InfoShield

AWS Cybersecurity Best Practices

November 12, 2018

AWS Security

Cloud computing has brought some amazing advantages to business. A lot of those large upfront investments aren't necessary, and deployment is moves nearly at the speed of 'click'. However there's still the security components that need to be managed. Infoshield offers a list you can use to make sure your systems are secure before putting your new product out there and finding someone getting in where you didn't intend.

AWS Security Checklist

by **Josh Susen, CISSP**

Run through this checklist when configuring your AWS Environment

❏ Protect the electronic keys linked to your root account like physical keys. Don’t leave them lying around for anyone to find!

❏ Use CloudTrail to audit AWS account activities. Track who’s making changes to the AWS system.

❏ The bigger your organization, the more levels of restricted access should be setup with the IT administrators of AWS.

❏ Use encrypted EBS volumes with AES-256 bit.

❏ Restrict network traffic to all EC2 instances with security groups. This is just like firewall management. Only allow what’s necessary!

❏ S3 buckets should not be public.

❏ Enforce S3 bucket encryption as appropriate.

❏ Use secure ports when accessing S3 endpoints (HTTPS, SFTP).

❏ Setup S3 versioning and lifecycle policies.

- ❏ Use S3 logging for necessary auditing.
- ❏ Configure patch management on your EC2 instances

If you need more help or would like a second set of eyes we're available to help.

Get more help from us

Other Resources and Further Reading

https://aws.amazon.com/whitepapers/

Infoshield is an IT Security Consulting Company

Fernandina Beach, FL