



Numero 119 - 10 de Mayo 2004

Centros de Operaciones de Seguridad (COS); oportunidad para la industria TIC y beneficios para usuarios

- ✓ **El concepto de COS un concepto con mas de 20 años en el mercado pero poco conocido**
- ✓ **La determinación de vulnerabilidades y el establecimiento de medidas para mejorar la comunicación entre usuario y prestador de servicios es prioritario**
- ✓ **La determinación de vulnerabilidades y el establecimiento de medidas para mejorar la comunicación entre usuario y prestador de servicios es prioritario**

Las organizaciones que usan tecnologías de información y comunicaciones (TIC) enfrentan diversos problemas en materia de seguridad y deben incrementar su nivel de alerta y medidas para el acceso a su información. Algunas empresas están conscientes de esta necesidad, y por ello han empezado a utilizar servicios administrados de seguridad, y otras incluso ya están haciendo uso de las facilidades de un Centro de Operaciones de Seguridad (COS), también conocido como SOC por las siglas en ingles de Security Operations Center.

"En una investigación reciente de Select, sobresale el hecho de que muchas organizaciones usuarias de TIC se han percatado de sus carencias de personal especializado en aspectos de seguridad, y de su insuficiente infraestructura tecnológica para administrar políticas y explotar bitácoras de dispositivos, aplicar metodologías y herramientas de análisis o administración e implementar correcciones de fallas de seguridad", menciona Saul Cruz Pantoja director ejecutivo.

¿Es el COS un concepto nuevo en Mexico?

Un Centro de Operaciones de Seguridad (COS) permite emplear remotamente los servicios que ofrecen empresas especializadas en seguridad, haciendo disponible un conjunto de recursos informáticos y servicios con énfasis en la seguridad, para garantizar el control y supervisión de dispositivos, ruteadores, firewalls, aplicaciones de antivirus, entre otras, que operan en la red del usuario.

"Select identifico COS en México con operaciones desde 1999, por lo que este concepto no es nuevo, pero si desconocido por muchos. De una muestra de proveedores de servicios de seguridad, dos terceras partes indicaron contar con un COS. En algunos casos el COS es empleado conjuntamente para ofrecer otros servicios externalizados de seguridad, ya sea para propósitos internos o para clientes de sus centros de datos, pero no para la prestación de servicios abiertos a terceros. Es evidente que aun falta FOCO en seguridad, ya que algunas empresas que disponen de un COS, prestan otros servicios de TIC en el mercado

mexicano, sin posicionarse como especialistas en servicios de seguridad", señaló Saul Cruz



Un COS significa "Cúmulo de Oportunidades en Servicios"

"Los servicios prestados con mayor frecuencia a traves de su COS son el análisis de vulnerabilidades, puesta a punto de elementos por administrar, definición de reglas de seguridad, VPNs, capacitación inicial al personal del usuario como contraparte del prestador de servicios, pruebas regulares de comportamiento del sistema, monitoreo de disponibilidad, utilización, ataques y respuesta a incidentes, generación y explotación de bitácoras, soporte técnico en materia de seguridad, notificación a terceros y optimización del sistema. Para beneficio de los usuarios, los servicios deben iniciar con la determinación de vulnerabilidades, incluyendo medidas para que exista una comunicación adecuada entre el usuario y el prestador de servicios y se debe contemplar la optimización de los servicios prestados", agregó Saul Cruz

Las actividades de seguridad están adquiriendo gran importancia debido al posible impacto de los accesos no autorizados a redes, presencia de virus y fallas naturales en diversos componentes electrónicos, entre otros factores. Es previsible que los presupuestos de seguridad para los próximos años se incrementen sensiblemente, especialmente entre grandes organizaciones, tanto del sector publico como del privado. Para muchas empresas, especialmente aquellas que se preocupan por revisar sus sistemas de seguridad, los servicios administrados pueden ser una solución a sus problemas, apoyándose en la experiencia de prestadores de servicios con diversas especialidades, contratando desde el diagnostico de vulnerabilidades hasta los servicios de recuperación en caso de desastres. Un COS puede ser una solución muy conveniente para las organizaciones que usan TIC, pero debe entenderse solamente con un auxiliar, sin descuidar los niveles de servicio adecuados para sus usuarios de TIC. Aunque algunos COS que existen en México ya pueden habar de casos de éxito, en general aun se esta construyendo la experiencia en México en la operación de estas facilidades.

"Los servicios administrados de seguridad tienen una concepción reciente, pero ya existe oferta de estos servicios en México y es predecible el incremento considerable de la

demanda, por lo tanto, los prestadores de estos servicios deben elevar el nivel de profesionalización de su personal asignado a aspectos de seguridad, entre otros aspectos mediante las certificaciones técnicas procedentes. Por otra parte, es necesario que los usuarios de TIC desarrollen una cultura de seguridad en TIC dentro de toda la organización en forma integral, incluyendo a las diversas unidades de informática y a los usuarios finales. Un análisis inicial de vulnerabilidades es imperativo para implementar adecuadamente actividades de seguridad, y sola así deben asignarse recursos para abordar operativamente el problema. Además, se debe invertir en capacitar al personal en conceptos relativos al COS y evaluar las posibilidades a futuro de una operación potencialmente conjunta entre la organización y el prestador de servicios. También es cierto, que dadas las diversas interpretaciones del concepto de un COS, las organizaciones usuarias deben validar apropiadamente los recursos que les ofrezcan los prestadores de servicios, seleccionando preferentemente soluciones certificadas", concluyo el director ejecutivo de Select.

La información de este boletín proviene del estudio *Centros de Seguridad Administrada*, con la colaboración de Saul Cruz Pantoja Director Ejecutivo

Si desea adquirir este estudio, por favor escribáenos a ruth.guzman@select.com.mx

**** Se han retirado acentos y caracteres especiales para facilitar la lectura en cualquier aplicación de correo electrónico. No se trata de faltas de ortografía ****

Director General: Ricardo Zermeno Gonzalez * Director Ejecutivo: Saul Cruz Pantoja * Coordinadora de Mercadotecnia y de Edición: Ruth Guzman Ramirez, con la colaboración de: **Saul Cruz Pantoja** * Producción: Antelmo Vanegas Sandoval

Select, Estrategia Local con Enfoque Global

Disenado para 1024 x 768

Todos los derechos reservados. D.R. © Servicios de Estrategia en Electronica, S.A. de C.V.

Numero de registro:

Prohibida su reproducción total o parcial, por cualquier medio o forma, sin la autorización expresa y por escrito de su titular.

[Terminos de uso y políticas de privacidad](#)

Esta página cuenta con protección legal integral, llevada a cabo por nuestro representante legal, [Rios, Aparicio & Asociados, S.C.](#)