CLOUD CAPE

HISCOX BUSINESS ACADEMY

RISIKEN UND CHANCEN ÖFFENTLICHER CLOUD-ANGEBOTE

WHITEPAPER ZUR SOUVERÄNEN ANWENDUNG

Sowohl im privaten als auch im geschäftlichen Bereich gewinnt das Cloud Computing aus gutem Grund immer mehr Anhänger: Anstatt in teure eigene Hard- und Software zu investieren, kann man IT-Dienste wie z.B. Speicherplatz, Rechenleistung oder ganze Softwareanwendungen günstig und flexibel über das Internet beziehen und umständliche Verwaltungs- und Wartungsaufgaben einfach dem Cloud-Provider überlassen.

Bei der Nutzung öffentlicher Cloud-Angebote darf jedoch nie außer Acht gelassen werden, dass die Verantwortung für die Sicherheit Ihrer Daten nie komplett an den Cloud-Provider abgeben wird und Sie selbst mitverantwortlich sind. Egal für welches öffentliche Cloud-Angebot Sie sich entscheiden und welchen Cloud-Provider Sie wählen, die Sicherheit der Daten bleibt immer in Ihrem Verantwortungsbereich!

Da immer mehr Unternehmen sensible Unternehmensdaten in die Cloud verlagern und wichtige Geschäftsprozesse von der Cloud abhängig machen, geben wir Ihnen in diesem Whitepaper die wichtigsten Informationen zur sicheren Nutzung von öffentlichen Cloud-Angeboten an die Hand.

DIE SERVICEMODELLE IN DER ÖFFENTLICHEN CLOUD

Das Konzept der öffentlichen Cloud (engl. „Public Cloud“) ist sehr weit gefasst. Öffentliche Cloud-Angebote zeichnen sind durch zwei Merkmale aus:

1. Sie sind für jedermann über eine Internetverbindung zugänglich.
2. Die physischen IT-Ressourcen im Rechenzentrum des Cloud-Providers werden zwischen den Kunden geteilt. Hierfür kommt Virtualisierungstechnologie zum Einsatz, welche für eine möglichst effiziente Auslastung sorgt.

Grundlegend unterscheidet man in der Cloud zwischen drei verschiedenen Servicemodellen:

1. Software-as-a-Service (SaaS)

SaaS bedeutet, dass ein Cloud-Provider die komplette Bereitstellung und Instandhaltung einer Softwareanwendung übernimmt. Die Einstiegshürde ist für den Nutzer dabei besonders gering. In nur wenigen Minuten kann man online ein Abonnement beim SaaS-Provider abschließen und die Software sofort nutzen, häufig direkt im Webbrowser. Daher haben mittlerweile viele Unternehmen SaaS-Dienste im Einsatz.
Beispiele für beliebte SaaS-Angebote sind Microsoft 365, Dropbox, Zoom, DocuSign, Salesforce, uvm.

2. Infrastructure-as-a-Service (IaaS)

IaaS bedeutet, dass ein Cloud-Provider einem Unternehmen virtuelle Rechenzentruminfrastruktur zur Verfügung stellt. Die Bestandteile der virtuellen Infrastruktur können z.B. Server, Netzwerkkomponenten und Speicherkapazität sein. Im Vergleich zu SaaS ist das Leistungsniveau des Cloud-Providers deutlich niedriger. Das nutzende Unternehmen muss sich um die einzelnen Infrastrukturbestandteile weitgehend selbst kümmern und sich eine eigene Lösung bauen. Ein Nutzer könnte z.B. einen virtuellen Server einrichten, konfigurieren und dann die gewünschte Software installieren.

Die bekanntesten IaaS-Provider in Deutschland sind Microsoft mit dem Cloud Computing Dienst „Azure“, Amazon mit „Amazon Web Services“ und Google mit der „Google Cloud Platform“. Neben den dominierenden US-Konzernen mit ihren global vernetzten Rechenzentren gibt es auch allerhand kleinere deutsche Provider auf dem IaaS-Markt. Dazu zählen beispielsweise STRATO und 1&1 IONOS.

3. Platform-as-a-Service (PaaS)

PaaS bedeutet, dass ein Cloud-Provider seinen Kunden eine Entwicklungsumgebung bereitstellt. Virtuelle Rechenzentrumsinfrastruktur wird vom Provider soweit verwaltet, dass sich die Cloudnutzer auf die Erstellung von eigenen Anwendungen fokussieren können. PaaS steht somit zwischen IaaS und SaaS.

Beispiele für bekannte PaaS Angebote sind z.B. die SAP Cloud Platform oder Red Hat OpenShift PaaS.

Bei allen drei Servicemodellen SaaS, IaaS und PaaS teilen sich Provider und Kunde die Verantwortung für die Datensicherheit. Es ist daher wichtig zu wissen, welche Sicherheitsrisiken in der Cloud bestehen und welche Möglichkeiten es gibt, diese zu reduzieren.

CLOUD CAPE

HISCOX BUSINESS ACADEMY

ALLGEMEINE RISIKEN BEI DER NUTZUNG ÖFFENTLICHER CLOUD-ANGEBOTE

Unternehmen sind immer mehr von der IT abhängig. Wird die IT in gravierender Weise beeinträchtigt, kann das im Extremfall sogar die Existenz eines Unternehmens gefährden. Bei der Nutzung von Cloud-Angeboten ist man grundsätzlich denselben Risiken ausgesetzt, wie bei der Nutzung traditioneller IT-Lösungen auch - allerdings haben diese Risiken aufgrund der öffentlichen Erreichbarkeit von Cloud-Diensten und der Abhängigkeit vom Cloud-Provider eine besondere Bedeutung.

Die wichtigsten Risiken und Bedrohungen in der Cloud sind:

1. **Identitätsdiebstahl:**
   Anmeldedaten für einen Cloud-Dienst werden gestohlen und für fremde Zwecke missbraucht.

2. **Verlust der Integrität von Daten und Systemen:**
   Durch Schadprogramme (Malware) oder gezielte Angriffe auf die eigene Cloud-Umgebung kann die Daten-- bzw. Systemintegrität verletzt werden.

3. **Verletzung gesetzlicher Datenschutzvorgaben:**
   Nicht autorisierten Personen gelingt Zugriff auf personenbezogene Daten.

4. **Abfluss sensibler Daten:**
   Sensible Informationen wie z.B. Geistiges Eigentum oder Kundendaten gelangen an unerwünschte Empfänger.

5. **Ausfälle wichtiger Dienste oder endgültiger Datenverlust:**
   Durch technische, menschliche oder externe Einflüsse geht der Zugang zu Daten vorübergehend oder permanent verloren, z.B. durch fehlgeschlagene Software-Updates des Cloud-Providers.

HÄUFIG AUFTRETENDE SICHERHEITSPROBLEME UND BEST-PRACTICES

Um zu verhindern, dass die oben genannten Risiken eintreten, möchten wir Sie auf häufig vorzufindende Sicherheitsprobleme in der Cloud aufmerksam machen und konkrete Hinweise zur Lösung geben:

1. SCHWACHSTELLEN IN DER CLOUD-ARCHITEKTUR

Kurzbeschreibung:
Sicherheit in der Cloud beginnt mit einem gut durchdachten Plan. Viele Unternehmen wollen den Weg in die Cloud möglichst schnell beschreiten und vernachlässigen die gründliche Planung ihrer Cloud-Migration. Bei der überstürzten Einführung von öffentlichen Cloud-Diensten ist die Cloud-Architektur häufig nicht robust gegen interne und externe Bedrohungen.

Beispiele:
- Bestehende IT-Sicherheitskontrollen werden einfach beibehalten und nicht an die Cloud-Welt angepasst
- Es herrscht ein Mangel an erfahrenem Personal für die Planung, Implementierung und den Betrieb von cloudbasierten IT-Landschaften

Schlussfolgerungen:
Nicht nur die Funktionalität einer Cloud-Lösung ist wichtig, sondern auch die Sicherheit. Vor einer Adaption eines Cloud-Angebotes sollte ein guter Plan entwickelt werden und ein Framework für die Sicherheit in der Cloud verfasst werden. Es kann ein sinnvoller Schritt sein, sich hierfür externe Unterstützung an Bord zu holen.

2. FEHLKONFIGURATIONEN VON CLOUD-DIENSTEN

Kurzbeschreibung:
Cloud-Dienste werden häufig unsicher eingerichtet, so dass sie sehr anfällig für böswillige Aktivitäten von Dritten sind.

Beispiele für Fehlkonfigurationen:
- Standardpasswörter werden nicht geändert
- Wichtige Sicherheitsfunktionen des Cloud-Dienstes bleiben deaktiviert
- Benutzerrechte werden zu weitreichend vergeben

Schlussfolgerungen:
Fehlkonfigurationen in der Cloud können schwerwiegende Folgen haben. Da sich Cloud-Umgebungen sehr flexibel ändern lassen, ist die Gefahr von Fehlkonfigurationen ein ständiger Begleiter. Es ist ratsam, sichere Grundeinstellungen zu definieren und permanent auf Verstöße zu prüfen, am besten automatisiert, sodass IT-Verantwortliche unverzüglich alarmiert werden.

HÄUFIG AUFTRETENDE SICHERHEITSPROBLEME UND BEST-PRACTICES

3. UNZUREICHENDER ZUGRIFFSSCHUTZ

Kurzbeschreibung:
Wenn der Zugriff auf Ihre Cloud-Dienste und Ressourcen nicht durch angemessene Maßnahmen und Richtlinien gesteuert und überwacht wird, können unautorisierte Benutzer Zugang zu Ihren Daten erlangen. Wirksame Nutzerzugangskontrollen sind bei Cloud-Diensten von großer Bedeutung und in der Praxis oftmals eine Herausforderung.

Beispiele für unzureichend geschützte Cloud-Dienste:
- Der Einsatz von starken Passwörtern wird nicht erzwungen
- Kein Einsatz von Multi-Faktor-Authentifizierung (MFA) beim Anmeldevorgang
- Keine Überwachung von auffälligen Zugriffsmustern (z.B. aus unüblichen Ländern)

Schlussfolgerungen:
Den Zugriff auf die eigenen Cloud-Dienste sicher zu gestalten sollte auf der Prioritätenliste sehr weit oben stehen. Hier kann mit wenigen Maßnahmen die Sicherheit bereits deutlich erhöht werden. Zu den absoluten Grundlagen gehören Richtlinien für sichere Passwörter und Multi-Faktor-Authentifizierung, insbesondere für Nutzer mit weitreichenden Befugnissen. Außerdem sollten die Zugriffe auf Ihre Cloud-Dienste überwacht werden und bei auffälligen Vorgängen sollte Alarm ausgelöst werden.

4. UNSICHERE ANWENDUNGSSCHNITTSTELLEN (SOG. APIS)

Kurzbeschreibung:
APIs dienen dazu, Daten zwischen Anwendungen in Echtzeit auszutauschen. In einer IT-Welt, die immer mehr zusammenwächst und freien Informationsfluss benötigt, sind APIs von enormer Bedeutung. Cloud-Provider stellen APIs zur Verfügung, um ihren Kunden die Interaktion mit der Cloud zu ermöglichen. Unsichere APIs stehen immer mehr im Fokus von Hacking-Angriffen und werden schnell zur Achillesferse eines Cloud-Dientes.

Beispiele für API-Sicherheitsprobleme:
- Die API-Sicherheit des Providers wird nicht ausreichend geprüft
- Es werden keine zusätzlichen Sicherheitsmaßnahmen, wie z.B. eine API-Management-Lösung, implementiert

Schlussfolgerungen:
Beide Seiten -sowohl Cloud Provider als auch Nutzer von APIs - sind gefordert ihren Teil zur API-Sicherheit beizutragen. Wenn Sie eine API verwenden möchten, um sensible Daten zu übertragen, sollten Sie vorab eine Gefährdungseinstufung vornehmen. Gegebenenfalls ist es anschließend ratsam, zusätzliche Sicherheitsmaßnahmen zu ergreifen.

HÄUFIG AUFTRETENDE SICHERHEITSPROBLEME UND BEST-PRACTICES

5. FEHLENDE VERSCHLÜSSELUNG VON DATEN IN DER CLOUD

Kurzbeschreibung:
Die Nutzung öffentlicher Cloud-Angebote bedeutet, dass Ihre Daten auf den Rechnern eines anderen Unternehmens gespeichert werden. Es sollte nicht nur der Zugriff auf diese Daten, sondern auch die sensiblen Daten an sich geschützt werden. Verschlüsselung spielt dabei eine wesentliche Rolle. Dieses Bewusstsein fehlt leider vielen Cloud-Nutzern. Gelingt der unautorisierte Zugriff auf unverschlüsselte Daten in der Cloud, sind diese lesbar und können abhandenkommen.

Beispiele für die fehlende Verschlüsslung sensibler Daten:
- Unternehmensdaten werden nicht nach Sensibilität klassifiziert und es gibt keine Richtlinie über die Verschlüsselung in der Cloud
- Unternehmensgeheimnisse, wie etwa Preislisten, Kundenlisten, Rezepturen, etc., werden unverschlüsselt in der Cloud abgelegt

Schlussfolgerungen:
Sensible Daten sollten in jedem Zustand verschlüsselt werden – d.h. sowohl im Ruhezustand also auch während des Transports von und zur Cloud. Im ersten Schritt ist es notwendig sensible Daten zu identifizieren und zu klassifizieren. Daten, die in höhere Vertraulichkeitsstufen fallen, sollten entsprechend einer Richtlinie verschlüsselt werden. Hierzu sind technische Vorkehrungen notwendig. Es muss geprüft werden, ob die Verschlüsselungsoptionen des Cloud-Providers mit dem Grad der Sensibilität der eigenen Daten in Einklang stehen. Ist dies nicht der Fall sollte ein Wechsel oder eine Drittanbieterlösung in Betracht gezogen werden, die im Optimalfall AES-256 Verschlüsselung bietet.

6. UNSICHERE ENDNUTZERGERÄTE

Kurzbeschreibung:
Die Arbeitswelt wird immer mobiler und entsprechende Endgeräte (Laptops, Tablets, Smartphones) greifen auf die Cloud-Dienste eines Unternehmens zu. Häufig fehlt IT-Verantwortlichen der Überblick und die Kontrolle über die Endgeräte, deren Programme und vor allem deren Sicherheitslücken. Die Endgeräte können somit zum Einfallstor für Schadsoftware in die Cloud werden.

Beispiele für ein mangelhaftes Management von Endgeräten:
- Es gibt keine Sicherheitsrichtlinie, die eine genehmigte Liste von Geräten und Programmen festlegt
- Der Zugriff auf die Endgeräte selbst ist nicht ausreichend gesichert

Schlussfolgerungen:
Unternehmen sollten die zentrale Verwaltung und den Schutz mobiler Endgeräte gut organisieren. Zur Bewältigung dieser Aufgabe ist eine Mobile-Device-Management-Lösung ratsam. Hiermit lassen sich über alle mobilen Geräte einheitliche Standards mittels Sicherheitsrichtlinien durchsetzen sowie die Nutzung und das Eigentum von mobilen Geräten verfolgen.

CLOUD CAPE

HISCOX BUSINESS ACADEMY

ZUSAMMENFASSUNG

Cloud-Dienste bieten Unternehmen jeder Größenordnung viele Chancen und sind definitiv für die Zukunft nicht mehr wegzudenken. Sie sollte sich auf diesen Paradigmenwechsel einlassen, jedoch zugleich die Risiken und Sicherheitsprobleme öffentlicher Cloud Angebote kennen. Bevor sie praktische und moderne Cloud-Lösungen einführen, sollten Sie sich ausgiebig mit Ihren individuellen Sicherheitsanforderungen und dem Thema Cloud-Sicherheit beschäftigen. Und auch dann ist der Prozess nicht abgeschlossen. Die Beschäftigung mit IT-Sicherheit bleibt eine fortlaufende Herausausforderung mit regelmäßiger Überprüfung.

Falls Sie bereits Nutzer von öffentlichen Cloud-Diensten sind, können Sie als Hiscox-Kunde übrigens ein Cloud-Sicherheitsaudit zum Vorteilspreis in Anspruch nehmen und Ihre wichtigsten Cloud-Dienste von Sicherheitsexperten auf den Prüfstand stellen lassen.

MISSION STATEMENT

Cloud Cape hilft sicherheitsbewussten Unternehmen dabei sich vor Cyberangriffen zu schützen und Transparenz über Vorgänge im eigenen Netzwerk zu schaffen. Als zukunftsorientiertes ‚Cloud-First'-Unternehmen begleiten wir mittlere Unternehmen auf dem Weg der sicheren digitalen Transformation. Wir arbeiten mit Kunden die wissen, dass IT-Sicherheit längst nicht mehr nur zur Risikobegrenzung dient, sondern als wahrer Business Enabler zu verstehen ist, der es erlaubt agiler zu sein, das Kundenvertrauen und die Kundenloyalität zu erhöhen und Teams den Freiraum zu geben, sich an neue Ideen zu wagen.

ZU CLOUDCAPE

Die Cloud Cape IT Security GmbH ist Ihr Partner Rund um die Themen Public Cloud und proaktive IT-Sicherheit aus Heilbronn. Cloudcape bietet eine ganzheitliche Unterstützung bei Ihren Public-Cloud-Projekten - von der Beratung und Planung über die Umsetzung bis hin zum laufenden Betrieb und Support. Zu den Leistungen zählen außerdem umfangreiche Sicherheitstests aus der Cloud durch zertifizierte Experten.

Ihr Ansprechpartner
Dennis Kionga
IT Security Consultant
dennis@cloudcape.de
+ 49 171 618 718 0

Cloud Cape IT Security GmbH
Bildungscampus 3
74076 Heilbronn
www.cloudcape.de

Hiscox
Arnulfstraße 31, D - 80636 München
www.hiscox.de