Cloud Security Basics

Demo

Instructor: In this video
We're going to take a look at cybersecurity information documents from the National Security Agency. The first one is for Cloud Security Basics.

First page here, we just have some background information and introduction to the cloud, things like infrastructure as a service, platform as a service, et cetera, that we've already seen, but on the next couple pages we get into some of the details like shared responsibility model. Cloud services providers are responsible for physical security of the cloud, organizations are responsible for application-level security, and it is the organization's responsibility to configure their

services according to their security requirements. So just little bit of a foot stomp driving that home, which we've heard before.

Within the threat model, it's important to understand that the primary risks to cloud infrastructure are malicious adversary activity and unintentional configuration flaws. We'll see the configuration one pop up over and over again. The federal and DoD requirements. It's important to understand that the Federal Risk and Authorization Management Program or FedRAMP one, provides a standardized framework for assessing and authorizing cloud services. So within the federal government, the DoD, you do have to go through an authority to operate an authorization program, and includes a number of things. You know, evaluate against FedRAMP compliance at certain levels is just one of those. Doing a privacy impact assessment is another one.

As far as access controls go, we see here misconfigured access controls in major cloud storage providers have resulted in exposure of sensitive data. Again, that goes to what we've seen as a top threat in that misconfiguration of cloud resources.

Cloud patching is also a little bit tricky. Depends a little bit on your service provider and how you have things configured. Certainly, if you're leveraging infrastructure as a service you'll need to apply patches at the operating system level. Platform as a

service, you'll need to ensure your application updates are appropriate, and software as a service you might not have the ability to update any of those components.

Multitenancy is a consideration. A big point that's made here is that the service provider is responsible for implementing the necessary controls to keep your data and compute resources isolated. We won't touch upon encryption, because we're going to cover that a little bit more in the next NSA document and it kind of presents that in a better way, and then of course when it comes to utilization, you should take advantage of all of the cloud security services that are available and supplement them with your on-premise tools. So they might not do everything that you're looking for or you may already have an investment in various tools within your enterprise. You have to evaluate ways to extend either cloud to the enterprise or enterprise to the cloud to get a consistent and cohesive solution.

The last one on our list here with data spillage. Need to ensure that the cloud service provider only stores and manipulates data that they're accredited to handle. So that goes back to the FedRAMP level and other classification levels that you're using for your authority to operate it.

Let's take a look at our other document. This one goes into a little more depth for mitigating common vulnerabilities. We still have some of

the background information on cloud components. You see identity and access management abbreviated as IDAM. You might see it as IAM. It's essentially the same thing, and we also see here compute networking and storage, and this cloud encryption key management, I said we were going to talk about that a little bit more. Customers can take advantage of the cloud service provider's Key Management Services that are designed to integrate with their other cloud services, so that makes them easy to use. It helps with backups, recoveries, those types of things, but there's a little bit of a risk there because the cloud service provider would essentially have access to that. So there's the malicious insider or misuse on the key--on the service provider side.

There's also the advantage of being able to leverage the hardware security modules that might be integrated with the hardware platforms underlying in the cloud infrastructure, and the next one here is that the cloud service provider may have already gone through an accreditation process for their team management solutions, so if that process, that technology is available and it can be used in conjunction with you bringing your own keys, that might be worth investigating as well.

So there is another comment in here that I've highlighted, Keeping encryption and key management outside the cloud ensures that

customer data is never exposed to cloud administrator. That kind of goes to the insider threat thing that I alluded to before. It also ensures that, you know, as they do destroy those drives, that the disks that might be supporting the storage of your data and your information, if that is encrypted and there's no key to unencrypt it, there is that extra level of protection.

So we also see the shared responsibility model detailed within this document and a little bit more on some typical threat actors. One of the things I want to point out here is three of these four, all in with administrator. So you're either looking at a rogue cloud administrator, a untrained or neglectful administrator within your organization, or, again, some malicious cloud administrator on your site as well. So it's really protecting those administrative services, which you want to do with multi-factor authentication and ensuring that they're properly trained and making sure that you have logging enabled and that you're monitoring for anomalous or suspicious activities and that you've configured these accounts with the least amount of privilege for what they need to do.

So those are the key pieces and they all really tie to administrators, and then of course there are bad guys out there, cyber criminals and nation-state actors, and they're going to leverage those weaknesses, but those weaknesses are usually in

architecture or using poor authentication, not using multi-factor authentication, leveraging those compromise credentials, et cetera, and, you know. So it really ties back to the poor administration that is going to lead to these cyber criminals potentially taking action.

So as we move on in the document we see some specific threats. Misconfiguration, for example, is highlighted. Prevalence is widespread and attacker sophistication is low, so this is a neat way to look at these threats. You know, it's really easy for a hacker to take advantage of an open-access control list or a weak password, that type of thing, and then it goes through and provides some examples of what happened there in the DoD space and what you can do to help protect that, and that really is leveraging encryption and access control lists, intrusion detection systems, web application firewalls, et cetera. Least privilege, which we mentioned, enabling defense-in-depth is important, whether it's the cloud or otherwise. You want to make sure you have layered defenses to either stop them at the gate or once they get in, to prevent pivoting, and just make it as difficult as possible.

Poor access control. Again, prevalence is widespread. It says Moderate here but it's not terribly difficult to take advantage of this. Some of it is, again, if you're not using multi-factor authentication you

can leverage some social engineering attacks to try to gain access to the system. You're also dealing with folks that are going to be scanning IP addresses for open remote administration ports, like an SSH or an RDP, right, and trying to access those with some group forcing techniques. So auditing for that type of activity, alerting on it. Maybe automatically configuring some deny rules within your firewalls. Those are some options.

Shared tenancy vulnerabilities are little more rare, and this is where we talk about if a hypervisor or another customer is compromised, it is possible for them to get access to the management plans and pivot to other customers. It's rare, it's difficult to do. Supply chain vulnerabilities, again, might be difficult to do, so it's a very sophisticated hacker that's going to pull that off. It doesn't happen often, but again, when you're dealing with that high level of trust at that lowest layer in the chips that you're integrating into your servers, into your hardware, into your graphics processors, whatever, You've got an assumed level of trust there, and so if your supply chain is somehow compromised and they're able to embed some code in there to tweak the encrypted cipher so they're not as strong as you think they are or maybe there's a backdoor key or maybe they're capturing information and sending to somewhere else, there's a number of ways that they can take advantage of that, and you have a couple of links to some

specific incidents and references here within the document.

And here on the last page, you have your conclusions from the NSA regarding cloud vulnerability and mitigation and several of the references that they use throughout four examples of those compromises. So pretty good document. It's a nice, short version of your best practices that you can review quickly and more easily and readily digest than the more comprehensive NIST guides and the Cloud Security Alliance guides.