Mehr zu unseren Services finden Sie auf:
orangecyberdefense.com/de/cloudsecurity

Mit dem Cloud Shadow Assessment zum Durchblick

Das Orange Cyberdefense Cloud Shadow Assessment bietet Ihnen die technische und organisatorische Basis zur Erfassung, Analyse und Bewertung aktuell genutzter Cloud Services und damit wertvolle Informationen für Ihre Cloud Security Strategie.

Die Analyse zeigt auf, welche Cloud-Dienste mit welcher Intensität verwendet werden, während die sicherheitstechnische Bewertung die dazugehörige Risikoeinstufung liefert.

Allein durch die Kenntnis, wie weit verbreitet der „Wildwuchs“ an Cloud-Diensten und wie gefährlich deren Einsatz ist, liefert das Assessment einen unschätzbaren Mehrwert.

Anhand dieser Erkenntnisse können Sie entsprechende Maßnahmen wie das Blocken oder das Absichern bestimmter Dienste ergreifen und so Verluste von unternehmenskritischen Daten verhindern, sowie Probleme aus regulatorischer Sicht vermeiden.

Diese Antworten liefert das Assessment:

- Welche Cloud-Dienste werden im Unternehmen verwendet?
- Wie intensiv und von wem werden diese Cloud-Dienste verwendet?
- Wie sind diese Cloud-Dienste aus Sicht der IT-Sicherheit zu bewerten?
- Ist es möglich, diese abzusichern oder müssen sie geblockt werden?

Nutzen & Ergebnisse

- Überblick zu den aktuell verwendeten Cloud Services
- Überblick der jeweiligen Nutzungsintensität
- Risikobewertung der jeweiligen Anwendung
- Empfehlung zur Absicherung
- **Optional:**
  Entwicklung einer Cloud-Security-Strategie

Ein zuverlässiger Cloud-Wächter: CASB

Kurz gesagt: Der Cloud Access Security Broker (CASB) ist Ihr Regenschirm. Korrekt in die Sicherheitsinfrastruktur integriert, macht er die Cloud für Sie transparent und kontrollierbar. Das Prinzip eines CASB ist es, eine zentrale Oberfläche zur Verfügung zu stellen, von der aus man die Security der im Unternehmen verwendeten Cloud-Dienste sichtbar machen und steuern kann.

Ein CASB regelt den Datenverkehr in- und aus der Cloud und stellt sicher, dass Ihre Regeln nicht an der Grenze des Firmenperimeters enden. Dabei ist er die zentrale Anlaufstelle für alle Cloud-Dienste und Plattformen. Zusammen mit Firewalls und DLP-Systemen sorgt der CASB dafür, dass Ihre Daten sicher bleiben, auch in der Cloud.

Diese Antworten liefert das Assessment:

- Kontrolle: Welche Dienste werden verwendet?
- Konfiguration: Verwendete Dienste können verwaltet werden (je nach Dienst unterschiedlich).
- Transparenz: Die APIs der Dienste werden verwendet, um den Inhalt zu scannen und Nutzungsdaten zu erhalten.
- Schutz: Man kann DLP Richtlinien einrichten, um den Datenfluss zu kontrollieren.
- Automatisierung: Je nachdem, welche Daten zu einem Dienst fließen, können verschiedene Aktionen ausgeführt werden z.B. Tokenisierung oder Verschlüsselung.
- Flexibilität: Deployment Modelle sind: Reverse Proxy, Forward Proxy, API. Ggfs. hilft ein Agent bei manchen CASBs (z.b. für Mobile Devices).
- Integration: Integriert werden ggfs.: IAM/IDaaS für die Anmeldung am Dienst, DLP anstatt des eingebauten DLP oder zusätzlich, Proxy (zum Blocken), Verschlüsselungsmethoden wie ein HSM Modul. Ein Anschluss an ein SIEM ist ebenfalls sinnvoll.

Mehr Infos finden Sie auf
www.orangecyberdefense.de

Orange Cyberdefense
Paul-Gerhardt-Allee 24, 81245 München

info@de.orangecyberdefense.com
+49 89 2000148 00