Niveles de seguridad física de un Data Center

El tema propuesto en nuestro blog de HostDime para esta oportunidad son los niveles de seguridad física de un data center. Se trata de un tema sensible y de suma importancia para quienes estamos en la industria de los centros de datos, tanto clientes como proveedores.

Inicialmente vamos a hacer un resumen teórico de los protocolos más usados y, posteriormente mostraremos las capas, los anillos de seguridad implementados en Nebula, el data center de HostDime en Colombia.

¿Cuántas capas son?

Personalmente esperaba encontrarme con una respuesta definitiva y por el contrario, halle distintas respuestas. Hay quien habla de 8, otros expertos mencionan 6 e inclusive hay voces divergentes mencionando 5.

Estándares de seguridad física del centro de datos

Ubicación

La evaluación de la seguridad del centro de datos comienza con la ubicación. El diseño de un centro de datos de confianza tendrá en cuenta:

- Actividad geológica en la zona
- Industrias de alto riesgo en la región
- Cualquier riesgo de inundación
- Otros riesgos de fuerza mayor

Puede evitar algunos de los riesgos enumerados anteriormente colocando barreras o redundancia adicional en el diseño físico. Estos eventos tendrán un impacto en el funcionamiento del centro de datos debido a los efectos nocivos y es mejor evitarlos por completo.

Edificios, estructuras y sistemas de soporte de centros de datos

El diseño estructural que conforma el centro de datos debe mitigar cualquier riesgo de control de acceso. La cerca alrededor del perímetro, el grosor y el material de las paredes del edificio, y el número de entradas al mismo. Todo esto puede afectar la seguridad del centro de datos.

Algunos factores clave también incluyen:

- Los gabinetes del servidor están equipados con cerraduras.
- Los edificios requieren más de un proveedor de servicios de telecomunicaciones y electricidad.
- Los sistemas de respaldo de energía adicionales, como UPS y generadores, son una infraestructura crítica.
- Usar autenticación. Esto implica colocar una esclusa de aire entre dos puertas separadas, las cuales deben estar certificadas

Control de acceso físico

Controlar el movimiento de visitantes y empleados alrededor del centro de datos es fundamental. Si tiene escáneres biométricos en todas las puertas, y registra quién tiene acceso a qué y cuándo, esto ayudará a investigar futuras infracciones. Las rutas de escape y evacuación de incendios solo deben permitir que las personas abandonen el edificio. No

debe haber manijas exteriores para evitar el reingreso. Abrir cualquier puerta de seguridad debería hacer sonar una alarma.

Asegure todos los puntos finales

Cualquier dispositivo, ya sea un servidor , una tableta, un teléfono inteligente o una computadora portátil conectada a la red de un centro de datos , es un punto final. Los centros de datos brindan espacio en bastidores y gabinetes para clientes cuyos estándares de seguridad pueden ser inciertos. Si los clientes no protegen adecuadamente sus servidores, todo el centro de datos puede estar en riesgo. Los atacantes intentarán explotar dispositivos inseguros conectados a Internet.

Por ejemplo, la mayoría de los clientes desean acceso remoto a las unidades de distribución de energía (PDU) para poder reiniciar los servidores de forma remota. En este caso de uso, la seguridad es una preocupación importante. Los proveedores de instalaciones deben comprender y proteger todos los dispositivos conectados a Internet.

Mantenga registros de entrada y video

Todos los registros, incluidas las imágenes de videovigilancia y los registros de entrada, deben conservarse durante al menos tres meses. Algunas vulnerabilidades se identifican cuando es demasiado tarde, pero el registro ayuda a identificar sistemas vulnerables y puntos de entrada.

Ver también: Retos de seguridad de los centros de datos, Multicloud: cómo reducir la superficie de exposición a los riesgos de ciberseguridad, La extinción de incendios en un centro de datos.