Cloud Computing - Individual

Dave E. Craciunescu

2019.05.24

Módulo de Seguridad

AWS o (Amazon Web Services) es el gran competidor de Microsoft Azure. Dentro de este apartado analizaremos los servicios análogos a aquellos que Microsoft Azure nos ofrecía. Cabe mencionar que dentro del módulo de Educación que AWS ha proporcionado a los diferentes estudiantes de la clase de Ampliación Avanzada de la UAH, estos no han dispuesto de prácticamente ningún tipo de autorización a la hora de realizar acciones o emplear servicios, por tanto las herramientas no han sido probadas de primera mano. Cualquier explicación que se encuentre más abajo se basa puramente en la documentación oficial de los mismos servicios.

Amazon Cognito

Amazon Cognito es una herramienta de Amazon Web Services que permite la creación de aplicaciones cada vez más seguras. El servicio proporciona *pools* de usuarios en los que la autenticación de estos mismos se realiza automáticamente mediante Amazon Cognito. De esta manera, no hay que reisntalar la arquitectura y servicios de autenticación cada vez que se quiera implementar un login seguro para una aplicación o cualquie tipo de herramienta que implique la identificación real de los usuarios.

Gracias a Amazon Cognito, se puede automatizar todo el servicio de autenticación y hacer tanto el guardado de los hashes de las contraseñas, como el proceso mismo de introducción de credenciales de manera segura extremadamente simple. Además, se puede customizar la interfaz gráfica de usuario para que estos mismos tengan una experiencia mucho más común y placentera.

En cuanto a este servicio respecta, su paralelo en Azure se encontraría dentro del servicio de autenticación de Microsoft mismo, que se emplea extensivamente en Azure Active Directory. En AWS, este mismo se puede exteriorizar y automatizar de manera muy simple, además, el coste *real* de la herramienta es considerablemente más adecuado. Por estos mismos motivos se considera que este servicio sea el superior en cuanto a las dos nubes.

AWS Secrets Manager

En Microsoft Azure comentamos la implementación, el uso, y las características de Key Vault. El servicio análogo a este en AWS se llama *AWS Secret Manager*. Este tiene prácticamente las mismas características que el mencionado con anterioridad, dado que son, a efectos prácticos, la misma herramienta.

AWS Secret Manager ayuda a los usuarios a proteger secretos o información privilegiada importante para las aplicaciones, servicios y recursos IT. El servicio permite una muy simple manera de rotar y administrar credenciales de bases de datos, por ejemplo, en base a sus APIs altamente documentadas y bien diseñadas.

Una característica extremadamente importante de AWS que no se ha encontrado en Azure Key Vault es la autogeneración del código necesario para la obtención de una clave en concreto en múltiples lenguajes. Esto es un gran punto a favor para AWS, dado que la herramienta no va a ser siempre usada en los frameworks estándar en los que se encuentra.

Con esto comentado, aunque las características sean parecidas y AWS tenga la autogeneración de código para diferentes lenguajes. Se considera el servicio de Azure Key Vault superior por la gran simplicidad que este conlleva y el hecho de que el mismo está integrado con el gran abanico de aplicaciones que es el framework de Microsoft.

AWS Security Hub

El Security Hub de Amazon es la versión de AWS del Security Center. Esta herramienta proporciona una vista simple y fácil de comprender de las prioridades de alto nivel y las alertas de seguridad de los diferentes servicios de AWS. En ella se encuentra un array enorme de herramientas de seguridad para el usuario, desde firewalls y protección de punto a punto a escáner de cumplimiento y vulnerabilidades. Se podría decir que la herramienta es prácticamente una navaja suiza de la seguridad empresarial.

Además, en la misma se encuentra un gran sistema de notificaciones y resúmenes de actividad diarios, junto con la creación automática de informes sobre vulnerabilidades muy detallados y con información pertinente. Todo esto se presenta en un dashboard fácil de entender y desde el cual no solo se puede visualizar la información sino también accionar sobre ella.

Según la mayoría de las métricas, el servicio de AWS Security Hub parece mucho más avanzado que su rival de Azure. Desde la integración con Amazon GuardDuty, Amazon Inspector y Amazon Macie hasta el hecho de la autogeneración de diferentes informes basados en características definidas por el propio usuario o administrador de seguridad del sistema. Sin dudarlo, el manager de seguridad de Amazon es mucho más detallado y avanzado en su funcionalidad.

AWS Shield

En último lugar, se encuentra Amazon Shield. Este servicio es una herramienta de protección contra ataque DDoS que salvaguarda aplicaciones que se están ejecutando en el AWS. De la misma manera que su rivan el Azure, AWS Shield proporciona mitigación contra ataques automática que minimizan el *downtime* de los servicios y la latencia que experimentan los usuarios.

Al analizar las características de las dos herramientas estas son tan similares que no sería descabellado decir que las compañías copiaron ideas las unas de las otras. Desde los informes de ataques y en análisis en tiempo real, los dos niveles de protección, el hecho de que no haga falta ningún tipo de intervención humana, etc.

Una característica que sí se encuentra en AWS Shield y que Azure no parece tener es la capacidad de crear layers por encima de los definidos por el propio software. Con AWS Shield *Advance* el administrador es capaz de escoger los recursos *específicamente* para proteger la infraestructura. Con esto se pueden crear reglas de protección altamente sofisticadas que mitiguen hasta el mejor diseñado ataque DDoS. Además, estas reglas pueden empezar a ser ejecutadas de manera inmediata, lo que hace el *blue-teaming* mucho más fácil y la protección de los servicios un juego de niños.