



CRISIS "SOBRE RUEDAS"

No corren buenos tiempos para el sector de la automoción. No importa que seas grande o pequeño, no importa que el sector emplee alrededor de un 10% de la población activa o aporte un 5% al PIB del país. Con más de un 30% de descenso en las ventas, el sector pasa por un periodo complicado, difícil de asumir en cualquier cuenta de resultados. Las dificultades pasan factura a todos los fabricantes y proveedores y afecta al final a todas las iniciativas de las compañías. No iba a ser menos en los departamentos de sistemas y seguridad informática de dichas organizaciones. Desde el punto de vista de la seguridad

—decantarse por la autenticación fuerte—, pero podemos dar por bueno el mecanismo ancestral de la contraseña si aceptamos sus limitaciones. Existen otras casuísticas encima de la mesa en época de crisis. ¿Elijo un software de cifrado bajo licencia o decido dar soporte y ofrecer similares funcionalidades con un software de libre disposición? Desde luego que ambas alternativas tienen sus pros y sus contras, y no será aquí donde se realice dicho estudio. Debido a que la seguridad informática interviene en todas las áreas dentro de los sistemas de información, podemos encontrar planteamientos similares

des pérdidas si estos caen en malas manos. Lamentablemente no se percibe como una prioridad, ya que es francamente complejo cuantificar esas hipotéticas pérdidas. Ocorre algo similar con servicios de consultoría llamados de valor añadido, inversiones en infraestructura para evitar posibles interrupciones de servicio, desarrollos con dudosos ahorros aunque aporten nuevas funcionalidades y así, un largo etcétera.

"Reduce" y vencerás

Hoy en día, más que nunca, se busca la reducción en los costes de servicio continuado, ya sea en infraestructuras, aplicaciones o servicios (internalizados o no) críticos para el negocio. Atrás quedan por el momento las funcionalidades extra del departamento IT. Al menos, por el momento.

Esta estrategia exclusivamente enfocada a la reducción de costes del día a día hace que proyectos diferenciadores e innovadores se queden en el cajón por un tiempo. La tendencia está ahora únicamente en consolidar, migrar del proveedor A al B porque B ofrece un descuento sobre A (con posiblemente alguna mejora de servicio) e implantar nuevos sistemas que supongan un ahorro directo en recursos del negocio (entiéndase en el amplio sentido de la palabra).

Lo que nos espera

Sin duda alguna, la estrangulación en futuros proyectos venideros en el sector automoción hará que volvamos a la casuística de los años 80, donde cualquier nueva implantación IT tenía una vida útil de más de 10 años, o incluso hasta 15. Tendremos que volver a acostumbrarnos a tener soportes específicos y caros sobre activos anticuados y con limitaciones funcionales.

Veremos en el año 2015 cómo funciona nuestro sistema de consolidación de logs, nuestra reciente implantación ERP o la virtualización de nuestros servidores. Es aquí donde tenemos que estar preparados, ya que será imprescindible una cabeza responsable capaz de gestionar todos los riesgos y retos que se nos vienen encima. Desde luego nuevas oportunidades y limitaciones para los responsables informáticos y sus proveedores de servicios. ■

La estrangulación en futuros proyectos venideros en el sector automoción hará que volvamos a la casuística de los años 80, donde cualquier nueva implantación IT tenía una vida útil de más de 10 años, o incluso hasta 15. Tendremos que volver a acostumbrarnos a tener soportes específicos y caros sobre activos anticuados y con limitaciones funcionales.

informática debemos preparar una estrategia para afrontar los meses venideros, donde se incrementarán las amenazas informáticas y escasearán los recursos.

Riesgo y seguridad

Explicado el contexto al que nos circunscribimos, y teniendo en cuenta que raramente los directivos aprecian el valor añadido de la seguridad informática, es cuando se nos plantea el primer axioma de los días en que vivimos: "Seguridad sí, pero sólo la que podamos pagar".

Lamentablemente este dicho no llega a cumplirse del todo, momento en el que interviene el segundo principio: "¿Qué riesgo estás dispuesto a aceptar?". De aquí concluimos una de las principales tendencias de las compañías en estos días, que no es más que la de analizar el riesgo.

Estas funciones permiten a las empresas llegar a relajar sus necesidades de seguridad informática, siempre que se conozcan realmente las dificultades que se puedan presentar. Para ello, es imprescindible disponer de medidas que mitiguen ese riesgo, y maneras para poder cuantificarlo. Ejemplos que el sector afronta son numerosos. Por citar alguna muestra, el famoso dilema de autenticación fuerte (mediante token o certificado) versus el archiconocido usuario y contraseña. ¿Implanto ahora el tan deseable y seguro sistema de autenticación de doble factor o confío en una cadena de caracteres?

Como Responsable en Seguridad Informática la respuesta puede resultar obvia

a los anteriormente descritos en diversos ámbitos, como si utilizamos redes públicas o redes privadas, o incluso infraestructura compartida o dedicada.

Sin rentabilidad económica, no hay proyecto

Otro de los pilares imprescindibles en estos días de dificultades, además de la gestión de riesgos, es la rentabilidad económica de todo proyecto. Cada día utilizamos más la relación entre beneficio e inversión en toda iniciativa, lo que se conoce en el mundo financiero como ROI (*Return of Investment*). Gartner postula que sobre el año 2012 no sólo se medirá el éxito del departamento IT utilizando dicho ratio, sino que habrá que tener en cuenta un nuevo parámetro, conocido como ROA (*Return on Assets*), que incluye el ciclo de vida y la depreciación que se hará sobre un activo determinado.

A pesar de esta acertada visión, a día de hoy exclusivamente se sigue utilizando en todo proyecto informático el indicador ROI, especialmente en los de seguridad IT. Es imperativo que el periodo de recuperación de la inversión sea lo más corto posible además de quedar descartadas de antemano propuestas con difícil justificación económica. Si retomamos ejemplos anteriores, siempre ha resultado complejo demostrar la viabilidad económica de cifrar todos los portátiles de una firma. Es cierto que si trabajamos con información secreta en nuestros dispositivos móviles, como prototipos de clientes o planes estratégicos, podemos llegar a atesorar gran-



Daniel Vallejo García
Responsable de Seguridad
y Riesgos TI para Europa
dvallejo@visteon.com
VISTEON CORPORATION