Transición a una solución corporativa en control de accesos

Cómo evitar escollos y problemas

Decidir la migración de un control singular a un sistema unificado de control de accesos conlleva una gran responsabilidad y requiere de amplios conocimientos. Informarse sobre la solución a implementar y hacerlo con las personas adecuadas es clave para una concreción exitosa.

Ricardo Pulido, *Gerente Regional de Ventas para el Norte de América Latina y el Caribe de Tyco Security Products.*

Un sistema corporativo puede significar cosas distintas para diferentes personas. En este caso, concebimos un sistema corporativo como aquel que mantiene un control centralizado sobre toda una solución de control de acceso, al tiempo que cada sede controla, de forma independiente, sus respectivas operaciones. La solidez de un sistema de este tipo brinda a los administradores del sistema de la sede principal, la posibilidad de configurar, administrar y monitorear todas las ubicaciones desde dicha ubicación. También les permite monitorear simultáneamente alarmas de varias instalaciones desde una estación de trabajo que les resulte conveniente. Ya sea que su organización esté compuesta por unas cuantas sedes, ubicadas en diferentes puntos de una región, o que cuente con muchas instalaciones distribuidas por todo el mundo, una solución corporativa se adapta al crecimiento de su compañía.

El factor más importante que debe considerarse al empezar a planificar la transición a una solución de control de acceso corporativa es la preparación. Para ello, debe saber de qué recursos dispone, quiénes serán las figuras principales que le ayudarán en este proceso y cómo desarrollar un plan sólido para poner a funcionar el sistema adecuadamente. Al migrar a un sistema corporativo, hay una serie de aspectos del proceso que son importantes y deben considerarse.

La migración a un sistema corporativo de control de accesos permite, entre otros puntos, revisar y limpiar bases de datos obsoletas, evaluar y corregir viejos procedimientos e implementar cambios y mejoras en los controles.

DEFINIR EL PARADIGMA OPERATIVO

Las organizaciones suelen experimentar tropiezos porque no definen el paradigma operativo. Para ponerlo en términos más simples: no se ocupan de los procesos administrativos, la generación de reportes y el monitoreo ni las experiencias de control. No han logrado tener una visión panorámica del proceso. Al pasarse a una solución corporativa, un gran número de funciones, reportes y procesos van a ser agregados a su solución de seguridad y es conveniente asegurarse de invertir el tiempo necesario para redistribuir la organización de este flujo de trabajo.

La transición a un sistema corporativo, brinda la oportunidad de revisar y limpiar las bases de datos, evaluar sus viejos modelos, procedimientos y sus antiguas tecnologías y ver dónde puede implementar mejoras o cambios. El momento perfecto para definir los puntos críticos es al principio del proceso, no al final. Con frecuencia, este proceso le proporciona al propietario del sistema la oportunidad de examinar y depurar su base de datos, la cual, muy probablemente, durante años habrá sido gestionada por diferentes personas y grupos.

Las siguientes son algunas de las preguntas que es necesario formular: ¿qué reportes existentes le pueden seguir siendo de utilidad y qué nuevos va a requerir? ¿Qué debe ser actualizado? Dado el número cada vez mayor de funciones del monitoreo de alarmas, ¿cómo las incorporará en su flujo de trabajo y asociarlo a la medición de gestión?

Un proceso administrativo igualmente importante es reevaluar su nomenclatura. ¿Su nomenclatura actual funcionará en todo el sistema corporativo o es necesario hacer modificaciones?. Asegúrese de tener una nomenclatura que funcione para todo el sistema corporativo, teniendo en cuenta cómo ésta afectará a diferentes grupos, entre ellos procesos como la administración, la generación de reportes, el monitoreo y las integraciones. Con un sistema corporativo, ahora deberá monitorear varios edificios, cada uno de los cuales tiene su propia puerta principal. ¿Cómo va a diferenciar una puerta de otra en su nueva nomenclatura, teniendo en consideración la importancia de tener todo esto organizado antes de iniciar la transición?.

También es fundamental optimizar la generación de reportes antes de empezar este tipo de proyecto. Actualmente su organización tiene información sobre

personas, lugares, políticas e ideas en varias ubicaciones. ¿Qué parte de estos datos va a conservar? y ¿Cómo van a convivir en el nuevo sistema unificado?

Un elemento importante es adoptar una solución avanzada de generación de informes, diseñada para recolectar y organizar adecuadamente la información de su empresa. Este tipo de herramientas le ayudarán a transformar la inteligencia empresarial en inteligencia de seguridad mediante interfaces intuitivas en línea, que le permiten examinar la información sin necesidad de imprimir ni revisar copias en papel.

FIJAR EXPECTATIVAS

El segundo gran paso para hacer una transición exitosa, es definir las expectativas en términos de desempeño y de escalabilidad.

Entender el volumen que está planeando procesar en su empresa le permite definir adecuadamente la arquitectura global del sistema. Después de todo, todos los sistemas tienen sus límites o conllevan costos adicionales potencialmente innecesarios, de modo que el análisis adecuado de la actividad de entrada, ya sea el monitor de estado de las puertas o la solicitud de tráfico de salida, le será de utilidad en este proceso.

COORDINAR LAS DISTINTAS PARTES IMPLICADAS

En la mayoría de los casos, la transición a un sistema corporativo implicará la coordinación entre varias partes (departamentos, sedes y distribuidores). Es fundamental comunicarse claramente con todos los grupos internos y externos involucrados, incluyendo los principales integradores y el departamento de TI, entre otros.

Conformar un buen equipo de trabajo es otra de las claves para una transición exitosa hacia un control de accesos corporativo. Hay que conocer quién lo diseñará, quién lo llevará a cabo y quién estará a cargo del mantenimiento.

Se solicitará a los integradores instalar las distintas aplicaciones, que van desde soluciones para la industria de seguridad y de protección contra incendios hasta soluciones CCTV, para el control de intrusos y la gestión de visitantes. Su equipo de TI puede encargarse de la transición a un entorno virtual y de supervisar estas necesidades durante el proceso.

Otro elemento que es necesario tener en cuenta, es el empleo de un equipo de mantenimiento adicional para que antes de la transición lleve a cabo una auditoria de todos sus sistemas actuales, a fin de determinar entradas o salidas inadecuadas o cualquier otro error en el sistema, como posibles problemas en su base de datos.

Esta auditoria puede identificar información oculta, no registrada en el diario, equipos dañados, credenciales que pueden no haber sido transferidas de un sistema a otro y otros reportes relacionados con el mantenimiento. Dicha auditoría sacará a la luz errores en el sistema actual, que pueden corregirse antes de la transición. Cuando se ocupa la migración de bases de datos, siempre es aconsejable que se comisione el proceso al integrador certificado y que éste presente un plan avalado por el fabricante o desarrollador de los nuevos sistemas, indicando claramente el alcance y limitaciones del proceso, si las hubiere.

CONFORMAR UN EQUIPO

Como dijimos, el éxito de una transición radica en tener un plan. Y tener un plan consiste básicamente en conformar un equipo. Decida quiénes harán parte de él, quiénes diseñarán el plan para migrar los datos desde sus sistemas de control de acceso actuales hasta la solución corporativa y quiénes harán mantenimiento del sistema y los datos una vez estén en funcionamiento.

Lo ideal sería que el equipo estuviera conformado por personas de recursos humanos, operaciones de seguridad, TI y gestión de servidores. Una vez conformado el equipo, defina quién será el responsable de cada tarea. Esta información debe quedar claramente documentada en una programación, en la cual se definen también los resultados esperados de cada miembro del equipo. Dichos resultados incluirán requisitos de importación y exportación, requisitos de reportes y los propietarios de datos.

Hacer esto le permitirá determinar cualquier problema que pueda surgir, el cual podrá ser almacenado de forma separada hasta que sea identificado y se implemente una solución importada para manejar adecuadamente la actualización del personal y las credenciales.

PREPARARSE PARA LO DESCONOCIDO

El último aspecto que debe considerarse es estar preparado para lo inesperado. No es fácil, por supuesto, pero es fundamental si el resultado deseado es una transición exitosa. Al entender plenamente el sistema y todo lo que lo rodea, usted está mejor preparado para afrontar posibles problemas. Para ello es aconsejable conocer los firewalls, la protección contra virus, el software malicioso, las copias de respaldo, las fuentes de datos, las políticas de gestión de escritorio, las políticas de actualización y asuntos similares. En el tema económico, aprender los costos anuales de licencias, servicios de soporte y actualización. Con frecuencia, ya están cubiertos en los primeros 12 meses de operación, pero se pasa por alto para el segundo año en adelante. Asegúrese de contratar este servicio de soporte anual, es la decisión costo-efectiva que le dará mayor tranquilidad a su operación.

La auditoría previa de todos los equipos le ayudará a determinar una parte de esto. Así que implemente un plan y sepa con anticipación qué detalles desea incluir.

Hacer la transición a una solución corporativa de control de acceso es un gran paso. Con requerimientos tan complejos, hay muchos aspectos que es fundamental tener en cuenta. Asegúrese de preparar todos los pasos del proceso, conozca sus recursos y el personal clave, y desarrolle un plan sólido. Si invierte el tiempo necesario y se prepara de forma adecuada, éste puede ser un proceso exitoso y sin contratiempos. ■