Security Review of Web infrastructure on AWS

A company, which will remain nameless, had delegated the management of its web presence to a managed service provider (MSP). That MSP had both designed he website as well as managed web hosting through the customer's AWS account. Unfortunately, the MSP had not provided any documentation, and the day finally came when the MSP went out of business.

The company needed a survey of their AWS infrastructure both to document their web assets and to understand how they were being served to the public. They requested MTech to conduct that survey and provide their findings.

Survey and Recommendations

Stage 1

We performed an immediate survey of the various services used within the AWS account. Even before access to the internal account was made available, we were able to ascertain from the public DNS records that AWS Route53 was hosting the company's DNS domain and that AWS CloudFront was fronting the web content.

After access was granted to MTech by the company, an internal inspection of the CloudFront distribution revealed that it was serving content from a mixture of AWS origins. That was all simple enough on the surface.

However, additional inspection revealed a medley of other S3 buckets (some of which were publicly accessible), security groups, and residual access credentials. Discussions with the company clarified that the medley of assets were from years of development of the website: prior versions, abandoned development efforts, and abandoned deployment pipelines that relied on undocumented network holes, an unknown Administrator user, and a long-lived access keys providing full Administrator access to the company's entire AWS account!

We strongly recommended (a) an immediate disabling of the holes in the networking firewall, (b) removing public access to the archival S3 buckets, (c) disabling of the unknown super-user's access and access key. The company agreed and we immediately deployed the security mitigations.

During a period of observation by both the company and MTech, we validated that the company's website was still fully functional and served quickly from access around the world.

Stage 2

We made further recommendations to remove the disabled credentials and security groups from Stage 1. The company agreed, and the recommendations were implemented.

Another validation by the company and MTech confirmed that the web presence remained fully functional and responsive throughout the security operation.

At the conclusion, the company director noted, “[MTech] did a great job. Excellent to work with, and an outstanding communicator!"

Get in touch for assistance with reviewing your company's cybersecurity posture.