consol

CLOUD SECURITY IN DER PRAXIS:

HERAUSFORDERUNGEN & BEST PRACTICES

CONSOL LEITFADEN

Wie kann man als Unternehmen mehr Sicherheit in der Cloud erreichen und sich optimal schützen?

ConSol zeigt Ihnen, auf welche Herausforderungen Sie beim Thema Cloud-Sicherheit achten sollten und gibt Ihnen Best Practices an die Hand.

HERAUSFORDERUNGEN BEI DER CLOUD-SICHERHEIT

1. **MIGRATIONSRISIKEN:** Wenn Anwendungen unter Zeitdruck in die Cloud übertragen werden, können Fehler passieren. Applikationen sind nicht ausreichend getestet und auf Sicherheitsstandards überprüft.

2. **FEHLENDE ÜBERSICHTLICHKEIT UND TRANSPARENZ:** Durch Nutzung der Cloud wird es schwierig, den Überblick zu behalten. Der Zugriff erfolgt auf viele Cloud-Dienste außerhalb des Unternehmensnetzwerks und über Dritte. Transparenz ist weit schwerer zu erreichen. Gerade in mittleren und großen Unternehmen greifen eine Vielzahl von Endgeräten von verschieden Abteilungen oder Standorten auf die Cloud-Services zu. Die Cloud-Infrastruktur wird komplex und unübersichtlich, wenn sie nicht konsequent gemanagt wird.

3. **MULTI-TENANCY-ARCHITEKTUR**: Bei einer Multi-Tenancy-Architektur wird nicht für jeden einzelnen Kunden eine dezidierte Infrastruktur bereitgestellt. Eine einzige Softwareinstanz versorgt mehrere unterschiedliche User. Jeder User hat zwar eigene Zugriffsrechte und Konfigurationsdetails, greift jedoch auf die gleiche Systemumgebung zu. Das ist zwar einer der großen Vorteile einer Cloud. Performance- und Sicherheits-Aspekte müssen je nach Ausprägungsmodell der Cloud und Anwendungsfall durchdacht werden.

4. **ZUGANGSVERWALTUNG UND SCHATTEN-IT:** Unternehmen mit lokaler Hardware sind in der Lage, Zugriffspunkte erfolgreich zu verwalten. Die Zugriffsverwaltung in der Cloud kann eine Herausforderung darstellen.

5. **FEHLKONFIGURATIONEN:** Falsch konfigurierte Assets können zu einem Schlüsselproblem in der Cloud-Umgebung werden. Zu den Fehlkonfigurationen zählen unzureichende Datenschutzeinstellungen oder die Beibehaltung standardmäßiger Administratorkennwörter.

6. **RISIKEN DURCH UNGESICHERTE APIS** (Application Programming Interfaces): APIs stellen potentiell ein Sicherheitsrisiko dar. Sowohl eigene APIs als auch die der Cloud-Provider müssen hinreichend abgesichert werden. Andernfalls können Hacker darüber unbefugten Zugriff auf Daten in der Cloud erhalten.

7. **COMPLIANCE:** Im Zusammenhang mit Cloud-Technologien sind einige Compliance-Vorgaben zu berücksichtigen. Dies betrifft gesetzliche, regulatorische und unternehmensinterne

Richtlinien. In Europa ist für die Speicherung und Verarbeitung personenbezogener Daten die Datenschutzgrundverordnung (DSGVO) wichtige Grundlage. Die Unternehmensführung hat hier die Aufgabe, zu prüfen, ob die vom Cloud-Anbieter bereitgestellten Leistungen den Compliance-Anforderungen der Firma genügen. Leitfäden und Frameworks können Ihnen hier helfen, Minimalanforderungen zu identifizieren. Automatisierte Tools dienen als Stütze, sicher zu stellen, dass die Sicherheitsanforderungen überwacht werden.

8. **BEDROHUNG DURCH INNEN:** Ihre in der Cloud befindlichen Daten können nicht nur von außen, sondern auch von innen bedroht werden. Sicherheitslücke: Mitarbeitende. Teammitglieder begehen durch Unwissen oder Fahrlässigkeit Fehler bei der Nutzung. Dies kann zu Sicherheitslecks oder Datenverlust führen.

9. **HYBRID WORK:** Corona hat die Art der Zusammenarbeit verändert. Remote Work bietet Chancen, kann aber zulasten der Cloud Security gehen. Dies liegt nicht nur an der Vielzahl der verwendeten Endgeräte, sondern auch an der gestiegenen Herausforderung beim Access-Management.

BEST PRACTICES FÜR MEHR SICHERHEIT IN DER CLOUD

Wie kann man als Unternehmen mehr Sicherheit in der Cloud erreichen? Einer der wichtigsten Punkte ist der Aufbau einer gut durchdachten Cloud-Strategie. Im Idealfall sollte ein/e Verantwortliche/r für die Cloud-Strategie im Unternehmen benannt werden. Diese/r legt Richtlinien fest, wie die Cloud sicher genutzt wird.

Diese Best Practices zur Erhöhung der Cloud-Sicherheit können Ihnen ebenfalls helfen:

1. **ÜBERPRÜFEN SIE IHREN CLOUD-PROVIDER:** Einige Aspekte der Cloud Security liegen in den Händen des Cloud-Providers. Prüfen Sie, ob dieser folgende Sicherheitskriterien einhält:

   - Führt der Cloud-Provider regelmäßige externe Audits durch?
   - Welche Maßnahmen unternimmt der Cloud-Provider, um zu verhindern, dass andere Kunden nicht auf Ihre Daten zugreifen können?
   - Welche Verschlüsselungsmethoden werden verwendet?
   - Wie streng vergibt der Provider Zugriffsrechte für verschiedene User?
   - Gibt es konkrete Richtlinien für die Speicherung von Kundendaten? Werden die datenschutzrechtlichen Vorgaben exakt eingehalten?
   - Ist mein Cloud-Provider zertifiziert? Als Orientierungsgrundlage kann hier der Cloud Computing Compliance Controls Catalogue (kurz C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI) dienen.

2. **VERMEIDEN SIE KONFIGURATIONSFEHLER:** Mit den aufgeführten Tipps können Sie Ihre Einstellungen optimieren und Ihre Cloud-Sicherheit signifikant erhöhen.

   - Benutzen Sie niemals Standardpasswörter oder leicht zu erratene Nutzer wie “admin”.
   - Achten sie konsequent darauf, welche Daten und Systemendpunkte öffentlich erreichbar sein sollen und sichern sie sämtliche andere ab.
   - Nutzen Sie den Sicherheits-Check Ihres Cloud-Providers: Viele Provider bieten Programme zum umfangreichen Sicherheitscheck Ihrer Plattform an. Aber auch Drittanbieter können Sie mit den passenden Tools in dieser Hinsicht unterstützten.

3. **MINIMIEREN SIE DEN KREIS DER ZUGRIFFSBERECHTIGTEN:** Je kleiner der Kreis der Zugriffsberechtigten, desto besser. Deshalb gilt das Least-Privilege-Prinzip: Seien Sie mit Berechtigungen zurückhaltend. Vergeben Sie gerade nur so viel, wie wirklich nötig.

4. **SETZEN SIE AUF STARKE PASSWÖRTER:** Empfehlen Sie allen Mitarbeitenden, schwer zu knackende Passwörter zu nutzen. Hilfreich kann hier ein Passwortmanager sein, der entsprechende Sequenzen generiert und speichert.

5. **VERWENDEN SIE EINE MEHRFAKTOR-AUTHENTIFIZIERUNG (MFA):** Eine Zwei-Faktor-Authentifizierung bietet mehr Sicherheit gegenüber der klassischen Variante. Hier können Sie Möglichkeiten wie die Codezusendung an ein Mobilgerät oder biometrische Anmeldeverfahren nutzen.

6. **NUTZEN SIE VERSCHLÜSSELUNGSTECHNOLOGIE:** Verschlüsseln sie Ihre Daten. Sowohl die Speicherung der Daten in der Cloud als auch die Transportstrecke dorthin muss verschlüsselt sein.

7. **SICHERN SIE SICH DURCH BACKUPS AB:** Wenn Sie regelmäßig Backups durchführen, stellen Sie sicher, dass Unternehmensdaten wiederhergestellt werden können.

8. **MIT VORSICHT SKALIEREN:** Behalten Sie die Kosten im Blick. Damit es nicht zu unerwarteten Kosten kommt, führen Sie eine regelmäßige Kostenkontrolle durch. Automatisch eingestellte Schwellenwerte senden Kostenwarnungen frühzeitig an zentrale Stellen.

9. **NUTZEN SIE DIE VORTEILE DER HYBRID CLOUD:** Dieses Modell bietet die Möglichkeit, sensible Daten in der Private Cloud zu speichern. Unkritische Daten werden in der Public Cloud abgelegt. Mit diesem Mischmodell kann den Sicherheitsanforderungen genüge getan werden.

10. **VERWENDEN SIE EIN VIRTUELLES PRIVATES NETZWERK (VPN):** Richten Sie sich ein virtuelles privates Netzwerk ein, um auf die Cloud zuzugreifen. So können Sie einen sicheren Datentransfer zwischen den Usern und der Public Cloud gewährleisten.

11. **SICHERN SIE DIE ARBEIT IM HOMEOFFICE AB:** Gerade durch die verstärkte Arbeit im Home-Office greifen viele Endgeräte auf Ihre Daten zu. Diese werden oft auch privat genutzt – ein erhöhtes Sicherheitsrisiko. Definieren Sie deshalb intern ein Verfahren, wie diese Endgeräte besser abgesichert werden können. Sensibilisieren Sie zudem Ihre Mitarbeitenden durch regelmäßige Schulungen für mögliche Gefahren. Es ist sinnvoll, dedizierte Endgeräte bereit zu stellen, die sich nur über VPN mit dem Firmennetz verbinden.

12. **SETZEN SIE SICHERHEITS-SOFTWARE EIN:** Installieren sie auf den Rechnern Ihrer Mitarbeitenden Antiviren- und Anti-Malware-Software.

13. **VERMEIDEN SIE DIE ENTSTEHUNG EINER SCHATTEN-IT:** Mit Leichtigkeit können neue IT-Services über die Cloud bezogen werden. Das erhöht die Entstehungsgefahr von Parallelstrukturen, einer sogenannten Schatten-IT. Verdeutlichen Sie deshalb Ihrem Team die bestehende IT-Infrastruktur und stellen Sie klar, dass sich neue IT-Dienste in das existierende System eingliedern lassen müssen.

14. **ACHTEN SIE AUF DIE EINHALTUNG DATENSCHUTZRECHTLICHER VORGABEN:** Stellen Sie sicher, dass Ihr Unternehmen den Schutz von personenbezogenen Daten nach den Richtlinien der Datenschutzgrundverordnung gewährleistet. Wichtige Maßnahmen wie die Datenmaskierung und die Klassifizierung sensibler Daten liegen in Ihrer Verantwortung.

GESETZLICHE ANFORDERUNGEN AN DIE CLOUD-SICHERHEIT

Um die Sicherheit der eigenen Anwendungen in der Cloud zu gewährleisten, sollte die Datensicherheit bei der Planung des Cloud-Einsatzes mitgedacht werden. Um gerade den Schutz personenbezogener Daten abzusichern, steht das Unternehmen selbst in der Verantwortung. Aber auch der Cloud-Provider hat die Aufgabe, für eine geschützte Cloud-Umgebung zu sorgen.

Zuständigkeiten zwischen Ihnen als Kunde und zwischen dem Cloud-Provider sind klar zu definieren. Diese Details der Datenverarbeitung werden in einem Data Processing Agreement – kurz DPA – festgelegt. Es ist rechtlich bindend und beinhaltet Vorgaben wie beispielsweise die deutsche Datenschutz-Grundverordnung (DSGVO).