DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Brand in der Cloud - wer ist verantwortlich

Was man aus dem Rechenzentrumsbrand bei OVH lernen sollte

12.04.2021Autor / Redakteur: Dipl.-Phys. Oliver Schonschek / Elke Witmer-Goßner

Wenn nach dem Brand in einem Rechenzentrum oder wegen kritischer Schwachstellen in Exchange-Servern Kritik an der Cloud-Sicherheit zu hören ist, sollte man genauer hinschauen. Nach dem Shared-Responsibility-Modell ist nicht immer der Cloud-Provider verantwortlich.

Cloud-Nutzer sollten die aktuellen Vorfälle zum Anlass nehmen, ihre eigenen Cloud-Security-Konzepte zu prüfen.
(Bild: © Feuerwehr Kehl)

Wir erinnern uns: Am 10. März 2021 ist ein Brand in einem der vier Rechenzentren von OVHcloud in Straßburg ausgebrochen, dem Rechenzentrum SBG2. Der Brand zerstörte hauptsächlich das Rechenzentrum SBG2 und beschädigte das Rechenzentrum SBG1 (von zwölf Serverhallen wurden vier zerstört). Die beiden anderen Rechenzentren waren nicht vom Feuer betroffen. Die Server in SBG3 und SBG4 wurden ausgeschaltet, aber nicht beschädigt.

Im weiteren Verlauf bot OVHcloud seinen Kunden unter anderem eine alternative Infrastruktur an: Bare Metal, Hosted Private Cloud und Public Cloud in den Rechenzentren von Gravelines (GRA), Roubaix (RBX), London (LON), Warsaw (WAW) und Frankfurt (FRA).

Die Folgen des Brandes in Straßburg waren immens. Viele betroffene Cloud-Nutzer beklagten einen Datenverlust, ohne Möglichkeit, die Daten wiederherzustellen. In manchen Medien konnte man lesen, dass das Vertrauen in die Cloud und in Cloud-Sicherheit nun schwer erschüttert sei. Dabei stellt sich allerdings die Frage, in welche Cloud-Sicherheit, die der jeweiligen Unternehmen oder die der Cloud-Provider?

Verantwortung für Cloud-Sicherheit ist geteilt

Unwiederbringlicher Datenverlust in Folge des Rechenzentrumsbrands bedeutet in aller Regel, dass die Cloud-Nutzer keinen Backup-Service gebucht oder selbst Backups erstellt haben. Aus gutem Grund verweist OVHcloud zum Beispiel darauf, dass es notwendig sein kann, dass die betroffenen Kunden eine Meldung bei der jeweils zuständigen Datenschutzaufsicht machen.

Eine solche Meldung müssen immer die Verantwortlichen machen. Und tatsächlich sind die Cloud-Nutzer für ihre Daten verantwortlich und nicht etwa der Cloud-Provider, wenn kein spezieller Backup-Service gebucht wurde. Datenschutzrechtlich bleibt der Cloud-Nutzer in der Verantwortung, wie die Datenschutz-Grundverordnung (DSGVO) zeigt.

Aus Sicht der Cloud-Sicherheit gilt das Shared-Responsibilty-Modell: So findet man zum Beispiel in den „Besonderen Vertragsbedingungen OVH Public Cloud“: Der Kunde ist insbesondere beim Hosting sensibler und/oder für die Fortführung seiner Tätigkeit notwendiger Inhalte und/oder Daten in vollem Umfang selbst verantwortlich für die Sicherung (das Backup) seiner Daten, die Einführung und das Management eines Kontinuitätsplans (Business Continuity Plan) und/oder eines Notfallwiederherstellungsplans (Disaster Recovery Plan) und ganz allgemein für alle technischen und organisatorischen Maßnahmen, die es dem Kunden ermöglichen, seine Geschäftstätigkeit im Falle einer gravierenden Funktionsstörung des Dienstes, welche die Kontinuität seiner Tätigkeit und die Verfügbarkeit und Integrität seiner Inhalte und Daten beeinträchtigen könnte, fortzuführen.

Ebenso findet man in den Vertragsbedingungen: OVHcloud weist den Kunden ausdrücklich darauf hin, dass ein Snapshot keine vollwertige und ordnungsgemäße Sicherung der Daten der Instanz darstellt, sondern nur eine „Momentaufnahme“ davon. Ein Snapshot entbindet den Kunden also in keinem Fall von der Erstellung eines Backups seiner Daten gemäß § 6 der vorliegenden Bedingungen.

Was ist ein Shared Responsibility Model?

Backup der Daten und Patchen von Anwendungen obliegen dem Cloud-Nutzer

Ein zweites Beispiel für massive Sicherheitsprobleme, das man sich ansehen sollte, sind die kritischen Schwachstellen bei Exchange-Servern. So meldete das Bundesamt für Sicherheit in der Informationstechnik (BSI) Anfang März 2021: Zehntausende Exchange-Server in Deutschland sind nach Informationen des IT-Dienstleisters Shodan über das Internet angreifbar und mit hoher Wahrscheinlichkeit bereits mit Schadsoftware infiziert. Betroffen sind Organisationen jeder Größe. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat begonnen, potenziell Betroffene zu informieren. Es empfiehlt allen Betreibern von betroffenen Exchange-Servern, sofort die von Microsoft bereitgestellten Patches einzuspielen.

Auch wenn man die Dienste des jeweiligen Exchange-Servers über eine Cloud bezieht, ist es nicht automatisch der Cloud-Anbieter, der sich um das Patchmanagement kümmern muss. Vielmehr ist der Anbieter nur dann verantwortlich, wenn dies im Rahmen eines Exchange Managed Service vereinbart wurde. Andernfalls müssen die Cloud-Nutzer, die einen Exchange-Server selbst in der Cloud betreiben (Private Exchange), die Sicherheitslücken selbst angehen.

Massenhack von Microsoft Exchange

Cloud-Migration oder Medienbruch – so schützen Unternehmen ihre Daten

Cloud-Security-Konzept mit Shared-Responsibility-Modell abgleichen

Die skizzierten Vorfälle machen deutlich, wie wichtig es ist, als Cloud-Nutzer die geteilte Verantwortung in der Cloud-Sicherheit im Blick zu behalten und das eigene Konzept für die Cloud-Sicherheit mit dem Modell der geteilten Verantwortung abzugleichen.

Wenn Sicherheitsaufgaben fälschlich beim Cloud-Anbieter gesehen werden, entsteht eine gefährliche Scheinsicherheit, und es klaffen Sicherheitslücken in der Cloud auf, die schwerwiegende Folgen haben können, wie die aktuellen Vorfälle zeigen. Das Vertrauen in die Cloud an sich sollte also nicht erschüttert sein, vielmehr muss hinterfragt werden, ob das Bild, das man sich von der Cloud-Sicherheit macht, auch wirklich stimmt.

Quelle: https://www.cloudcomputing-insider.de/was-man-aus-dem-rechenzentrumsbrand-bei-ovh-lernen-sollte-a-1013655/

Ausfälle und Datenverluste OVH-Großbrand hat gravierende Folgen

17.03.2021Autor / Redakteur: Martin Hensel / Dr. Jürgen Ehneß

Der Großbrand im OVH-Rechenzentrum in Straßburg verursachte große Aufmerksamkeit und mitunter verheerende Folgen für Kunden des Cloud-Hosters. So verschwanden insgesamt 3,6 Millionen Websites durch den Brand aus dem Netz.

In Straßburg wurde ein Rechenzentrum des Cloud-Hosters OVH durch einen Brand zerstört. (Bild: gemeinfrei / Pixabay)

In den frühen Morgenstunden des 10. März 2021 brach im OVH-Rechenzentrum SBG2 in Straßburg ein Feuer aus. Der Brand konnte nicht mehr unter Kontrolle gebracht werden, das fünfstöckige Datacenter mit Platz für rund 12.000 Server brannte völlig aus. Zudem wurde das benachbarte Rechenzentrum SBG1 teilweise zerstört. Die Standorte SBG3 und SBG4 konnten isoliert werden, sind aber derzeit nicht einsatzfähig.

OVH ist derzeit mit Reparaturmaßnahmen beschäftigt und hat 111 Fachkräfte im 24-Stunden-Dienst vor Ort. Im Rechenzentrum SBG2 war nichts mehr zu retten; es handelt sich um einen Totalverlust. Im beschädigten SBG1 sind vier von zwölf Serverräumen betroffen, SBG3 und SBG4 sind unbeschädigt. Derzeit ist der 22. März als Termin für einen graduellen Neustart der Server in Straßburg vorgesehen. Zudem erhalten betroffene Kunden Ersatzkapazitäten in den OHV-Standorten Roubaix und Gravelines. Insgesamt will der Cloud-Anbieter in den kommenden Wochen rund 15.000 neue Server bereitstellen, um die Ausfälle zu kompensieren.

Massive Auswirkungen

Die Folgen des Brandes sind verheerend: Direkt nach dem Feuer waren rund 3,6 Millionen Websites über 464.000 Domains hinweg offline. Laut dem britischen Internetdienstleister Netcraft waren etwa 18 Prozent aller mit OVH verbundenen IP-Adressen nicht mehr erreichbar. Betroffen war eine Vielzahl an Web-Präsenzen, darunter auch staatliche Stellen aus Polen, der Elfenbeinküste, Frankreich, Wales und Großbritannien. Am heftigsten hat es .fr-Domains erwischt: Nach dem Feuer waren 1,9 Prozent aller .fr-Domains weltweit vom Netz.

Besonders bitter: Die in Rauch aufgegangenen Daten sind wohl endgültig verloren. Auf die kostenpflichtige Option eines Backups in einem anderen OVH-Rechenzentrum hatten viele Kunden verzichtet. So verlor der Spielehersteller Facepunch alle europäischen Server seines Online-Spiels „Rust“ inklusive aller gespeicherten Daten. Ähnlich erging es der international tätigen Anwaltskanzlei Leroi & Associés, die ebenfalls einen erheblichen Datenverlust zu beklagen hatte. Man darf davon ausgehen, dass dies nicht die einzigen derartigen Fälle bleiben werden.

Kritik und Verschwörungstheorien

Nach dem Brand sah sich OVH harter Kritik ausgesetzt. Experten bemängeln unter anderem die Containerbauweise des Rechenzentrums und deren Eigenheiten. So habe es zwar Alarmsysteme gegeben, aber keinerlei Löschanlagen wie beispielsweise eine Sprinklerinstallation. Dies sei ein wesentlicher Grund, warum sich der Brand ungehindert habe ausbreiten und letztlich das gesamte Rechenzentrum vernichten können. Die Ermittlungen zur Ursache dauern noch an, ersten Informationen nach könnte eine am Vortag gewartete USV-Anlage der Auslöser gewesen sein.

Im Internet werden derweil diverse Verschwörungstheorien im Zusammenhang mit dem OVH-Brand diskutiert. So soll OVH beispielsweise bereits 2019 mit dem Aufbau einer französischen Cloud beauftragt worden sein, wobei eine US-Beteiligung gezielt ausgeschlossen worden sei. Mit im Boot sei dabei der Konzern Dassault gewesen. Dessen Erbe, Aufsichtsrat und Politiker Olivier Dassault kam nur zwei Tage vor dem OVH-Brand bei einem Hubschrauberabsturz ums Leben – Grund genug für angeregte Debatten im Internet. Auch die erst Ende vergangenen Jahres von OVH veröffentlichen Börsenpläne sorgen im Netz wegen ihrer zeitlichen Nähe zum Brand für Stirnrunzeln.

Quelle: https://www.cloudcomputing-insider.de/ovh-grossbrand-hat-gravierende-folgen-a-1008467/