Habilitar la protección de Denegación de servicio distribuido (DDoS)

Un ataque por denegación de servicio (DoS) es un ataque que tiene el objetivo de impedir el acceso a servicios o sistemas. Si el ataque se origina desde una ubicación, se denomina DoS. Si el ataque se origina en varias redes y sistemas, se denomina DDoS (denegación de servicio distribuido).

Antes de aprender más sobre DDoS, debe saber qué son las redes de robots (botnets), que son colecciones de sistemas conectados a Internet que un individuo controla y usa sin el conocimiento de sus propietarios. Los propietarios de redes de robots (botnets) las utilizan para diversas acciones que decidan realizar.

A menudo, las usan para el envío de spam, el almacenamiento de datos, DDoS o varias otras acciones que dependen de la persona que controla la red de robots (botnets). En el pasado, las redes de robots (botnets) estaban conformadas solo de equipos en peligro, pero ahora también incluyen dispositivos de Internet de las cosas (IoT). Los hackers malintencionados pueden tomar el control de este tipo de dispositivos con una seguridad deficiente, como cámaras de seguridad, grabadoras de vídeo digitales, termostatos y otros dispositivos conectados a Internet.

Por lo tanto, DDoS es una colección de tipos de ataque destinados a interrumpir la disponibilidad de un destino. Estos ataques implican un esfuerzo coordinado que usa varios sistemas conectados a Internet para iniciar muchas solicitudes de red en DNS, servicios web, correo electrónico y mucho más. Prácticamente cualquier aplicación a la que el hacker malintencionado pueda acceder podría convertirse en el destino de un DDoS. El objetivo del hacker malintencionado es sobrecargar los recursos del sistema de los servidores de destino para que ya no puedan procesar tráfico legítimo, lo que hace que el sistema sea inaccesible.

Por lo general, un DDoS implica muchos sistemas que envían tráfico a destinos como parte de una red de robots (botnet). En la mayoría de los casos, los propietarios de los sistemas de una red de bots (botnet) no saben que sus dispositivos están en peligro y forman parte de un ataque. Las redes de bots (botnets) son cada vez más un problema mayor debido al creciente número de dispositivos conectados.

Diseñar y compilar para la resistencia frente a DDoS requiere planear y diseñar para una serie de modos de error. En la tabla siguiente se enumeran los procedimientos recomendados para crear servicios resistentes a DDoS en Azure.

Procedimiento recomendado 1

Asegúrese de que **la seguridad es una prioridad a lo largo de todo el ciclo de vida de una aplicación**, desde el diseño y la implementación a las operaciones. Las aplicaciones pueden tener errores que permitan que un volumen relativamente bajo de solicitudes use una gran cantidad de recursos, lo que da lugar a una interrupción del servicio.

Solución 1

A fin de proteger un servicio que se ejecuta en Azure, comprenda la arquitectura de la aplicación y céntrese en los **cinco pilares de calidad del software**. Son las siguientes:

Pilar

Descripción

Escalabilidad

La capacidad que tiene un sistema para controlar el aumento de la carga

Disponibilidad

La proporción de tiempo en que un sistema es funcional y está en funcionamiento

Resistencia

La capacidad que tiene un sistema de recuperarse de los errores y seguir funcionando

Administración

Procesos de operaciones que mantienen un sistema en ejecución en el entorno de producción

Seguridad

Protección de aplicaciones y datos frente a amenazas

Debe conocer los volúmenes de tráfico típicos, el modelo de conectividad entre la aplicación y otras aplicaciones, y los puntos de conexión del servicio expuestos a la red pública de Internet.

Resulta fundamental garantizar que una aplicación es lo suficientemente resistente como para controlar un DoS destinado a la aplicación misma. Las características de seguridad y privacidad se integran en la plataforma Azure, empezando por Ciclo de vida de desarrollo de seguridad (SDL) de Microsoft. El SDL aborda la seguridad en cada fase de desarrollo y se asegura de que Azure se actualice continuamente para que sea aún más seguro. Examinaremos SDL más adelante en este curso.

Procedimiento recomendado 2

Diseñe las aplicaciones para que escalen horizontalmente a fin de satisfacer las demandas de una carga amplificada; en concreto, en caso de un DDoS. Si la aplicación depende de una única instancia de un servicio, crea un único punto de error. El aprovisionamiento de varias instancias hace que el sistema sea más resistente y más escalable.

Solución 2

Para Azure App Service, seleccione un Plan de App Service que ofrezca varias instancias.
Para Azure Cloud Services, configure cada uno de los roles para utilizar varias instancias.
Para Azure Virtual Machines, asegúrese de que la arquitectura de la máquina virtual incluye más de una máquina virtual y de que cada máquina virtual está incluida en un conjunto de disponibilidad. Se recomienda usar conjuntos de escalado de máquinas virtuales para contar con funcionalidades de escalado automático.

Procedimiento recomendado 3

Implemente defensas de seguridad en capas en una aplicación para reducir la posibilidad de que se complete correctamente un ataque. Implemente diseños con seguridad mejorada para las aplicaciones mediante las funcionalidades integradas de la plataforma Azure.

Solución 3

Tenga en cuenta que el riesgo de ataque aumenta con el tamaño, o el área expuesta, de la aplicación. Para reducir el área expuesta, utilice listas de direcciones IP permitidas para cerrar el espacio de direcciones IP expuesto y los puertos de escucha que no son necesarios en los equilibradores de carga (para Azure Load Balancer y Azure Application Gateway).

También puede usar grupos de seguridad de red para reducir la superficie del ataque. Puede usar etiquetas de servicio y grupos de seguridad de aplicaciones como una extensión natural de la estructura de una aplicación a fin de minimizar la complejidad para crear reglas de seguridad y configurar la seguridad de red.
