



EL ENFOQUE DE LA GESTIÓN DE LA SEGURIDAD EN UN CONTEXTO INTERNACIONAL

Las nuevas oportunidades de negocio han llevado a muchas empresas a la diversificación de sus actividades que, en muchos casos, ha provocado un proceso de internacionalización con el fin de disponer de nuevos mercados que favorezcan su crecimiento. De esta internacionalización nacen nuevos escenarios de relación entre empresas, clientes, proveedores, instituciones y en general, cualquier entidad imputable a los nuevos procesos de negocio.

Desde el punto de vista de la seguridad de la información esto supone la aparición de nuevos contextos caracterizados por la heterogeneidad de sus componentes, tanto en el plano conceptual como en el de implantación. Aparecen nuevos

que no han iniciado todavía la integración, o están en fase de hacerlo.

Nos encontramos pues, en un escenario global donde es necesario ir de la mano de un proveedor de servicios de red que disponga de la cobertura necesaria de su red pública para hacer una distribución estratégica por regiones. Cada región deberá disponer de una cabecera o nodo principal al que se conectarán las distintas sedes que dependan de esa región a través de proveedores locales. Todos estos nodos conectan con los Sistemas de Información Centrales. Estos nodos son centros de *colocation* provisionados generalmente por un operador local, donde implantamos nuestros

adecuándose a cada sistema vigente. Como siempre, es más que recomendable ir de la mano de ISO 2700x para abordar los distintos proyectos de seguridad y actuar especialmente en aquellos contextos que precisen de una normativa específica.

El Centro de Operaciones de Seguridad (SOC) es el punto neurálgico donde se gestionan entre otras, las tareas de monitorización y respuesta ante incidentes, por lo que es necesario extender su ámbito a los nodos regionales. Es importante, además de un SOC nacional, tener uno o más SOC a nivel internacional. La externalización del servicio de SOC puede ser una buena alternativa y la empresa que lo presta debería tener cobertura internacional propia o a través de terceros.

En determinadas situaciones se hará uso de Internet como red pública global como en el caso de las Extranets o acceso VPN. Con todo esto, una solución de NAC nos permitirá disponer de controles que validen la integridad del puesto y en el caso de no cumplimiento se lance un proceso de "remediación". Existen un conjunto de tecnologías que permiten alcanzar niveles de seguridad en conformidad con nuestra política, pero la idea es que los accesos seguros a los sistemas de información no requieran de soluciones intrusivas.

En este sentido, el acceso a los sistemas de información a través de un portal corporativo cobra fuerza. La tecnología web permite mínimas exigencias en un modelo arquitectónico cliente-servidor y está al alcance de cualquier usuario allá donde se encuentre. Es una forma cómoda y rápida de desplegar aplicaciones o entornos de trabajo que, complementados con soluciones de NAC y VPN, pueden ofrecer los niveles de seguridad que necesitamos.

Conclusión

La internacionalización trae consigo la aparición de nuevos y desconocidos escenarios de actuación pero esto nunca debe implicar una transformación traumática en nuestra organización en todos los niveles de IT y en concreto en la Seguridad.

Si hemos trabajado bien en la estrategia de centralización y potenciación de la infraestructura de comunicaciones global, se conseguirá la escalabilidad necesaria y nuestro SGSI se adecuará a la nueva situación sin apenas esfuerzo. ■

El acceso a los sistemas de información a través de un portal corporativo cobra fuerza. La tecnología web permite mínimas exigencias en un modelo arquitectónico cliente-servidor, está al alcance de cualquier usuario allá donde se encuentre y es una forma cómoda y rápida de desplegar aplicaciones o entornos de trabajo que, complementados con soluciones de NAC y VPN, pueden ofrecer los niveles de seguridad que necesitamos.

retos que se materializarán en nuevos proyectos y la manera de abordarlos depende, en gran medida, del grado de madurez que poseemos en relación a la gestión de la seguridad.

En este punto es importante determinar el "estado de salud" de los sistemas de información de que disponemos. El haber llevado a cabo procesos de consolidación y concentración de dichos sistemas de información es estratégicamente recomendable para disponer de un entorno centralizado que va a favorecer la capilaridad, esto es, el poder difundir, sin apenas esfuerzo, aquellos controles que alimentan nuestro SGSI allá donde las comunicaciones lo permitan.

Un factor a tener en cuenta es lo relativo a la externalización de la gestión de la seguridad. El hecho de delegar determinadas funciones de seguridad en empresas que cuentan con la cobertura internacional y el nivel de especialización necesario, incrementa el grado de madurez, nos proporciona cobertura para ejecutar los planes acordados y nos permite más disponibilidad para elaborar estrategias que busquen la alineación con el negocio.

Infraestructura global de comunicaciones

Nos hemos referido a la capilaridad, para la cual es necesario disponer de una determinada topología de red que la permita. Un entorno centralizado es una gran solución para irradiar la seguridad y llegar al nivel necesario en la gestión del riesgo, mas aún cuando al otro lado nos vamos a encontrar, muy probablemente, con empresas de reciente adquisición, fruto de la expansión,

recursos que son gestionados íntegramente por nosotros, y serán punto de presencia tanto de los distintos operadores locales como del operador global.

Esta idea persigue varias cosas:

- Mantener la autonomía de las sedes locales para que desarrollen su actividad, y nos permita ofrecerles el uso de los sistemas de información centrales con el grado de seguridad necesario para favorecer su integración dentro del ámbito corporativo.

- Permitirnos disponer de la visibilidad necesaria para la monitorización y análisis mediante el despliegue de los distintos controles que se integrarán en el S.I.E.M. corporativo para dar respuestas adecuadas a posibles situaciones anómalas.

- La posibilidad de ofrecer servicios de redes convergentes así como Internet a toda la región desde un mismo punto, minimizando los costes y la gestión.

- Disponer de un punto común para gestionar aspectos de seguridad, priorización y calidad de los flujos de tráfico.

Gestión de la seguridad

Las distintas relaciones de la Empresa con el exterior (clientes, instituciones, etc.) están sujetas a la jurisprudencia aplicable en cada región y no siempre es la misma ("*common law*", "*civil law*", "*musulman law*", etc.), por lo que parece necesario proveer a nuestro SGSI de herramientas que verifiquen el cumplimiento, la regulación y la legalidad de nuestras actividades en el normal proceso de negocio,



Andrés Antón Abeledo
Responsable de Seguridad
Departamento de
Comunicaciones
GRUPO FERROVIAL