Mini Project 17: Cloud Security Part 1

Mini-Project Overview

Time Estimate: 2 hours

Context: Read through this brief about cloud security from Attack Solutions, Inc., a provider of cybersecurity service, before proceeding to **Project Submission Steps**:

> Operating in the cloud undoubtedly delivers significant advantages and security improvements for most organizations…
>
> [However,] when scoping a move to the cloud, businesses need to assess security in the context of this environment and evaluate Cloud Service Providers (CSPs) accordingly. Moving to the cloud means adopting a partnership approach to security that requires high levels of trust and transparency between all parties. These should be established at the start of the relationship.
>
> Partnering with a CSP allows you to access the security expertise of a business whose success depends on providing the most advanced levels of protection. Cloud providers have economies of scale. This allows your

> company to invest far more into talent and adoption of the latest innovative infrastructure protection and defense technology than any single organization could commit financially.
>
> Due diligence around your CSP is important when entrusting core systems to a third party. Therefore, it is critical to take the time to work with them to ensure that your cloud instance is secure and well maintained.

(Tombs, G. (2020, October 31). *Why cloud security is more important than ever*. Attack Solutions. http://attacksolutions.com/why-cloud-security-is-more-important-than-ever/.)

Project Submission Steps

One of the major security concerns of cloud-based information assets is access control.

Read the scenario below and perform the required task.

Scenario

An insurance company has a claims application used to capture data about their policyholders and any property damage they suffer. A hurricane is projected to strike the Gulf Coast region of the US, likely causing massive property damage. This will create a huge spike in claims which will in turn create an enormous load on the corporate IT infrastructure. The company's decision is to use a public cloud provider to deliver virtual machines to handle the expected demand. The company must control access between the enterprise system and the virtual machines hosted by the cloud provider, limiting access to only authorized agents of the company. The company must securely transmit any data created by cloud-based instances of the application back inside the corporate firewall. The cloud provider must ensure that no traces of the application or its data remain whenever a virtual machine is shut down.

The insurance company is based in the U.S. and only has domestic offices (there are no operations outside of the U.S.). The company is using Microsoft Active Directory (AD) for authentication, with workstations running Windows 10. The claims systems are running Oracle Database 19c on Linux.

Assignment

Paper (2-4 Pages)

You have been tasked with implementing an access control solution based upon users' roles. Write a 2–4 page paper on how you would go about doing this assuming that the cloud environment is either Microsoft Azure or Amazon Web Services (AWS) (pick only one).

Your paper should include details on the following RBAC/access control features:

- Roles
- Secure remote access
- Policies
- Encryption
- Federation/Single Sign-on (SSO)
- Logging and monitoring
- Resource permissions

If you need additional guidance on how to conduct and use research in your paper, feel free to use Purdue University's Online Writing Lab to help you figure out where to begin, how to figure out what information you need, and how to synthesize and use resources. Knowing how to professionally integrate research into your solutions and proposals will help prepare you to build a reputation on-the-job as a cybersecurity professional who knows how to use their resources in their work.

Your paper should include details on the following RBAC/access control features:

- Roles
- Secure remote access
- Policies
- Encryption
- Federation/Single Sign-on (SSO)
- Logging and monitoring
- Resource permissions