Aus- & Weiterbildung, CAS Cybersecurity

Sicherheit in der Cloud

25. November 2021

Welche Sicherheitsmöglichkeiten gibt es in Cloud-Diensten?

Immer mehr Unternehmen beziehen Cloud-Services und vertrauen ihre Anwendungen und Daten externen Dienstleistern an. Neben Vorteilen wie Flexibilität, Mobilität sowie einfache und schnelle Verfügbarkeit und Skalierbarkeit, sind vor der Nutzung von Cloud-Services die damit einhergehenden Risiken zu beurteilen und zu minimieren

Cloud-Sicherheit ist die Gesamtheit der Strategien und Verfahren zum Schutz von Daten und Anwendungen, die in der Cloud gehostet werden. Neben Überlegungen zur Datenhoheit (Berücksichtigung relevanter Datenschutzgesetze) sind auch die technischen Sicherheitsaspekte von Cloud-Services sicherzustellen. Die Sicherheit in der Cloud umfassend sicherzustellen ist sehr komplex, einerseits da durch das Outsourcing vieles aus der Hand gegeben wird und die Services

nur als Blackbox gesehen werden, anderseits neue Schnittstellen zwischen Systemen und Netzwerken geschaffen werden. Mit einer gut durchdachten Cloud-Sicherheitsstrategie lassen sich die Risiken bei der Nutzung von Cloud-Services erheblich verringern.

Folgende Risiken treffen insbesondere auf die Nutzung von Cloud-Services zu:

- Lock-in Effekte (Abhängigkeit von einzelnen Providern)
- Ungenügende Verträge
- Compliance Risiken
- Insolvenz des Providers
- Verlust von Daten
- Unbefugter Zugriff auf Daten
- Angriffe auf den gesamten Cloud Provider oder auf einzelne Services
- Nichtverfügbarkeit der Services

Um die Risiken bei der Wahl eines Providers zu beurteilen und in Einklang mit den eigenen Sicherheitsanforderungen zu bringen, ist es sinnvoll, die Risiken identifizieren und zu bewerten. Neben einer grundlegenden Analyse der wirtschaftlichen Situation, Abhängigkeiten und Besitzverhältnisse des Providers sind die zentralen Prozesse, Business-Continuity-Vorkehrungen und technischen Schutzmassnahmen zu beurteilen.

1. **Prozesse**

Bei der Wahl eines Providers muss geprüft werden, ob die wichtigsten Prozesse wie Change, Incident- und Problem-Management dokumentiert, umgesetzt und getestet sind. Weiter sollte ein regelmässiges Reporting über vereinbarte Kennzahlen erfolgen. Dieses Reporting soll Key Indicators aus den Bereichen Verfügbarkeit, Performance und Kostenentwicklung enthalten.

2. **Business Continuity**

Der Provider muss aufzeigen können, wie die Business Continuity im Rahmen der vereinbarten Service-Levels sichergestellt ist. Dies umfasst ein Notfall-Management sowie entsprechende Recovery-Pläne. Diese Pläne sollten regelmässig in Übungsszenarien geprüft werden – im besten Fall im Zusammenspiel mit dem Kunden.

3. **Technik**

Für die meisten Typen von Cloud-Services sind die Themen Verschlüsselung, Identitäts- und Zugriffsmanagement und Firewalls zentrale Bestandteile zur technischen Absicherung der Dienste.

Verschlüsselung: Bei der Verschlüsselung werden Daten so verschlüsselt, dass nur autorisierte Parteien die Informationen lesen können. Wenn ein Angreifer in die Cloud eines Unternehmens eindringt und unverschlüsselte Daten findet, kann er mit diesen Daten eine Vielzahl von böswilligen Aktionen durchführen (Veröffentlichen, Verkaufen, für weitere Angriffe verwenden usw.). Wenn die Daten des Unternehmens jedoch verschlüsselt sind, findet die Angreiferin nur unbrauchbare Daten vor, die nicht verwendet werden können, es sei denn, sie kommt irgendwie an den Dechiffrierschlüssel heran. Daten sollten immer chiffriert übertragen werden, egal über welchen Weg sie transportiert werden. Die Verschlüsselung von Daten während der Übertragung sollte sowohl für Daten gelten, die zwischen einer Cloud und einem Nutzer übertragen werden, als auch für Daten, die von einer Cloud zu einer anderen übertragen werden. Des Weiteren sollten Daten

verschlüsselt werden, wenn sie in einer Datenbank oder über einen Cloud-Speicherdienst gespeichert werden.

Identitäts- und Zugriffsmanagement (IAM): Regelt, dass nur bekannte und vertrauenswürdige Benutzer auf die entsprechenden Anwendungen und Daten ihres Unternehmens zugreifen können. IAM regelt wer eine Benutzerin ist, was sie tun darf, und verweigert unbefugten Benutzern den Zugriff. IAM kann mehrere verschiedene Dienste umfassen oder es kann ein einziger Dienst sein, der alle der folgenden Funktionen vereint:

- Identitätsanbieter (IdP) ist ein Dienst, der die Benutzeridentität authentifiziert.
- SSO-Dienste (Single Sign-On) helfen bei der Authentifizierung von Benutzeridentitäten für mehrere Anwendungen, so dass sich die Benutzer nur einmal anmelden müssen, um auf alle ihre Cloud-Dienste zuzugreifen.
- Multi-Faktor-Authentifizierungsdienste (MFA) stärken den Prozess der Benutzerauthentifizierung
- Zugriffskontrolle erlauben und beschränken den Benutzerzugriff

Firewall: Eine Cloud-Firewall bietet eine Schutzschicht um die Cloud-Ressourcen, indem sie bösartigen Webverkehr blockiert. Im Gegensatz zu herkömmlichen Firewalls, die vor Ort gehostet werden und den Netzwerkrand schützen, werden Cloud-Firewalls in der Cloud gehostet und bilden eine virtuelle Sicherheitsbarriere um die Cloud-Infrastruktur. Die meisten Web Application Firewalls fallen in diese Kategorie.

Cloud-Firewalls blockieren bösartige Bot-Aktivitäten, die Ausnutzung von Sicherheitslücken, filtern und sperren ungewollten Netzverkehr. Dadurch wird die Wahrscheinlichkeit verringert, dass ein Cyberangriff die Cloud-Infrastruktur eines Unternehmens lahmlegt.

Fazit

Sind diese Punkte geklärt und die Risiken adressiert können Cloud Services ohne schlaflose Nächte genutzt werden.

Literaturquellen

Wisler, A. (2018) Cyber-Sicherheit im 21. Jahrhundert. Sicherheitskonzepte und praktische Umsetzung für KMU. BPX Edition, Rheinfelden

Links (Beispiel)

Cloudflare, Inc. (2021), https://www.cloudflare.com/de-de/learning/

IDG Business Media GmbH, München,
Computerwoche, https://www.computerwoche.de/a/ratgeber-it-sicherheit,2363872

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html

Autorenteam:
Daniele Zugno
Roger Casagrande, LinkedIn-Profil