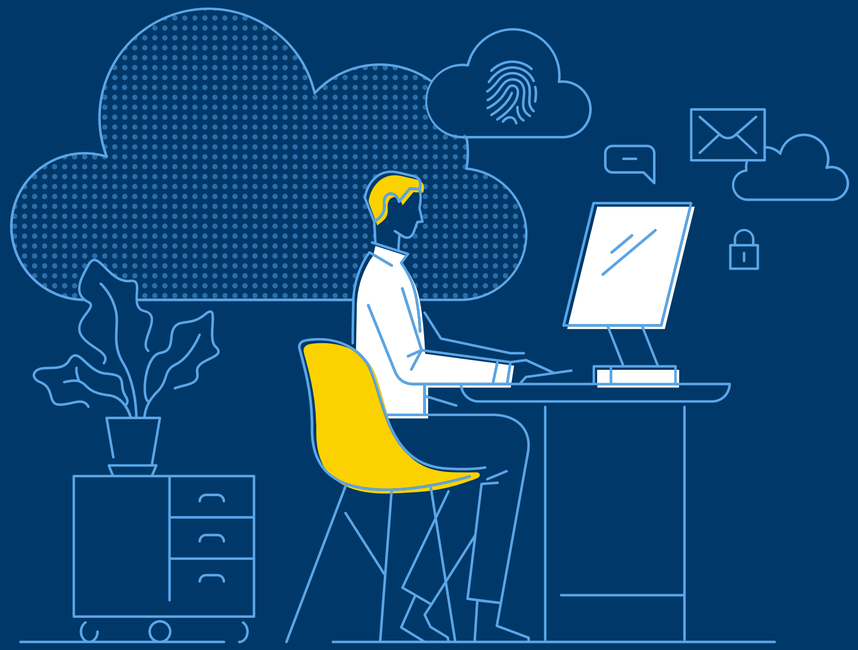
Cloud sicher betreiben

Sicherheit garantieren durch geschulte Partner

BTC



Vorwort

Ingo Vorreiter
Business Development
Berater

M +49 173 6976 607
ingo.vorreiter@
btc-ag.com

Liebe Leser*innen,

egal welche Branche, welche Produkte, welche Themen – die Masse an zu organisierenden Daten wird in jedem Unternehmen größer. Mit wachsenden Datenmengen stellt sich aber nicht nur die Frage nach Speicherort und Verarbeitung, auch die Datensicherheit bekommt einen immer höheren Stellenwert. Unternehmen haben längst erkannt, dass dieses Thema ihre sofortige Aufmerksamkeit braucht, und können nun zwischen zwei Möglichkeiten entscheiden: die Speicherung der Daten im hauseigenen Rechenzentrum oder die Nutzung der durch Unternehmen wie Microsoft und Amazon zur Verfügung gestellten Cloudlösungen.

Bedeutet ein eigenes Rechenzentrum nun, dass hier Datenschutz und Datensicherheit perfekt geregelt sind und man sich der Frage nach Sicherheit gar nicht mehr stellen muss? Mitnichten! Oft herrscht die Meinung vor, Daten seien an den Speicherorten der Hyperscaler unsicherer und im eigenen Rechenzentrum geschützter. Natürlich ist eine gesunde Skepsis bei der Nutzung von Cloud-Services angebracht, aber es ist schon auffällig, wieviele klassische RZ-Kunden in den letzten 12 Monaten Opfer von Ransomware- und DDOS-Attacken geworden sind und wie selten wir dies insbesondere bei Azure- und AWS-Kunden beobachten.

Das Bemerkenswerte ist: Es scheint hier ein starkes Ungleichgewicht zwischen gefühlter und realer Bedrohung zu geben.

Lesen Sie 5 Punkte, wie man eine Cloudlösung sicherer macht als das hauseigene Rechenzentrum! Es ist Zeit, das Verständnis für einen reibungslosen Cloudbetrieb von Grund auf zu erneuern und Sie mit Ideen zu versorgen, **wie Sie Ihre IT-Strategie einfach und risikoarm in einen Cloud Service einbauen, der sicherer ist als jede OnPremise-Variante**.

Inhalt

Die 5 wichtigsten Punkte für einen Wechsel und eine sichere Inbetriebnahme Ihrer neuen Cloud-Lösung – und wie qualifizierte Partner wie BTC Sie dabei unterstützen können.

Definition von Schutzbedarfsklassen und ToMs

Definieren von Schutzbedarfsklassen

Daraus können direkt technisch-organisatorische Maßnahmen abgeleitet werden

Die Definition von Schutzbedarfsklassen hilft Ihnen, konkrete Anforderungen zu formulieren, beispielsweise:

- Die Verschlüsselungsanforderungen ruhender und transportierter Daten
- Identitäten
- Der Zugang zu öffentlichen IPs
- Administratorenkonzepte
- Datensicherung
- Archivierung u.v.m.

Sicher gehört diese Aufgabe auch jetzt bereits zu den Standards in Ihrem Rechenzentrum. Im Unterschied zu diesem werden Sie in der Cloud aber in der Lage sein, die Ergebnisse Ihrer Anforderungen direkt in Regeln zu gießen. Die Definition von zwei bis drei Schutzbedarfsklassen ist hierbei völlig ausreichend, die Liste an Maßnahmen kann allerdings bis zu 100 Punkte umfassen.

BTC

Best Practices der Cloud Provider nutzen

Best Pratices der Cloud Provider nutzen

Verschmelzen Sie Ihren Schutzbedarf direkt mit den Fähigkeiten der Expert*innen

Die Grundlage für Ihren gesamten Workload ist der Bau einer Landing Zone – einem sicheren Zuhause für Ihre Aktivitäten, wenn Sie so wollen. Alle Hyperscaler, egal ob AWS, Microsoft Azure oder GCP, bieten mindestens in der Zielsetzung ähnliche Konzepte für den Bau an. In der Landing Zone werden die grundlegendsten Regeln festgelegt, zum Beispiel welche Regionen und Länder verwendet werden dürfen oder wie der Aufbau der Netzwerkarchitektur aussehen soll.

Was zunächst klingt wie ein einfacher Benefit, ist eine nicht zu unterschätzende Notwendigkeit. Wenn man bereits vor der ersten Applikation IP-Adresskreise für die Kommunikation mit Ihrem Rechenzentrum festlegt, können Sie sich im Nachhinein einen sehr aufwendigen Umbau ersparen. Diese IP-Adresskreise werden idealerweise nach rein internen Anwendungen und Anwendungen mit Kontakt zur Außenwelt (Public IPs) getrennt.

Die Services der Hyperscaler (Cloud WAN von AWS oder Virtual WAN von Azure) helfen dabei, Ihre Arbeitsumgebung später leicht managen zu können.

Verzichten Sie auf eine frühzeitige Festsetzung dieser Regeln, kann es passieren, dass Sie zu einem späteren Zeitpunkt feststellen müssen, wie Sie und Ihre KollegInnen vor einem unüberwindbar scheinenden Berg an Mehrarbeit stehen, den Sie durch den Einsatz der richtigen Lösungen sehr früh schon hätten vermeiden können.

BTC

Zero Trust statt DMZ

Zero Trust statt DMZ

Schließen Sie Ihre Sicherheitslücken

Um die Sicherheitsstrategien in Rechenzentren und ihre Schwächen zu erläutern, stellen wir uns das zentrale System als Festung vor, um die Sie einen Burggraben ziehen, damit sie vor Eindringlingen geschützt ist. Die Festung fungiert als demilitarisierte Zone, in der alle Komponenten des Systems ungehindert miteinander kommunizieren können. Klingt zunächst wie eine einleuchtende Technik, allerdings setzen erfolgreiche Ransomware-Angriffe meist genau hier an. Es gibt tausende Möglichkeiten, in die DMZ einzudringen. Der Clou: Dort setzen sich die Angreifer nicht nur im Betriebssystem fest, wo Virenscanner sie relativ leicht finden können, sondern auch in der Ebene darunter, z. B. über Switche oder Security-Software (erkennen Sie die Ironie?).

Zwischen dieser Infektion mit der Malware und dem tatsächlichen Angriff können bis zu mehreren Monaten vergehen. Das heißt, auch wenn eine Security-Lücke bei Ihnen längst geschlossen ist, kann sie trotzdem noch Schaden verursachen.

Um das zu vermeiden, sollte man in der Cloud eine Zero-Trust-Strategie implementieren. Alle Hyperscaler empfehlen diese Methode, auch wenn es in der Verantwortung jedes einzelnen Kunden liegt, deren Einhaltung sicher zu stellen.

Obwohl es absolute Sicherheit vor Angriffen auch in der Cloud nicht geben kann, stellen Zero-Trust-Konzepte sicher, dass ein Angriff von außen sich nicht einfach auf ein anderes Ihrer Systeme in der gleichen Cloud-Umgebung ausbreiten kann. Das wird durch ein konsequent über Regeln implementiertes Konzept garantiert.

Eine weitere Methode, um sicherzustellen, dass die Ransomware-Angriffe ihre Kraft und Bedeutung verlieren, ist, Ihre Systeme zusätzlich zu normalen Backups auch in ein unveränderliches Archiv zu schreiben. Der Vorteil: Es entstehen keine so hohen Kosten wie für ein WORM-Hardware-Device, welches Sie in Ihrem Rechenzentrum einsetzen würden.

Monitoring- und Advisory-Services

Monitoring- und Advisory-Services

Keine Cloudanwendung kommt ohne Überwachung

Egal von welchem Hyperscaler Sie Ihre Cloud-lösung beziehen, alle werden die Cloud an sich schützen und diese Aufgabe auch nicht ab-geben. Die Anwendungen innerhalb der Cloud zu schützen ist aber Ihre Aufgabe. Haben Sie beispielsweise versehentlich einen Objektspei-cher mit öffentlicher IP-Adresse, wird dieser mit hoher Sicherheit durch böswillige Crawler gefunden und angegriffen.

Hier greift die Advisor-Funktion, die der Cloud-Provider Ihnen zur Verfügung stellt. Über ihn werden Sie regelmäßig über poten-zielle Schwachstellen in der Anwendungs-Architektur informiert und über Maßnahmen aufgeklärt, die Sie zur Beseitigung ergreifen können. Den Empfehlungen des Advisors zu folgen, liegt hierbei aber vollständig in Ihrer Verantwortung.

Die wichtigsten Services sind die Folgenden:

Security

- Erkennen von Angriffen
- Anomalien im Zugriff
- Erkennen von Schwachstellen in der Konfiguration

Kosten

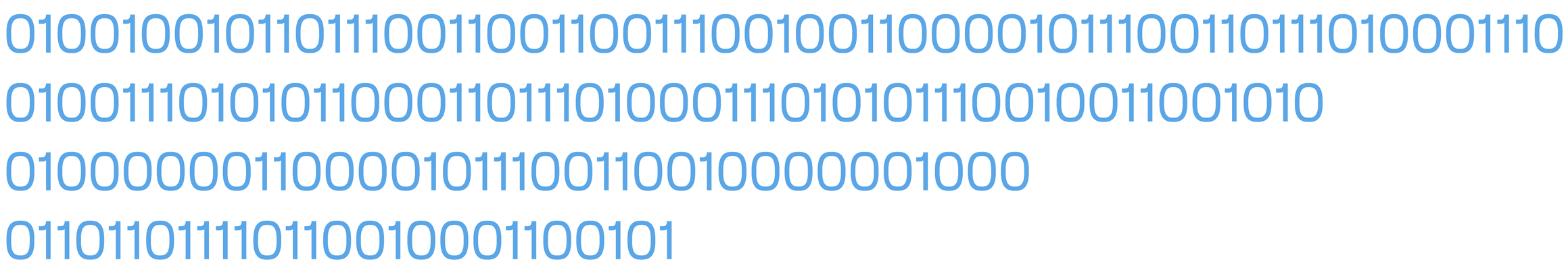
Die Cloud ist genauso grenzenlos wie die Möglichkeit, Geld dafür auszugeben.

Ein monatliches Cost Reporting reicht daher nicht aus, es wird ein **Monitoring** in Echtzeit gebraucht, um zum Beispiel:

- das Überschreiten von Budgetgrenzen zu erkennen
- das Sizing der Server um Auge zu behalten
- den Einsatz von Reserved Instances zu verwalten, um bis zu 70% der Serverkosten einzusparen
- mit Bring-your-own-Lizenzkosten (Hybrid-Lizenzen) zu sparen
- Systeme, die nicht durchgehend gebraucht werden, abzuschalten

BTC

Infrastructure as Code



Infrastructure as Code

Immer!

Egal ob es um Themen wie Automatisierung oder auch nur Dokumentation Ihrer Cloud-Infrastrukturen geht: Infrastructure as Code ist der Schlüssel.

In der Cloud könnten Sie sich nahezu zu jedem Baustein, den Sie brauchen, einfach durchklicken. Zum Testen der Funktion und zum Lernen des Aufbaus ist das durchaus sinnvoll. Für einen effektiven und sicheren Cloudbetrieb ist es jedoch ein absolutes No-Go!

Der richtige Weg ist die Beschreibung der Struktur und aller ihrer Teile als Code, wobei es hier Ermessens- und letztendlich Geschmackssache ist, ob man die Cloud-nativen Skript-Sprachen oder Cloud-übergreifende verwendet. Terraform, ARM Templates (Azure) oder Cloudformationen (AWS) – alle gängigen IaC-Systeme funktionieren und sichern einen fehlerlosen Betrieb.
In Kombination mit der passenden Continious Integration / Deploymente Pipeline (CI/CD) halten Sie Ihre Umgebung außerdem leicht zu managen, egal ob Sie auf Container, virtuellen Maschinen oder Cloud-Services ausrollen.

BTC

Cloud Security

Was umfasst Cloud Security?

Und wie steht Ihnen die BTC als vertrauenswürdiger Partner zur Seite?

Folgende Leistungen bieten wir Ihnen an:

- Aufbau des Fundaments: Landing Zones entsprechend Ihrer Governance und allgemeinen Best Practices
- Aufbau von Datenplattformen in Azure oder AWS – Data Lakes und Lakehouses
- Architektur-Reviews für AWS nach dem Well Architected Framework und für Azure gemäß der Microsofts Enterprise Scale Architecture und dem Cloud Adaption Framework (CAF)
- Aufbau von sicheren, isolierten Sandbox-Umgebungen
- Cloud Plattform-, Infrastruktur- und Applikationsbetrieb
- SaaSifizierung – Betrieb für ISV-Anbieter

Wenn wir von Cloud Security sprechen, stellen wir konkret folgende Frage: Welche Maßnahmen können wir ergreifen, um Sie vor den bei der Nutzung von Cloud Services möglichen Risiken wie Datenverlust, Serviceausfall oder dem unbefugten Zugriff Dritter zu schützen?

Die Maßnahmen bestehen aus einem Mix aus Prozessen und technischen Vorgaben, die sicherstellen, dass gesetzliche Regelungen eingehalten und alle Daten sicher gespeichert und verarbeitet werden können. Außerdem muss die Infrastruktur der Cloud und ihre Anwendungen geschützt werden.

Was wir tun

Was wir tun

Und warum

BTC ist langjähriger AWS-Partner, Microsoft Lösungs-Partner für Azure Infrastructure, Data & AI, Digital App & Innovation und natürlich Modern Work, sowie seit Kurzem mit dem Expert Status der SAP ausgezeichnet. Beim AWS Gameday Partner League konnten wir zudem den Gesamtsieg unter 52 teilnehmenden Teams aus Europa, dem Nahen Osten und Afrika, erringen. Als Ihr Spezialist für einen strategischen und sorgfältigen Umzug Ihrer Daten und Ihres Rechenzentrums in eine Cloudlösung verfügen wir sowohl über das technische Knowhow, den Transfer zu vollziehen, als auch über die Fachkompetenzen, die es braucht, um Ihre Mitarbeiter zu schulen und optimal auf die Arbeit in der Cloud vorzubereiten.

Eine Cloudlösung kann Ihre Daten auf die bestmöglichste Weise schützen – wenn sie richtig benutzt wird! Es kommt hierbei darauf an, dass man beim Einsatz einen guten Partner an seiner Seite hat, der einschätzen kann, wie aus einem Medium ein sicheres Medium gemacht werden kann. Die BTC steht hierfür gerne an Ihrer Seite.

Unsere Cloud-Expert*innen begleiten Sie auf dem Weg in eine neue Arbeitswelt. Wir begeistern uns für Digitalisierung und die Menschen, denen unsere Cloudlösung ihre Zusammenarbeit erleichtern.

Autor

Ingo Vorreiter
Business Development
Berater

M +49 173 6976 607
ingo.vorreiter@
btc-ag.com

Über BTC

Die BTC Business Technology Consulting AG ist eines der führenden IT-Consulting-Unternehmen in Deutschland (Hauptsitz Oldenburg).

Das Dienstleistungsangebot reicht von der Prozessberatung über die Systemeinführung und -integration bis zum Applikations- und Systemmanagement. Branchenschwerpunkte liegen in den Bereichen Energie, Industrie und Dienstleister, Öffentlicher Sektor und Telekommunikation.

BTC

BTC AG
Escherweg 5
26121 Oldenburg
Deutschland
www.btc-ag.com