Cinco Consideraciones Básicas para Prevenir Ataques al Servidor para Siempre

CHATSWORTH PRODUCTS

Las empresas globales experimentaron un cambio radical en el 2020, ya que muchas tuvieron que pasar a tener a su personal trabajando de forma remota y distribuida con rapidez y sin mucha preparación. En el segmento de la ciberseguridad, los ciberatacantes vieron estas circunstancias como oportunidades.

No es sorprendente que, además de un aumento general en los ataques de ransomware, phishing y malware, el acceso al servidor fue el tercer tipo de ataque más común en el 2020, según el X-Force Threat Intelligence Index 2021 de IBM, un informe anual publicado por la sección de seguridad de IBM. El informe define un ataque al servidor como un "actor amenaza que obtiene acceso no autorizado al servidor de una víctima, ya sea mediante la explotación de credenciales robadas del servidor, la explotación de una vulnerabilidad u otros medios".

En una realidad en la que los datos se han convertido en el activo más valioso del mundo, la privacidad y la administración ética de los datos deben ser una prioridad máxima para las organizaciones y los centros de datos, en especial en momentos en que el trabajo remoto se está convirtiendo en la norma y no en la excepción.

Chatsworth Products (CPI), un experto en soluciones inteligentes de administración de energía e infraestructura de tecnología de la información y las comunicaciones (ICT, por sus siglas en inglés), recomienda que los centros de datos incluyan una medida sólida de sistema de control de acceso como parte de su marco integral de ciberseguridad.

Aunque las normas y reglamentos de la privacidad de datos requieren medidas de control de acceso físico para el equipo de procesamiento y almacenamiento de datos, depende de cada organización decidir qué método específico de tecnología utilizar.

En general, el cumplimiento de los reglamentos requiere un método para:

Asegurar de manera física el equipo de procesamiento y almacenamiento de datos.

Identificar y administrar accesos autorizados.

Administrar el acceso al espacio físicamente seguro.

Mantener registros de acceso al espacio físicamente seguro.

Cinco Consideraciones Básicas al Construir un Sistema de Control de Acceso

Seguridad Física: Primera Línea de Defensa

Para un sitio de un solo inquilino propiedad de una empresa, la seguridad a nivel de sala podría considerarse suficiente. Sobre todo en los centros de datos de múltiples inquilinos (MTDC, por sus siglas en inglés), también conocidos como instalaciones de colocación, y en sitios remotos, el control del acceso físico a nivel de gabinete simplifica la administración y evita que los usuarios no autorizados accedan a los servidores y switches en los que se almacenan los datos.

Las cerraduras electrónicas y los sistemas de control de acceso automatizan el monitoreo, la documentación y el control del acceso y permiten una rápida reprogramación si cambian los derechos de acceso o si se pierde o roban una credencial.

Administración de Claves y Derechos

Cuando se utilizan cerraduras con clave para asegurar los gabinetes de equipos, las empresas deben tener un programa de administración de claves sólido y eficaz. Independientemente de cómo estén codificados los gabinetes, se requiere un sistema sólido para documentar el acceso.

Por el contrario, el bloqueo electrónico se puede reprogramar rápidamente con nuevos códigos de acceso y no es necesario modificar el hardware. Cada usuario puede tener diferentes derechos, y la configuración de derechos en el software documenta en simultáneo los códigos de acceso asignados (claves).

Registro de Informes y Auditoría

Hacer que los usuarios se registren en el acceso controlado en la entrada del edificio garantiza que haya un registro documentado de la presencia de la persona en el edificio, pero no su acceso a los gabinetes individuales.

Los sistemas de bloqueo electrónico y control de acceso automatizan el registro de acceso a nivel de gabinete y permiten informes automatizados por usuario o gabinete. Esto acelera la preparación para una auditoría y ayuda a reducir el alcance de las investigaciones de eventos.

Respuesta al Evento

Cuando se produce una filtración de datos, la respuesta inmediata al evento es fundamental. Con un sistema de cerradura con clave, los equipos de TI deben verificar manualmente el estado de las puertas y cerraduras. Si una clave se pierde o es robada, deben volver a poner una clave en la cerradura.

Los sistemas de bloqueo electrónico y control de acceso simplifican, acortan y, en algunos casos, automatizan estas respuestas. Además, estos sistemas permiten a los equipos de TI administrar de forma remota los intentos de acceso y el estado de la puerta, desde una interfaz de software.

Jurisdicción: ¿TI o Administración de Instalaciones?

En la mayoría de las instalaciones de centros de datos, la seguridad se implementa a través de una plataforma del sistema de administración de edificios, poseída y administrada por la administración de instalaciones. Cuando se trata de gabinetes y sistemas de centros de datos, la seguridad suele estar controlada por TI, que monitorea la protección de datos y la seguridad de los equipos.

Estas consideraciones y capacidades antes descritas son un buen lugar para comenzar, pero hay otros elementos importantes que, cuando se combinan, crean un ecosistema de gabinetes inteligente totalmente preparado para el futuro. Para obtener más información, vea el video en chatsworth.com/data-centers.

CHATSWORTH PRODUCTS