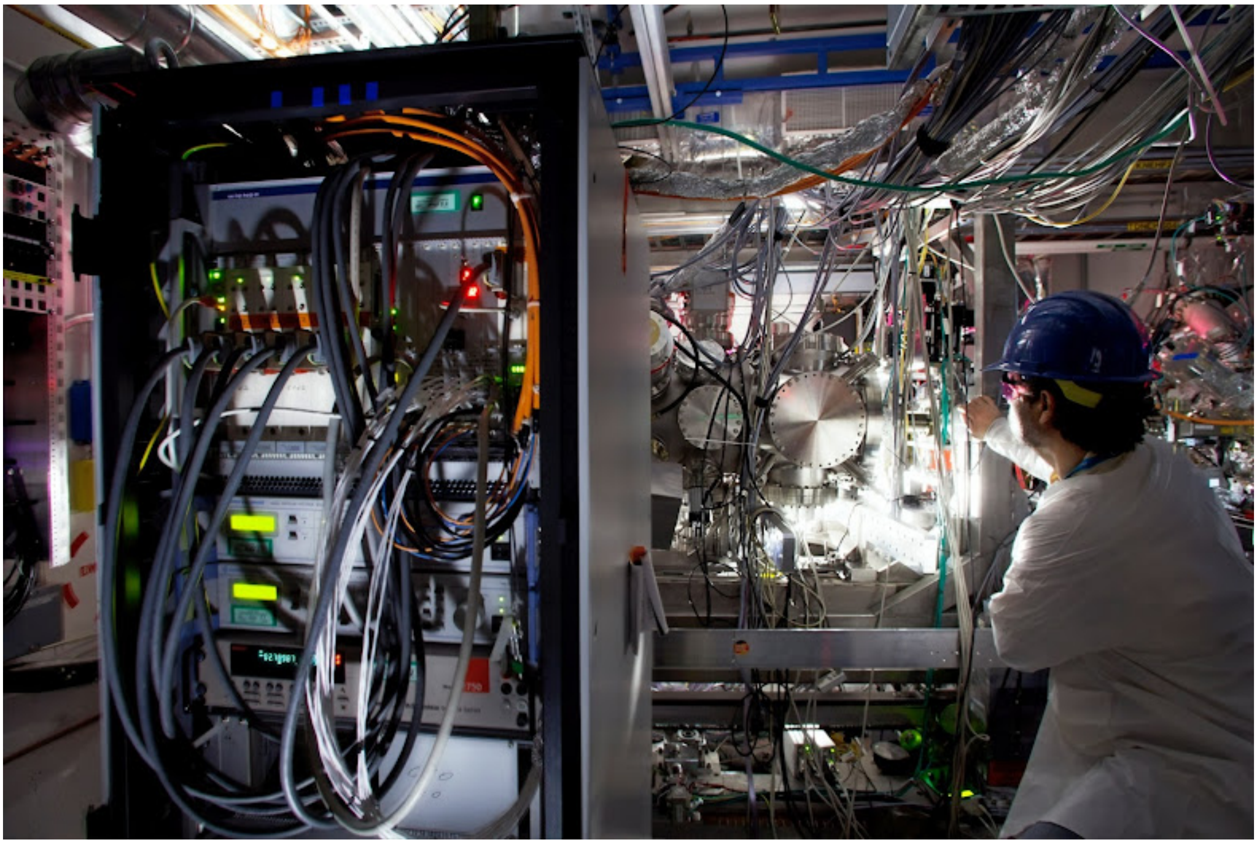
What is Operations?

September 11, 2020



If your web app has a bug, and a hacker manages to capture your entire user list, that's on you. The cloud provider has no responsibility when it comes to the code you deployed. A good engineer will write safe code, but it's never possible to ensure that your app will be completely free of bugs. That's why a proper security environment includes things like regular audits, penetration tests, written policies for your employees and users, good firewall rules, and so on.

There is a lot of necessary knowledge when it comes to securing an entire cloud infrastructure. For example, if you host a Linux instance in AWS, are you allowed to do a penetration test to see whether any port are open on your instance? The answer is no. These are the things a good IT person will know, especially if they have a SecOps background.

When you ask a software developer to create a web app, they will likely ask you where they should be deploying it, then start coding. Maybe they'll even have some DevOps knowledge and be able to setup a deployment pipeline. Although in many cases, probably not.

A proper environment includes a lot of moving pieces. First, you want a Test and a Production environments, and they need to be as close to each other as possible. The last thing you want is to deploy a feature update that brings your entire site down. Then you want a build pipeline that will deploy your code to Test, and make sure that tests are actually run correctly, before it gets deployed to Production.

Once in Production, the code should be scalable. This means that if the instance the code runs on isn't big enough for the demand in traffic, it should scale up, or more instances should be brought up. But scaling is more than enabling an auto-scaling group in your web dashboard. What if at some point you realize that you have a large influx of traffic from the UK, but your web site is hosted on the US west coast? Having a geographically distributed infrastructure is crucial if you want international visitors, because no one will wait for long when a site doesn't load fast enough.

All of these concerns are things that IT has had to deal with for a long time, and that typically gets handled by Operations.

Backups

Believe it or not, but to this day there are still businesses that don't have backups, and that get forced to close their doors after they get hacked, infected with ransomware, or suffer a critical hardware failure. A non-techy business owner might be tempted to install a free backup software, or manually use a Zip utility to backup files that they think are important. But what you may not realize if you don't have an IT background, is that malware is very smart these days. If you have a backup instance that's reachable from one of your infected machines, the malware will actively scan your network, find it, replicate itself to your backup server, and wipe it out. A backup solution needs to be configured so that it reaches out, and no one can reach in.

Monitoring

Typically, I see two types of environments when it comes to logs and monitoring. On the one hand, businesses without an active IT team will not even bother with logs. If something happens and they need to review the logs to find out what happened, someone needs to connect to the server, then look around for logs, hoping they're actually there. On the other hand, I see businesses that setup an expensive array of monitoring software, export every possible log and metric from every system they own, and then dump it all in a giant pool of data. Then no one ever does anything with the terabytes of data, at least until you need to search through it.

There is no right answer when it comes to a monitoring solution, but there are a lot of wrong answers. The entire point of monitoring is for you to be able to tell right away when something goes wrong, usually with metrics, and find answers as to what exactly happened, usually by parsing logs.

Governance

The Operations group also needs to assist the business owners to make sure they are doing the right things. It's easy for managers to take decisions based on finances and potential revenues, everyone understands the need to make money. But if you decide to deploy your web site in the US, then start accepting personal data form European citizens, you're likely to be breaking EU directives. If you've decided to allow an external contractor to access your infrastructure, and that person then opens up a port that you didn't expect, you may end up with hackers coming into the environment while no one is looking.

IT is a crucial part of all businesses, and is important especially in startups. If you don't start with proper policies from the on-set, you'll always be playing catch-up. It's not because you're 100% virtual, with no physical office, that IT is suddenly redundant. Operations is about far more than clicking on the "Launch VM" button on your web host's dashboard.