

Adalberto Trujillo

Infrastructure Security and Resilience

OVH Cloud is a Cloud Data Center that manages over 1.5 million customers around the world. A fire broke out in Strasbourg, France on March 10th, 2021, at approximately 00:47. OVH is comprised of 27 datacenters worldwide and 3 of them are located in France, where the fire occurred. The affected datacenters that were impacted by this fire were SBG2 and a partially affected data center named SBG1. This research paper will discuss the leading events and hazards that led to this disaster with a focus on what roles were involved in response to this infrastructure disaster.

Furthermore, this research paper will also discuss the relevant vulnerabilities that were discovered and the consequences that impacted this disaster. Lastly, this research paper will identify external site dependencies, the restoration process, and resilience analysis and will include recommendations to enhance resiliency and vulnerability reducing to this infrastructure disaster. On March 10th at approximately 00:47, a fire broke out in one of the cloud data centers owned by OVH. The impacted cloud data centers were located in Strasbourg, France.

OVH Cloud issued a public statement on their cloud server support website regarding the incident. They wrote “we are currently facing a major incident in our Data centers of Strasbourg with a fire declared in the building SBG2. Firefighters were immediately on the scene but could not control the fire in SBG2” (OVH Cloud Server Support, 2021). OVH Cloud Datacenters are highly used by various private sector companies around the world. Due to the fire destruction that impacted a few data centers on this site, these private sector companies

and organizations were urged to activate their disaster recovery plan to get their sites back up and running again. Furthermore, they were instructed to change their Domain Name System (DNS) to point it at another server and upload their site backups immediately.

The impact of this disaster has led to a few hazards to be identified and relevant parties to respond to control this disaster. One of the hazards was that there was maintenance on the uninterruptible power supplies (UPS) which served as emergency power in case if there was a power outage. This UPS was assigned to SBG2 datacenter and was labeled as UPS7. Relevant parties who responded to control the fire were the firefighters and OVH Cloud designated team in accordance with protocols in place for the energy rooms located in these data centers.

Furthermore, OVHcloud teams were assigned to study images from surveillance cameras on the Strasbourg site, and authorities and insurance companies were contacted to investigate the outbreak and identify the cause of the fire. Although the investigation is at an early stage of the process, it will take several months to complete. The vulnerabilities and consequences will be discussed leading to this disaster. During the investigation process to determine the cause of the fire, “firefighters found UPS systems burning when they reached the disastrous fire at OVHCloud's SBG2 data center in Strasbourg on Wednesday, the French cloud provider has revealed” (Judge, 2021). One of the vulnerabilities that were found in this disaster was that UPS7 which was assigned to the SBG2 datacenter was under maintenance the day before the fire broke out.

Another vulnerability that was found in the SBG2 datacenter was that the datacenter where the fire occurred "was an older generation center built in 2011 and that the company is working towards replacing older infrastructure with newer technology” (Sharma, 2021). If older

and legacy systems are used in modern technology infrastructure, there could be faulty within the hardware which will require a lot of maintenance and there will also be software/hardware/power related problems regarding performance issues. According to the thermal surveillance cameras from UPS 7 and UPS 8, a fire was detected on both UPSs which was one of the reasons for the fire.

SBG2 was in the area of “hosting towers” which contained servers inside and were designed as metal cubes for efficient cooling. Due to the destruction of the fire of SBG2, it also “destroyed four rooms of data center SBG1 and caused a shutdown of the servers in SBG3 and SBG4” (Coble, 2021). The consequence for the fire destruction has led to 3.6 million websites on 464,000 domains to be offline. These domains were being hosted by news sites, online shops, banks, and webmail services, all of them being shut down as a result of the fire. One major site that was affected by this outage was the UK Government’s Vehicle Certification Agency website.

Housing multiple datacenters in one location can be a hazard and also a vulnerability. If one data center is impacted by the fire, another data center will also be impacted by the fire. This illustrates a domino effect where datacenters would be knocked down offline one-by-one if they are in the same vicinity of the fire. Some companies who used OVHCloud didn't have disaster recovery plans in place in case something like this happens, therefore the consequence was that they had to rebuild their websites as quickly as they can and point to another DNS to another server that isn’t impacted by the fire destruction.

Due to the firefighters trying to stop the fire ablaze in the impacted data centers, they weren't able to control the fire in Datacenter SBG2. The firefighters who were the first to

respond to the fire remained at the site of the impacted data center until the building cooled down. This is to make sure no unaffected data center is overheated which can potentially cause failure to the unaffected datacenters. The fire destruction has also left water damage to some of these data centers which is another identified vulnerability. "The fire was extinguished by 7 a.m. local time, but firefighters continued to water the buildings to reduce the temperature. Data centers SBG3 and SBG4 were isolated in time, but to prevent a fire there, they were switched off from power" (HostTelecom, 2021). Datacenters in general become overheated if proper ventilation is not implemented correctly. Due to the fire and the heat from the fire disaster, the unaffected datacenters had to be switched off to prevent overheating and not cause another fire damage.

In order to restore services and replace impacted datacenters equipment, support teams needed to be deployed to restore all affected datacenters in the location of the fire disaster. Firefighters didn't allow any staff member in the building until it was safe to do so. Upon extinguishing the fire, a support crew was deployed to restore datacenters and get all servers back up and running again. From the morning of the 10th of March, "teams were mobilized with one goal: to restore at least an equivalent service as soon as possible, for as many of our customers as possible" (OVHCloud, 2021). Upon determining the cause of the fire, firefighters took thermal images which showed two UPS units to be ablaze with fire. More than 30 OVHCloud employees were deployed to Strasbourg to bring back up datacenters SBG1, SBG2 & SBG3. "Electrical, climate and networks engineering: several partners, specialized in cabling and restoring datacenter pillars, worked to support the restoration of the power, the network

distribution and the cooling systems" (OVHCloud, 2021). All of these relevant parties were called in to help with the restoration of the impacted data center where the fire occurred.

OVHCloud set priorities in place at the start of the restoration process. The first one is to reserve infrastructures and data centers in other locations so that affected customers can be able to use these datacenters at other site locations to bring their site back up and running again. Therefore, companies who had reserved servers on the impacted datacenter of the fire site were migrated to another data center and urged to initiate their disaster recovery process. For those who did not back up their data, it will be very difficult to retrieve this data loss and it is unclear to this point if OVH will be able to restore this loss data that was saved on the cloud servers on the impacted datacenters.

New infrastructure was provided to deploy on the impacted datacenters to enhance OVHCloud Datacenter equipment. Due to the destruction of the fire, a lot of hardware equipment such as servers, UPS's and ventilation, fiber cables, needed to be all replaced. As for the restoration of the impacted data centers, SBG1 was inspected, cleaned, and repaired. They were reconnected to get SBG1 up and running again. Since SBG2 was completely damaged from the fire, OVHCloud prioritized its customers with alternative servers to get connected as quickly as possible. Datacenter SBG3 was at about 95% operational, it was made available to customers. However, there was a malfunction on the equipment of this data center on April 1st at around 6:00 AM but had no impact on any service. As for SBG4, there was no fire damage impact on this data center and its servers were 100% available to customers. All of these data centers had to be fully cleaned and the cleaning time for each server rack took approximately 7 hours to clean.

Environmental experts were deployed on the scene to assess the smoke impact.

Although the investigation is still ongoing, during the start of the fire, “detection systems were instantly activated and our teams were able to respond according to the protocol in place for the energy rooms, where the smoke was detected” (OVHCloud, 2021). This shows how detection systems were effective which brought to the attention of firefighters to respond to the scene of the fire and have OVH Cloud support crew be aware of the incident. Data recovery specialists were also called on scene to try to determine if it's possible to recover data from hard drives in the rooms affected by the fire.

During the restoration process, electrical engineers and network engineers were called in to restore power and network dedicated to the datacenters. “On 11 March, two express containers dedicated to the network and high-voltage electricity were prepared in Croix and sent out for installation in Strasbourg on 12 March” (OVH Cloud, 2021). Datacenters require a significant amount of dedicated power to function properly to avoid any power-related issues from the high use of electricity. Network engineers were deployed on-site “to physically migrate the servers from SBG1 to the other Strasbourg datacenters (SBG3 and SBG4)” (OVHCloud, 2021). Following the fire disaster, several servers needed to be physically moved to an unaffected data center and restore service on them as quickly as possible.

OVHCloud prioritized the restoration of impacted cloud servers to be replaced as quickly as possible. OVHCloud responded quickly as possible by deploying multiple employees to the site of the disaster. Furthermore, multiple external site dependencies and relevant parties were called in to assist with the disaster. These site dependencies and relevant parties included multiple OVHCloud Employees, Firefighters, Electrical, Climate, Environment, Network, and

Data Recovery Engineers. OVH was able to quickly secure the site and ensure a safe environment before beginning the restoration working process. Furthermore, general management, civil engineering, and logistics were called in to strengthen the structure of the impacted datacenters and ship in new equipment as quickly as possible to stock up on new servers and replace the damaged ones.

To accommodate the businesses whose servers were impacted by the fire disaster and initiating disaster recovery plans, there was a timely schedule set to get the impacted data centers functioning again as quickly as possible. However, "the schedule is also subject to Covid-19 and security protocols, defined for on-site interventions, with the goal of maintaining the health and ensuring the safety of our technical teams" (OVH Cloud, 2021). Due to the current COVID-19 pandemic situation, it was more complex for employees to assist in the disaster site. Government protocols were respected to ensure the safety of all employees deployed to the site of the fire disaster.

As of April 22nd, 2021, multiple cloud services were partially or fully restored. Bare metal cloud is at 99% restored, "the last 400 servers from SBG1 are in the process of being restored in SBG3 by April 25th, 2021" (OVH Cloud, 2021). 99% of public cloud services were restored to customers whose servers were impacted by this fire disaster, and 88% of private hosted cloud services were partially restored to customers. "Through our 32 datacenters, 400,000 servers, 2 factories, 2,450 employees, and our network of over 3,000 partners in the 140 countries where our services are available, we will do everything we can to restore this unique bond that makes OVHcloud the market leader in providing a cloud service that respects European values" (OVHCloud, 2021). This shows how resilient OVHCloud is on restoring its infrastructure and

services and any new investigation findings and information will draw key lessons which will serve as lessons learned for similar disasters not to occur again.

We can see how similar events such as OVHCloud that can be replicated such as datacenters being destroyed which interrupted website services from many businesses and organizations. For example, the terrorist attacks leading up to 9/11 show how data centers can be vulnerable if they are located in the same vicinity of the organization or business that are using these data centers. "9/11 and later major disasters as leading to the modern cloud storage industry. The attacks showed that a single data center is more vulnerable than backing up data at multiple locations," (Gross, 2011). Having a single data center that houses all the servers of a company or organization is a hazard that could be vulnerable to natural disasters, physical/cyber-attacks, or catastrophic disasters. If any of these disasters occurred in this single data center that operates a business/organization, their entire operation can be wiped out in an instant, especially if the business or organization had no backups of their data.

We can see how OVH Cloud housed all of their data centers in one single building which was the reason for multiple data centers to go offline. A single point line of failure can lead to multiple failures to occur if they are interconnected to each other. By taking a look at another example of how data center facilities can be vulnerable to attacks, we can point to a plotted attack at an Amazon Web Services data center in Virginia. "a 28-year-old Texas resident, who was charged with plotting to blow up an Amazon Web Services facility in Ashburn, Virginia. Pendley was arrested after allegedly attempting to obtain an explosive device from an undercover FBI employee in Fort Worth, saying he planned to attack a data center and "kill off about 70 percent of the Internet" (Miller, 2021). Following the events of 9/11, the data center

industry is vulnerable to catastrophic attacks, natural disaster attacks, and man-made attacks and more security posture has to be put in place for these data centers to be well protected on any of these known attacks.

Following the OVH Cloud Datacenter fire disaster, there are lessons to be learned and recommendations to be made to enhance resilience and reduce vulnerabilities found on this infrastructure. “Early indicators point to the failure of a UPS, causing a fire that spread quickly. However, there may be other reasons why a fire started at or near that location. At least one of the UPSs had been extensively worked on earlier in the day, suggesting a maintenance issue may have been a main contributor” (Lawrence, 2021). SBG2 Datacenter was an older generation data center that was built in 2011. Due to the data center having outdated infrastructure, it required a lot of maintenance. Following the recent maintenance on UPS 7, which was assigned to SBG2 Datacenter, there was a point of failure which led to smoke coming out of UPS 7 and then moments later burst into flames.

OVH Cloud was working towards replacing this older infrastructure data center with modern technology infrastructure. OVH Cloud didn't prioritize the replacement of this older infrastructure, which lead to this fire disaster on this infrastructure. There needs to be a prioritization of replacing older infrastructure to avoid any problems that relate to software issues, hardware issues, or any power-related issues with combining powerful UPS with an older data center infrastructure, which could lead to a hazard and cause a major disaster. To establish prioritizing of replacing older infrastructure on a datacenter, first, there needs to be coordination between its customers and inform them about maintenance being conducted on their servers. OVH Cloud could be able to migrate these customers to another data center that

is not an older generation datacenter until the upgrade was complete. This would've prevented the fire hazard from UPS 7 which was used on SBG2, an older generation datacenter.

Furthermore, "SBG2 was built in 2011 using a tower design that has convection-cooling based "auto-ventilation." Cool air enters, passes through a heat exchange for the (direct liquid) cooling system and warm air rises through the tower in the center of the building" (Lawrence, 2021). Due to the tower design, this led the tower to act more like a chimney. This was one of the reasons why the fire was so powerful that it made it difficult for firefighters to put out the fire on SBG2.

There needs to be a redesign on OVH Cloud datacenters with an updated design that can withstand fire damage and implement a better solution for cooling systems. Such implementations can include adding modern ventilation to withstand the heat that is build up by the data centers. Furthermore, a fireproof design needs to be designed to handle a certain amount of fire, such as designing the datacenter with titanium surroundings that can withstand higher temperatures and are heat resistant.

Lastly, businesses and organizations need to rethink their disaster recovery plan and not put their eggs in one basket. These businesses and organizations need to backup data on multiple data centers, preferably far away from each other to avoid losing all their data and wipe out their entire operations from a disaster such as the one which occurred in the OVH Cloud Strasbourg site in France. Having a carbon copy/image of data and have it sync regularly, will ensure data to be restored quickly and avoid losing any data, instead of building a site from scratch which will take weeks to build.

Works Cited:

- (2021, April 18). *OVH Data Center Fire Darkens Popular Sites Worldwide*. Search Engine Journal. <https://www.searchenginejournal.com/ovh-data-center-fire-darkens-thousands-of-sites-worldwide/398485/#close>.
- Judge, P. (2021, March 12). *OVH fire: Octave Klaba says UPS systems were ablaze*. All Content RSS. <https://www.datacenterdynamics.com/en/news/ovh-fire-octave-klaba-says-ups-systems-were-ablaze/>.
- Sharma, A. (2021, March 12). *OVH data center fire likely caused by faulty UPS power supply*. BleepingComputer. <https://www.bleepingcomputer.com/news/security/ovh-data-center-fire-likely-caused-by-faulty-ups-power-supply/>.
- Writer, S. C. N. (2021, March 15). *OVH Data Center Fire Impacts Cyber-criminals*. Infosecurity Magazine. <https://www.infosecurity-magazine.com/news/ovh-data-center-fire-impacts/>.
- *OVHcloud, a large cloud provider, lost its data center in France by fire*. Host. (2021, March 11). <https://www.host-telecom.com/industry-news/ovhcloud-a-large-cloud-provider-lost-its-data-center-in-france-by-fire/>.
- OVHCloud. (2021). *Strasbourg datacentre: latest information...* Strasbourg datacentre: latest information. <https://www.ovh.com/world/news/press/cpl1787.fire-our-strasbourg-site>.
- Gross, G. (2011, September 8). *9/11: Attacks Changed the Way Companies View IT*. PCWorld. https://www.pcworld.com/article/239693/911_attacks_changed_the_way_companies_view_it.html.
- Miller, R. (2021, April 12). *Foiled Plot to Attack Amazon Reflects Changing Nature of Data Center Threats*. Data Center Frontier. <https://datacenterfrontier.com/foiled-plot-to-attack-amazon-reflects-changing-nature-of-data-center-threats/>.

- Lawrence, A., & Judge, P. (2021, March 31). *Learning from the OVHcloud data center fire*. All Content RSS.
<https://www.datacenterdynamics.com/en/opinions/learning-ovhcloud-data-center-fire/>.