Overview of Two NIST Publications on Cloud Computing Demo

Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission.

Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

DM20-0577

Instructor: In this video, we're going to take a look at two NIST special publications. The first one is SP 800-145, which defines cloud computing. It's actually a relatively short document, but what you have is the essential characteristics of cloud computing, meaning on-demand, self-service, broad network access, resource pooling, rapid elasticity, measured service. It also has the service models listed so we know what software as a service is, along with platform as a service and infrastructure as a service, and finally the deployment models, private, community, public, and hybrid. It's not a very long document, as I said, but it is the foundation of what cloud

computing is, and it's referenced quite often by the cloud security alliance as well as your cloud service providers and what they define cloud to be.

The next document is special publication 800-144. This one is quite a bit longer, about seventy/eighty pages and it is the guidelines for security and privacy in public cloud computing. So, we won't take a look at everything within the table of contents, but I have a few things highlighted that are worth mentioning to reinforce some of the key aspects or key learning objectives for our course.

The first is in the executive summary. It's important to carefully plan the security and privacy aspects of cloud computing solutions before you engage them. So, it's really important to understand your data and your business. What are you collecting? How are you collecting it? How does it need to be protected, and what are the controls associated with that because, once you can define all of that on paper, then you can start to evaluate what cloud solutions are out there to help you provide those services.

It's also important to understand that, whatever those cloud offerings are, they may not exactly fit one to one with what your needs are. So, you need to take a look at that and see what they have for antivirus, for vulnerability assessment scanning, the various agents, controls for

identity and access management, etc. And you want to try and get as closely as you can with the solutions that they offer, and, where they can t be a one-to-one match, where can you develop compensating controls to meet your needs.

The next consideration is regarding accountability. Since you don t actually control all of the resources in that area, it's really important that you implement the right management practices. How are you going to keep track of all of the services that you're subscribing to, the resources that are available, who has access to them, what privacy controls are in place, all of that good stuff? You need to have that as documented as much as possible, and you need to have good processes in place for maintaining that documentation.

You also need to collect as much information as possible. You've got to be wary of information overload here so tuning the log collection and the alerting mechanisms inherent with the cloud so that, when you do get alerts, it's something you can take action upon. That's really where the continuous monitoring comes in. It's like what kind of automated tools can you put in place to guarantee your success.

As far as managing risk in the cloud, It's a little bit challenging because, again, you don't control the entire environment. So, you don't see what the cloud provider has really got in place for their security and privacy

controls, and that's why it's important to craft your service level agreements, and when you get into a contract with a cloud provider, you want to see what they can provide, whether it's their third-party audit or what controls they have. A lot of times a cloud service providers won't provide those two without an NDA in place, a non-disclosure agreement, or as part of your cloud services agreement.

Here, just before we get into the meat of the paper, there's a list of publications that are available, including federal information processing standards and NIST special publications that really help guide what cloud security is, or security in general, and they have adapted them a bit for this particular document.

So, we're going to skip ahead just a little bit and come to a particular point of interest here. In this section, We're talking about security and privacy upsides, what are the benefits of cloud computing. And one of the ones that we want to point out is this data concentration, the idea that your data is now in one place, so it makes it easier for it to be accessible by everybody within your organization. Instead of having it distributed on different laptops and servers and how is it backed up and maintained and having maybe different procedures in place for each one, now we have everything inside of one cloud, perhaps. So, managing it might be a little bit easier. Access

might be a little bit easier, but you also add a little bit of a risk because if something happens to that data in that one spot, that's obviously not available to you or your company.

That's part of the risk also associated with a shared multi-tenant environment, the idea that if an attacker could pose as a consumer to exploit vulnerabilities within the cloud, they could then pivot and access other legitimate resources. So, protecting that management plane is paramount for a cloud service provider, and you need to understand that, when you do have your services in a cloud, there is a bit of a risk that if some other tenant or customer were to get compromised, that could potentially lead to your compromise if, in fact, it was serious enough.

And then when we talk about Internet facing services, we need to understand that a lot of the things that we're not defining are accessible via the Internet. So, previously, they might have only been available on your internal network, and now they exist within the cloud. So, how are you going to allow access to those resources? Are you going to have a VPN tunnel between your enterprise and your cloud environment so that you're still restricting access, or are you going to open that up to the Internet in general? In which case, you might need access control lists via IP addresses or some other mechanism.

You re also dealing with a risk of loss of control. You don t actually own the underlying infrastructure. So, you Don't control it. You don't maintain that asset inventory, which could put you at risk of non-compliance. So, working with your cloud provider to make sure you have the documentation that demonstrates their ability to meet these compliance controls and these compliance requirements is paramount.

Here's an example of just a scenario of how botnets in the cloud might be used. There's a couple of scenarios here. The first being that, because it's easy enough to spin up lots and lots of machines in a cloud environment and have them launch a denial of service against a particular infrastructure, either yours or a cloud provider per se, it's kind of hard to track that down. Things spin up. They go down. Spin up. Go down. And it could be coming from all over the world and multiple different IPs from different regions from a specific cloud provider. So, it is a risk that they have this distributed computing environment that can be used to attack not just you but the cloud provider itself. So, that is a risk that you need to be aware of. In most cases, they have denial of service protections in place at standard and advanced levels.

Another thing to understand is the risk associated with the power of the cloud. So, in this particular example, four hundred virtual machines were pulled together to do some password

cracking in a short amount of time. So, you can use some of these things for good or evil if you're harnessing that power for, in this case, a compute intensive applications. Another example might be crypto mining. So, it makes your cloud resources a very attractive target so somebody that can compromise those and then use that compute resource for something like crypto mining or password cracking or that type of thing, and which case, it saves them some money, and they're able to accomplish this nefarious activity.

800-144 does a great job of introducing some governance and compliance related things to keep in mind, one of which is the E-Government Act of 2002, which requires federal agencies to complete a privacy impact assessment, or a PIA. You'll need to do this with your cloud service provider, but, again, it really goes back to what applications and systems are you going to have in the cloud environment, what sort of data or information is going to be residing on them, and then based off of that classification, what controls are in place to protect that.

And then here's another one that's important to understand is any external provider handling federal information or operating information systems on behalf of the federal government must meet the same security requirements as the source federal agency. So, that just means you can't downgrade. If you have to have certain protections for

protecting your information, all of those types of controls need to be in place when you migrate to the cloud.

And then you also need to consider what sort of information that is. If it's payment card data or health information, that requires additional protections as well. You need to make sure that those can be met by your provider.

And then we've got one last thing on this page at least for us to discuss, and that really is understanding that when that information crosses borders, whether it's for backup purposes or distribution for load balancing, whatever the case might be, there might be different rules around governance in those jurisdictions. So, you need to understand those very well. Where is your data being stored? Is there a way you can control it to restrict it to certain regions? If it's going to be in another region, what sort of assurances do you have from your cloud service provider that those controls are being adhered to?

Another important consideration is electronic discovery. So, electronically stored information is not just email and attachments, but there's other objects that are stored on the computer, such as metadata. So, how is that being preserved within your cloud environment? Is there retention time set up on logs so that your flow data or some other logs are automatically deleted within thirty days or sixty days, and if you need

them stored for ninety days or a year or two years or three years based off of your policy or whatever that type of information is, you need to ensure that that's configured appropriately and that the cloud service provider has a mechanism in place to allow you to do that.

Another concern is visibility. Cloud service providers may do a great job monitoring their own infrastructure, but they might now have those same controls and tools enabled, by default, in your environment. So, you really need to understand what is available, how to tune that to meet your monitoring needs.

Another important consideration is data sanitization. If you have a fileserver in your enterprise and it's being used to compute sensitive information or store sensitive information, you're not just going to throw that in the dumpster. You're going to go ahead and wipe that hard drive in a secure fashion or degauss it or do something to it, so you know for a fact that there's no evidence and no artifacts on that hard drive. Is your cloud service provider doing the same thing with any physical hard drives that it's removing from production? If you're dealing with your data that's encrypted, there's a couple of ways to help with this. If you don't have the keys to decrypt the data, you've built in a little bit of safeguarding for yourself. So, how are those keys managed? How are they destroyed, rotated etc.? So, this way even if something is not security

wiped, the data that resides on there is encrypted and is of no use to a criminal.

Incident response in the cloud is another concern mainly because you don't control that underlying infrastructure. You don't know, for certain, what the cloud service provider's process is for incident response, the whole identification, triage, remediation type of thing. If there's a compromise, does that mean a service or a system has to come offline, and, if so, how does that impact you? If there's a warrant or an investigation for another tenant that happens to be in your same computing environment physically, how does that impact the services that you are providing to your customers or your organization? So, having that assurance that it's not going to disrupt your service if something else happens is quite important, and then, of course, understanding their process and what controls and procedures they have in place to protect your business if an incident does occur. All of those things have to be considered.

And then there's a whole list of summary recommendations in here, which is a great asset where you can come to quickly and get recommendations based off of governance, compliance, trust, etc. Here's the rest of the categories for you.

We're going to skip ahead to another section here that we have something

valuable for you, and this is right here in the summary of this NIST Special Publication 800-144. It's really, really important for you to understand that the accountability for security and privacy in the public cloud deployment cannot be delegated to the cloud provider. It remains the obligation of the organization to fulfill. So, that means even though there is this shared responsibility model in terms of what the cloud s going to protect and what you need to protect like your data and your access and all that other good stuff, it's ultimately your responsibility, as the custodian of the data and the information, to ensure that all the controls are in place, and that either means by configuring them or by working with the cloud service provider to have them document the controls that they have in place and the other compliance things that they've done for or deemed their data center, etc., to make sure that everything has the best possible security in place, a good defense in depth strategy, etc.