Manuel Sampedro,
VOCAL DE LA COMISIÓN DE SEGURIDAD AUTELSI. DIRECTOR DE SERVICIOS Y SOLUCIONES DE SEGURIDAD DE UNISYS EN ESPAÑA

El quinto dominio

En la última década se han realizado inversiones masivas para asegurar que los usuarios no pueden acceder, operar o modificar datos sin los permisos adecuados. Comunicaciones cifradas, firma digital, firewalls, IDS/IPS y otra miríada de elementos han sido desplegados con esta aproximación; y complementado con otros orientados a cubrir los riesgos de fallos del sw y hw.

Aunque este enfoque cubre un amplio abanico de riesgos, los atributos clave de seguridad de la información (confidencialidad, integridad y disponibilidad) pueden verse afectados por amenazas y vulnerabilidades que provengan tanto del mundo lógico como del físico. La ISO 27002, estándar de facto en seguridad de la información, reconoce este hecho al incluir en su quinto dominio a la "Seguridad física y del entorno".

Los Centros de Proceso de Datos se han convertido en las estrellas de la infraestructura de IT, al soportar todas las aplicaciones y datos de misión crítica, pero ¿son suficientemente seguros? Algunas cuestiones deben ser resueltas:

• ¿Quién accede y cuándo? ¿La identificación corresponde a la persona autorizada? ¿Y si un usuario con permisos no puede acceder? ¿Es posible acceder por puntos no autorizados?

• ¿Qué acciones se realizan dentro? ¿Qué ocurre si se realizan acciones no autorizadas?

• ¿Proporcionan los sistemas de disponibilidad tradicionales (incendios, SAIs, aire acondicionado) información agregada o dispersa en diferentes herramientas?

• Si se dispone de varios CPDs dispersos geográficamente, ¿es posible conocer su estado de seguridad en tiempo real?

• ¿Se puede identificar un incidente / riesgo inminente en tiempo real? ¿La información registrada es suficiente para un análisis forense y determinar responsabilidades?

La aproximación correcta a la seguridad física de los CPDs debe contemplar todos los vectores de riesgo con un enfoque de negocio y, para ello, una solución tecnológica de Gestión de Seguridad Física de CPDs debería:

• Cubrir uno o múltiples CPDs mediante una consola de Comando y Control Unificada que proporcionara a los responsables de seguridad información visual del estado de seguridad en tiempo real mediante indicadores y mapas sinópticos de las instalaciones.

• Posibilitar a los administradores la asignación de permisos de acceso con las mismas herramientas utilizadas para asignarlos a recursos digitales, siguiendo las mejores prácticas de convergencia de seguridad lógico-física.

• Proporcionar a los operadores una experiencia de usuario orientada a los "procesos de seguridad", no a las tecnologías usadas, permitiéndoles interactuar de forma homogénea con los dispositivos desplegados (lectores, cámaras, sensores, interfonos, etc.) con independencia de su naturaleza.

• Asegurar que los usuarios son quien dicen ser, evitando los intercambios de credenciales.

Existe una necesidad derivada de un riesgo, en muchas ocasiones no correctamente percibido o no ponderado adecuadamente, y no hay mayor peligro que la falsa sensación de seguridad. ✦