Casos de éxito

1. El cliente

Atio Cloud Services ofrece servicios de protección y recuperación de información a un grupo importante de consorcios gasolineros, los cuales están distribuidos a nivel nacional, dicho servicio está enfocado en la protección de datos volumétricos de cada estación, información de facturación (pdf y xml), entre otros datos importantes. Teniendo en cuenta que gran porcentaje de las estaciones puede operar 24 horas 7 días de la semana los 365 días del año, lo cual genera la necesidad de tener protegido los datos de una manera importante para dar continuidad de operación de cada estación.

Atio Cloud Services cuenta con una herramienta para ofrecer este servicio de protección de datos llamada Commvault; esta solución implementada cuenta con una arquitectura que consiste en una instancia en la nube y conexión a contenedores para el almacenamiento de datos, detrás de ello se tienen configuraciones de firewall, control de accesos, configuraciones de puertos, etc. donde dicha instancia funciona como intermediario para realizar los respaldos de las base de datos y archivos hacia almacenamiento en la nube, la cual viaja por la WAN de una manera segura, y rápida, contando además con funcionalidades de deduplicación, compresión y encriptación de los datos.

SC Empresarial apoya a Atio Cloud Services, a través de una póliza de servicio administrado y mesa de soporte que incluye administrar, gestionar y mejorar esta arquitectura robusta de solución, con lo cual se garantiza la oferta de servicio a los clientes finales de Atio Cloud Services.

2. Problemática

¿Qué problema o desafío enfrentó el cliente que requirió la ayuda externa del socio?

El ransomware es un código malicioso diseñado por ciberdelincuentes para obtener acceso no autorizado a sistemas y datos, con ello encriptar esos datos para bloquear acceso por usuarios legítimos. Una vez que el ransomware ha bloqueado a los usuarios sus sistemas y encriptaron sus datos confidenciales, los ciberdelincuentes demandan un rescate antes de proporcionar una clave de descifrado para desbloquear el sistema. En teoría, si el rescate se paga dentro del el tiempo asignado, los sistemas y los datos se descifran y se ponen a disposición nuevamente, recuperando operaciones normales. Sin embargo, si el rescate no es satisfecho, las organizaciones corren el riesgo de destrucción permanente o fugas de datos públicos controladas por el atacante.

Uno de los clientes finales de Atio Group presentó la problemática del cifrado de su servidor de aplicaciones por virus y se requirió el levantamiento urgente de los servicios afectados en menos de 24 horas. En ese momento no contaban con una estrategia de recuperación ante un desastre o emergencia, razón por la cual buscaron soluciones enfocadas en dos sentidos:

Casos de éxito

- Acciones preventivas, la protección hacia estos ataques, donde la prioridad es establecer configuraciones dentro de su arquitectura para la protección del ambiente que se encarga de administrar los datos de los clientes de Atio Cloud Services.

- Acciones correctivas, contar con el ambiente disponible para atender las demandas de recuperación de cada cliente por algún ataque presentado en cualquier momento.

3. Solución y arquitectura propuestas

¿Qué servicios de AWS se usaron como parte de la solución?

Para el servidor virtual se utilizó el servicio de EC2, que son instancias en la nube con el fin de tener el ambiente siempre disponible y de acceso desde cualquier lugar, cumpliendo con las medidas de seguridad. Se ha configurado una instancia robusta para garantizar eficiencia en el servicio.

En el servidor virtual se realizó la instalación de la aplicación de Commvault para el respaldo de la información. Se utilizó la IP Pública del servidor virtual y se ligó a un DNS para que los equipos desde cualquier lugar tengan comunicación con la herramienta y realicen los respaldos programados.

El segundo servicio utilizado es almacenamiento en buckets de S3 que permiten alojar cualquier tipo de información en la nube y siempre disponible para su descargar cuando se necesite.

A través del Commserve Server de Commvault se configuraron las librerías hacia buckets de S3 para que la información respalda se almacene en la nube. Así que cuando un equipo se respalda pasa primero por el servidor virtual (Commserve Server).

Se realizaron configuraciones adicionales como:

Segmento de nubes privadas virtuales de Amazon (VPC de Amazon). La segmentación de la red mitiga la congestión del tráfico local y también mejora la seguridad al asignar solo los recursos específicos para el usuario, lo que disminuye significativamente las formas en que los atacantes pueden moverse lateralmente dentro de la red.

Puede aprovisionar secciones lógicamente aisladas de la nube de AWS donde puede iniciar recursos de AWS en las redes virtuales que defina.

Segmentación de VPC de Amazon en componentes aislados, ya sea por grupos de seguridad y listas de control de acceso a la red (ACL) para que solo el tráfico necesario está disponible puede reducir la capacidad de propagación del ransomware indiscriminadamente en todos los entornos de AWS.

Establecer políticas sólidas de IAM que determinen qué sistemas y datos están disponibles para usuarios individuales o grupos de usuarios, y bajo qué condiciones en que los datos son accesibles, pueden limitar la amplitud del ransomware capaz de acceder al medio ambiente.

A nivel de usuario, AWS le permite definir un control de acceso detallado definiendo qué usuarios o roles tienen acceso a ciertos sistemas y datos. Estos controles determinan qué acciones pueden ser realizadas en un recurso dado en AWS, permitiendo a los usuarios con privilegios en una base de

Casos de éxito

"necesidad de saber" basada en las necesidades del negocio y las responsabilidades laborales.

AWS IAM le permite administrar el acceso a los servicios y recursos de AWS de forma segura. Con IAM, puede crear y administrar usuarios y grupos de AWS, y permisos de uso para permitir y denegar su acceso a los recursos de AWS. Tomando en consideración las mejores prácticas, AWS recomienda seguir el principio de mínimos privilegios para usuarios de redes internas y externas. Por ejemplo, algunas cepas de ransomware están diseñadas para usar una cuenta administradora del sistema para realizar sus operaciones. Con este tipo de ransomware, disminuyendo los privilegios de la cuenta de usuario y terminando todo el sistema predeterminado las cuentas de administrador pueden crear un obstáculo de seguridad adicional.

Las copias de seguridad son críticas para mitigar el impacto que puede tener el ransomware en su organización. El elemento disuasorio más eficaz para el ransomware es hacer copias de seguridad de forma regular y luego verificar sus sistemas. Al definir su estrategia de copia de seguridad y recuperación de datos, ayuda a proteger contra la eliminación o destrucción de datos durante un ataque de ransomware al estar preparado hacer que los datos almacenados en una copia de seguridad estén disponibles en ambientes de producción.

Las vulnerabilidades sin parches son una de las formas más comunes que el ransomware infecta el entorno de una organización. Identificando rápidamente y reparando vulnerabilidades, las organizaciones pueden reducir su exposición a amenazas de ransomware al limitar las formas en que puede entrar.

Con Amazon Inspector, puede buscar entornos de AWS para vulnerabilidades y exposiciones comunes, evalúe sus instancias con respecto a los puntos de referencia de seguridad y automatice completamente notificando a los ingenieros de seguridad y TI cuando los hallazgos están presentes. Una vez Se han identificado las vulnerabilidades, parcheando herramientas como AWS Systems Manager Patch Manager puede ayudarlo a implementar operaciones sistema y parches de software automáticamente en grandes grupos de instancias para cerrar exposiciones.

AWS Shield; AWS proporciona AWS Shield Standard y AWS Shield Advanced para protección contra ataques DDoS. AWS Shield Standard se incluye automáticamente sin costo adicional más allá de lo que ya paga por AWS WAF y sus otros servicios de AWS. Para mayor protección contra ataques DDoS, AWS ofrece AWS Shield Advanced. AWS Shield Advanced proporciona protección ampliada contra ataques DDoS para sus instancias Amazon Elastic Compute Cloud, equilibradores de carga Elastic Load Balancing, distribuciones Amazon CloudFront, zonas alojadas Amazon Route 53 y sus aceleradores AWS Global Accelerator.

SC EMPRESARIAL®

4. Resultados de la solución

4.-Resultados de la solución: / entrega de servicios de AWS y cómo el proyecto benefició al cliente:

Casos de éxito

La migración de las operaciones de respaldo a AWS es atendiendo una estrategia para la continuidad de las operaciones al tener una plataforma de ágil despliegue disponible en todo momento, con una seguridad adicional que permite evitar ataques a esta plataforma de vital importancia en el modelo de negocio para Atio Cloud Services, con una reducción de costos al no tener infraestructura propia en sitio.

Resultados vistos por el cliente:

"*Los servicios fueron reestablecidos en corto tiempo, AWS demostró ser una plataforma ágil para considerarla como una solución de continuidad operativa.*"

"Crecimiento de recursos ágil de manera horizontal y vertical, lo cual ayuda a la continuidad operativa del servicio, como consecuencia ayudará a más de 2,000 estaciones a dar continuidad operativa por el servicio que se despliega en esta arquitectura."

-Alfonso Mendez, Gerente de operaciones y TI.

Datos del cliente

Empresa: Atio Cloud Services

Nombre del cliente (quien da la referencia): Alfonso Méndez

Cargo: Gerente de operaciones y TI

Correo: amendez@atio.com.mx