Fact About

factcloud

Insights

Wie wir einen reibungslosen Betrieb sicherstellen

fact digital uncomplicators

Software as a Service (SaaS) ist in aller Munde.

Ein Text von: **Thomas Ulken**

Knappe Verfügbarkeit von guten IT-Mitarbeitenden, Aufbau von technischem Anwendungs-Know-How bei Mitarbeitenden, Konzentration auf das Kerngeschäft und vieles mehr sind Argumente, welche für einen SaaS-Betrieb sprechen. Genauso laut ist aber auch die Kritik am Cloud-Betrieb. Herausgabe von (sensiblen) Daten, Auslagerung von für den Unternehmensbetrieb relevanten Softwarekomponenten, ohne die Kontrolle darüber zu behalten, IT-Sicherheit sind Argumente, welche vermeintlich gegen einen Cloud-Betrieb sprechen.

Die Fact betreibt Ihre Anwendungen auch als SaaS. Dementsprechend wollen wir der kritischen Betrachtung eines SaaS entgegentreten und in diesem Whitepaper einige Einblicke gewähren, wie wir einen reibungslosen und sicheren Cloud-Betrieb gewährleisten.

Zunächst einmal sei gesagt, dass die allgemeine Einschätzung, dass nur der Selbstbetrieb auch ein guter und sicherer Betrieb ist, der Einschätzung unterliegt, dass die interne IT oder ein bestehender IT-Dienstleister die eigene Umgebung bestmöglich betreiben und absichern kann. Bei einer Vielzahl von Anwendungen in jedem Unternehmen, welche auch alle ein anwendungsspezifisches Know-how benötigen, eine individuelle Konfiguration und auch ein entsprechendes Monitoring ist allerdings genau das schwierig.

Um das an dieser Stelle auch klar zu formulieren: Ein Selbstbetrieb ist möglich und wir bieten diese Option unseren Kunden auch explizit für First Cloud und Flextax Cloud an, aber man braucht genügend Ressourcen und Know-how um das tun zu können.

Sicherer Betrieb

Zuerst die Basics. Der Betrieb der Fact Cloud und der darauf liegenden Anwendungen wird von uns im Rahmen unserer Zertifizierung ISO 27001 erbracht. Die ISO 27001 gibt grundlegende Regelungen vor, dass Prozesse definiert sind und verwendet werden. Hierbei sind insbesondere der Change-Management-Prozess sowie der Incident-Management-Prozess von großer Bedeutung. In beiden Fällen wurden die Rollen Change-Manager sowie Incident-Manager klar benannt. Die hinterliegenden Prozesse wurden dokumentiert und allen Mitarbeitenden gegenüber kommuniziert. Dadurch kann Fact ein reibungsloses Vorgehen bei Änderungen oder Vorfällen garantieren. Des Weiteren bilden Rollendefinitionen innerhalb des Unternehmens mit darauf basierenden Zuständigkeiten, Rechten und Genehmigungsprozessen die Grundlage unserer Arbeit in der Cloud-Umgebung. Wir agieren unter der Maßgabe des Need-to-know-Prinzips und beschränken dahingehend Zugriffe und Rechte auf ein Minimum.

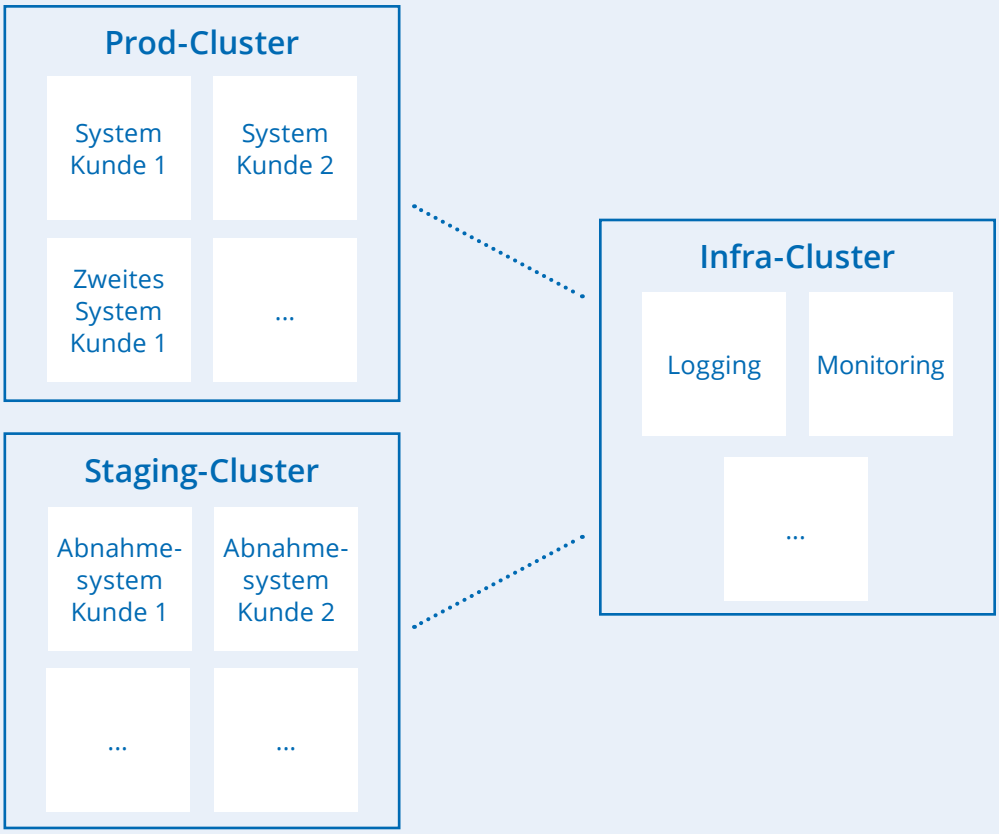
In all unseren Entscheidungen bezüglich des Aufbaus sowie den Sicherheitsmaßnahmen im Cloud-Umfeld stehen wir in engem Austausch mit dem Informationssicherheitsbeauftragten sowie dem Datenschutzbeauftragten der Fact. Wir achten darauf möglichst viele technische und organisatorische Maßnahmen umzusetzen und hierdurch Ihre Anwendung sicher und rechtskonform zu gestalten.

Wir legen bei unseren Maßnahmen auch ein besonderes Augenmerk auf die Minimierung des Sicherheitsrisikos durch den Faktor „Mensch“, durch eine präventive Vorgehensweise.

Es erfolgen daher regelmäßige Schulungen unserer Mitarbeitenden im Bereich Informationssicherheit und Datenschutz. Darüber hinaus ist ein verpflichtendes E-Learning-Programm zu diesen Themen sowie eine interne Phishing-Kampagne für die Sensibilisierung aller Mitarbeitenden der Fact seit einigen Jahren umgesetzt.

Wir haben klare Vorgehensweisen für den Umgang mit Informationssicherheitsvorfällen etabliert, welche auch die rechtzeitige Kenntnisnahme dieser umfassen. Auch werden etwaige Risiken durch unsere Risikomanagerin fortlaufend identifiziert und frühzeitig mit Maßnahmen hinterlegt. Weiterhin umfasst das Personal der Fact eine offiziell benannte und zertifizierte Compliance-Managerin, welche unter anderem sicherstellt, dass rechtliche Vorgaben frühzeitig bekannt und umgesetzt sind.

Ein weiterer technischer Baustein für einen sicheren Betrieb und die sichere Verwaltung Ihrer Daten ist die Trennung der Kundenumgebungen, sowohl untereinander als auch zu Entwicklungssystemen oder weitergehenden Infrastrukturkomponenten. Die infrastrukturellen und internen Systeme liegen in eigenen Clustern. Die Kundensysteme liegen in zwei Clustern. Dabei werden die produktiven Systeme von Staging- oder Testsystemen getrennt, auch um im Rahmen von SLAs diese besser voneinander separieren zu können. Innerhalb der Cluster läuft jede Kundenumgebung in separaten Namespaces, welche voneinander getrennt sind (ähnlich wie bei virtuellen Netzwerksegmenten). Die Namespaces interagieren nicht miteinander und die Networkpolicies werden entsprechend automatisiert überwacht. In einem Namespace läuft die Anwendung selbst, aber auch die Nutzdaten und die Datenbank werden dort gespeichert.



Zu einem effizienten SaaS-Betrieb gehört natürlich auch eine Lösung für ein zentrales Monitoring und Logging. Auf jedem System werden dafür Loggingdaten aber auch Systemmetriken (CPU-Auslastung, RAM-Auslastung, Netzwerkmetriken, Storagemetriken, Datenbankmetriken, uvm.) an das zentrale Infrastrukturcluster der Fact Cloud gesendet. Diese Daten dienen der Überwachung der Systeme, der Problemanalyse und bilden auch die Grundlage für ein Alerting im Rahmen von SLAs. Zudem werden darüber auch präventive Maßnahmen möglich, welche im nachfolgenden Kapitel beschrieben werden.

Präventive Maßnahmen

Zu einem guten und sicheren Betrieb gehören vorausschauende Maßnahmen und präventive Eingriffe. Diese umfassen selbstverständlich auch Anpassungen von CPU über RAM bis hin zu Festplattenressourcen. Da ein System im Laufe der Zeit lebt und sich Datenbestände und Datenmengen sowohl in der Speicherung wie auch in der Verarbeitung ändern, ist ein fortlaufendes Monitoring notwendig. Hier können Ressourcen angepasst oder auch Softwarefehlverhalten festgestellt werden. Für genaue Einstellungen der Anforderungen ist hier häufig eine Abstimmung notwendig, da auch imperformante Schnittstellen Systemauswirkungen haben können (z.B. da die gleiche Datenbank involviert ist) und man daher nicht einfach nur das Verhalten der Software ändern oder an der Hardwareschraube drehen kann, um Fragestellungen zu beantworten.

Systempflege

Im Rahmen von Festplattenspeicher und der Datenhistorie eines Systems ist es aber auch notwendig Systempflege zu betreiben und z.B. Historien zu verkürzen, alte Jobverzeichnisse zu löschen oder auch Berichte zu archivieren. Dies geschieht nicht im Rahmen der allgemeinen Maßnahmen des SaaS-Betriebs und es sind sehr kundenspezifische Vorgänge. Dies kann beispielsweise als individuelles Kundenprojekt erfolgen und muss es auch, da ein System, welches nach und nach „vollläuft“ in Sachen Performance und Wartbarkeit auf Dauer ein problematisches Verhalten bekommen kann. Wir empfehlen unseren SaaS-Kunden für diesen Sachverhalt einen regelmäßigen Austausch mit uns zu pflegen.

PenTests

Auch PenTests und eine regelmäßige Überwachung und Erneuerung von verwendeten Drittanbieterbibliotheken (häufig OpenSource) gehören zu den präventiven Maßnahmen. PenTests werden auf separaten Namespaces auf von uns gestellten Systemen innerhalb der Cluster durchgeführt. PenTests haben immer mehrere Komponenten. So wird z.B. über Portscans aktiv nach erreichbaren Services und Schwachstellen in der Infrastruktur gesucht, aber auch im Rahmen von zur Verfügung gestellten Userlogins die Software getestet auf z.B. Rechteausweitungen, SQL-Injection oder CrossSiteScripting um nur einige der standardmäßig durchgeführten Tests zu nennen. Auch veraltete Softwarebestandteile oder öffentlich bekannte Schwachstellen von verwendeten Softwarekomponenten werden verprobt und als Findings gelistet, sollte es hier Potential für Sicherheitsrisiken geben.

Scans

Unsere Software mit all ihren Komponenten unterliegt auch regelmäßigen automatisierten Schwachstellenscans, um hier über branchenübliche öffentliche Quellen Informationen zu potenziellen Schwachstellen zu erhalten. Diese sind bereits kategorisiert und werden von uns im Rahmen der Verwendung in der Software zusätzlich eingeschätzt, um hier ein umfassendes Bild zu erhalten.

Für den Fall der Fälle

Sollte der Fall der Fälle eintreten, dann möchten wir gewappnet sein. Daher tun wir alles dafür, dass in einem Notfallszenario keine Panik ausbricht, sondern ein geordnetes und eingeübtes Vorgehen kontrolliert ablaufen kann. Im Rahmen unserer Richtlinienlandschaft gibt es dazu diverse Dokumente, welche bestimmte Notfallszenarien beschreiben und ein Leitfaden sind. Desaster-Recovery Übungen sind ein wichtiger Bestandteil für Routine im Notfall. Diese werden von uns regelmäßig durchgeführt und optimiert.

Zum Glück führt nicht jeder Ausfall von Hardware auch gleich zu einem Systemausfall. Früher war man gewohnt, dass Software in einem Rechenzentrum auf einem bestimmten Server läuft und jeder Hardwareausfall eines Servers hatte direkte Auswirkungen auf die Lauffähigkeit oder Verfügbarkeit der darauf laufenden Anwendungen. Im Rahmen von Virtualisierungen der Umgebungen wurde hier bereits Redundanz geschaffen in dem man verschiedene Server zusammengeschaltet hat und auch z.B. Festplatten redundant ausgelegt hat. Cloud-Infrastrukturen verbessern diese Redundanzen nochmals. Durch horizontale Skalierungen können bereits in Lastphasen Hardwareressourcen dynamisch dazugeschaltet werden. Gleiches passiert auch bei Ausfällen der Hardware. Es werden neue Server „hinzugebucht“ und ersetzen die weggefallenen. Dadurch dass die Anwendung in vielen Einzelteilen (Containern) auf mehrere Nodes (vergleichbar mit Servern) laufen, sind bei einem Ausfall einer Node nur bestimmte Programmteile betroffen, die kurzzeitig wegfallen bevor der Automatismus in der Cloud dafür sorgt, dass eine neue Node bereitsteht und Kubernetes dafür sorgt, dass die Applikation wieder in ihren Originalzustand versetzt wird. Dieser Vorgang wird auch als Auto-Heal bezeichnet. Auch bei Festplatten gibt es eine mehrfache automatische Redundanz innerhalb von Rechenzentren oder sogar übergreifend.

Sollten diese Redundanzen nicht ausreichen und Rechenzentren oder gar eine ganze Region ist nicht mehr erreichbar, **dann kommen Backups zum Tragen**. Diese werden automatisiert vom System erzeugt und in mehreren Regionen innerhalb der EU gespeichert. Aus diesen Backups können die Applikationen vollständig wiederhergestellt werden. Sowohl die Datenbank als auch die Informationen zur Softwareversion wie auch die sonstigen Nutzdaten sind Bestandteil der umfänglichen Backups. Die Wiederherstellungen erfolgen auf Knopfdruck und in großen Teilen vollautomatisch, so dass ein rasches Wiederanlaufen gewährleistet werden kann.

Fazit

Wie Sie sehen, greifen sehr viele Maßnahmen ineinander, welche einen sicheren Betrieb als SaaS ermöglichen. Viele dieser Maßnahmen sind auch für einen Selbstbetrieb notwendig und es lässt sich der dahinterstehende Aufwand erahnen. Wir als Fact haben über die letzten Jahre bereits viele Erfahrungen im Bereich SaaS sammeln können und verbessern unsere Infrastruktur fortlaufend.

Wir sind gerne bereit weitere Informationen zu unserer Infrastruktur, unseren Maßnahmen und Prozessen mit Ihnen zu teilen und freuen uns über jeden Kunden, der in Zukunft unsere Fact Cloud nutzt.

Haben Sie Fragen oder möchten Sie sich zu diesen Themen austauschen? Lassen Sie uns darüber sprechen!

Thomas Ulken
Lead Software Architect
+49 2131 777 210
t.ulken@fact.de

Aleksandar Ivezić
Senior Manager, Sales
+49 2131 777 238
a.ivezic@fact.de

fact digital uncomplicators

Fact Informationssysteme & Consulting GmbH

Hauptsitz Neuss
Hellersbergstraße 11 | 41460 Neuss | +49 2131 777-0 | info@fact.de

Standort Frankfurt am Main
Wilhelm-Leuschner-Straße 81 | 60329 Frankfurt am Main | +49 69 8740313-121 | info@fact.de

Standort Erfurt
Erich-Kästner-Straße 1a | 99094 Erfurt | +49 2131 777-0 | info@fact.de

www.fact.de

Wir haben Ihnen dieses Fact About gerne zu unverbindlichen Informationszwecken überlassen. Bitte beachten Sie aber, dass die darin enthaltenen Informationen allgemeiner Natur sind und eine Beratung im konkreten Einzelfall nicht ersetzen können.

Die Fact Informationssysteme & Consulting GmbH hat diese Unterlage nach bestem Wissen erstellt und die Inhalte sorgfältig erarbeitet. Die Informationen werden ständig geprüft und aktualisiert. Gleichwohl können Fehler nicht ausgeschlossen werden. Bitte haben Sie deshalb Verständnis dafür, dass wir keine Garantie und/oder Haftung für die Aktualität, Richtigkeit und Vollständigkeit übernehmen. Infolgedessen haften wir nicht für direkte, indirekte, zufällige oder besondere Schäden, die Ihnen oder Dritten durch die Verwendung der Informationen dieser Unterlage entstehen.

Inhalt, Darstellung und Struktur dieser Unterlage sind urheberrechtlich geschützt und eine Nutzung, Verwendung, Reproduktion oder Weitergabe an Dritte – ganz oder teilweise – ist nur mit unserer ausdrücklichen vorherigen schriftlichen Zustimmung zulässig.

Alle Rechte sind vorbehalten.

Stand Mai 2024

Folgen Sie uns auf LinkedIn