Retos de seguridad de los centros de datos

Vamos a ver los retos de seguridad de los centros de datos en esta ocasión. Los datos son el activo central de una organización digital. La seguridad de los datos está relacionada con el funcionamiento diario de la organización, afecta las decisiones comerciales de esta, interfiere con la producción y la prestación de servicios de la Corporación, e incluso afecta la competitividad y la supervivencia de la empresa.

El centro de datos aloja de forma centralizada todos los servicios importantes de datos y aplicaciones de la organización, por lo que la seguridad del centro de datos es muy importante para la Compañía.

Riesgos

En la actualidad, los centros de datos se enfrentan principalmente a los siguientes riesgos de seguridad:

1. En los sistemas relacionados con la infraestructura de la información y de datos, los atacantes internos y externos pueden explotar las vulnerabilidades del software y de configuración, etc. para atacar, destruyendo la disponibilidad de la infraestructura, los sistemas y los datos.
2. Los atacantes internos y externos acceden ilegalmente a los activos de datos y los roban al explotar las vulnerabilidades del sistema de aplicaciones y las configuraciones frágiles.
3. Los usuarios ilegales utilizan el acceso no autorizado a

los activos de datos mediante el robo de credenciales y otros medios, lo que resulta en la fuga de datos confidenciales y de privacidad.

4. En el proceso de desarrollo y mantenimiento de aplicaciones, operación y mantenimiento de datos, así como mantenimiento del sistema de infraestructura, a menudo se producen daños maliciosos a los sistemas, aplicaciones y datos debido a la mala operación del personal y los impulsos emocionales, e incluso conduce directamente a la interrupción del negocio.

Consejos para reforzar la seguridad del centro de datos

1. Construya un área de acceso seguro

Cree un área de acceso seguro, centralice los portales de acceso del centro de datos y aísle lógicamente a todos los usuarios y aplicaciones que acceden al data center.

2. Protección de fronteras

- Control de acceso sobre el tráfico entrante y saliente en el límite del área de acceso de seguridad, y solo permite el tráfico de acceso a servicios abiertos al mundo exterior;
- La detección y protección contra intrusos en la red se realizan en los límites internos y externos del área de acceso, y la detección de amenazas y la inspección de fuga de datos se realizan en todo el tráfico de acceso;
- Acceder a los dispositivos para el descubrimiento, y realizar regularmente escaneos de vulnerabilidad del dispositivo y verificaciones de la línea de base de configuración para los dispositivos descubiertos.

3. Protección de dominio de acceso de usuario

En el dominio de acceso del usuario, el proxy de acceso oculta los servicios de aplicaciones reales, agrega el acceso de todos los usuarios, aplica la política de autenticación de usuarios, verifica la identidad del terminal y la información de seguridad ambiental, y realiza la autenticación de acceso a nivel de aplicación para los usuarios.

Al mismo tiempo, instala el software de protección de seguridad para los servidores de aplicaciones en el dominio de acceso del usuario, realiza el escaneo de vulnerabilidades y la administración de parches, verifica la configuración de vulnerabilidades en los servicios y sistemas de aplicaciones, realiza el refuerzo de la configuración, la detección y eliminación de virus.

Recopila comportamientos del sistema, analiza y confirma amenazas desconocidas y realiza verificaciones de políticas en el control de acceso a la red del host.

4. Protección de dominio de acceso a aplicaciones

Realiza la autenticación de identidad y la inspección del entorno de seguridad en las aplicaciones que acceden al centro de datos y proporciona capacidades de acceso a datos para aplicaciones externas.

5. Protección de seguridad del centro de datos

En el límite de acceso al centro de datos, se realizan aplicaciones internas o subdominios de datos, control de acceso al tráfico, detección de amenazas de red y detección de fuga de datos; en el límite del subdominio de datos, se

realizan control de acceso y auditoría de acceso para operaciones de acceso a datos.

Al mismo tiempo, la solución también puede proporcionar autenticación de identidad y autorización y autenticación unificadas para todas las entidades que acceden al centro de datos y, a través de la capacidad de percepción del entorno del terminal, recibir la información del estado del entorno del terminal y el servidor, implementar políticas de seguridad empresarial para controlar equipos de servicio, y agregar todos los procesos de acceso, información de riesgo y ajustar los derechos de acceso de los usuarios de manera oportuna.

6. Gestión de privilegios

Unifique los derechos de gestión y operación de dispositivos de red, hosts de servidores, bases de datos, middleware y sistemas de aplicaciones en el centro de datos y el área de acceso de seguridad, realice autenticación centralizada y autorización refinada, perciba y confirme operaciones peligrosas y audite todos los comportamientos de operación.

Conclusión: Retos de seguridad de los centros de datos

Los centros de datos proporcionan una gran cantidad de aplicaciones, servicios y soluciones para muchas empresas, y los recursos de estos, son cada vez más importantes para las empresas. Con la proliferación de dispositivos inteligentes, algunas aplicaciones de IoT y basadas en la nube también aumentan rápidamente los riesgos de seguridad del centro de datos.

Co
mo
un
a

función muy crítica, el centro de datos también desempeña un papel cada vez más

importante en el funcionamiento de la empresa. Debido a esto, el centro de datos suel

e
se
r
má
s
vu
ln
er
ab
le
a
lo
s
at
aq
ue
s.

La importancia de la seguridad para los data centers es evidente, especialmente hoy en día, cuando las personas prestan más atención a la seguridad de la información, los incidentes de seguridad no son un asunto trivial. Una vez que ocurre un problema grave de seguridad en un centro de datos, la pérdida para este, es inconmensurable.

La seguridad del data center está centrada en los datos, del acceso, uso, destrucción, modificación, pérdida, fuga y otras dimensiones de los datos, por lo que también se derivan muchos métodos técnicos. Desde el software hasta el hardware, desde el perímetro de la red hasta el núcleo, desde la entrada hasta la salida del centro de datos, los dispositivos de seguridad se pueden implementar dondequiera que haya datos. Se implementan muchos dispositivos de seguridad del centro de datos, pero aún son atacados constantemente. ¿Por qué?

De hecho, la seguridad del centro de datos es un proyecto sistemático, no solo mediante la implementación de algunos firewalls. El centro de datos es directamente responsable de

las tareas de agregación de datos, integración de recursos con los mismos, prestación de servicios de datos y mantenimiento del funcionamiento de toda la red.

Es la base para el funcionamiento seguro de diversas actividades de la red.

Es necesario llevar a cabo un diseño de esquema de seguridad detallado, de modo que el esquema de seguridad penetre en cada enlace del centro de datos, para garantizar la seguridad de los datos del centro de datos.

A nivel de aplicación, virus, gusanos, troyanos, puertas traseras y bombas lógicas, etc., a los ojos de unas pocas personas con segundas intenciones, todo tipo de datos clave almacenados en el centro de datos son invaluables, impulsados por intereses económicos u otros específicos. Para estos fines, estas personas utilizan varios medios para atacar el data center o intentar penetrar en las instalaciones y realizar varios accesos no autorizados y operaciones ilegales en los datos clave del mismo.

Como resultado, los datos clave del centro de datos pueden ser monitoreados, robados, falsificados y manipulados, los servidores puede funcionar con lentitud, el rendimiento se degradará o colapsará y el servicio de datos no se podrá proporcionar al mundo exterior, e incluso el el hardware se dañará, lo que provocará grandes pérdidas. Por lo tanto, la operación segura del centro de datos es de suma importancia.

En HostDime estamos orgullosos de nuestro Data center Nebula, que cumple todas estas exigencias de seguridad, siempre pensando en sus usuarios.

Leer también: Protección contra incendios en un Data center; Nuevos sistemas de refrigeración en Data centers; Gerente de data center, administrador, funciones