Autora: Lizzette Pérez Arbesú
lizette@netmedia.info

Cuando no se miden los riesgos

Es un hecho que no hay incidentes que se repitan de la misma forma ni afectan por igual a las empresas. Entonces, ¿cómo efectuar un análisis de riesgos en su organización?

De no ser por una práctica amigable de su competidor, los secretos de Coca-Cola habrían sido expuestos hace poco. De acuerdo con varios medios, tres personas (una de ellas, empleada de Coca-Cola Company), intentaron vender a Pepsi secretos industriales de la primera, incluyendo una muestra de una bebida nueva.

Pero no contaban con la honestidad de los ejecutivos de Pepsi, quienes mostraron a los directivos de la gaseosa de etiqueta roja, una carta, supuestamente escrita por un importante empleado de Coca, que prometía información detallada y confidencial a cambio de un millón y medio de dólares. "Nosotros hicimos lo que cualquier compañía responsable haría. La competencia puede ser feroz, pero también necesita ser limpia", dijo el vocero de Pepsi, Dave DeCecco.

Por su parte, Neville Isdell, jefe ejecutivo de Coca-Cola, agradeció a su competidora y se dirigió a sus empleados a través de un comunicado interno en el que establecía que todos tienen la responsabilidad de vigilar la protección de sus secretos comerciales. Seguramente se alegró de que solo hubiera sido un susto, una llamada de atención, y que los ingredientes de su fórmula se encuentren a salvo.

Sólo un susto, esta vez, pero ¿qué si no la cuenta? ¿Cuántas empresas hay que no corren con la misma suerte? Y es que a pesar de tener tecnología de punta, las compañías seguirán siendo vulnerables. Cuando no se filtra información vía telefónica, o en una conversación en un ascensor, se extraen archivos mediante dispositivos usb o simplemente se transfieren a un contacto del mensajero electrónico.

Nunca faltan, tampoco, los espías de la competencia, o empleados insatisfechos dispuestos a vender hasta su alma con tal de conseguir algún beneficio económico. Y qué decir de otros factores que afectan también la continuidad del negocio, como los que se explican en el artículo dedicado a la continuidad en esta misma edición.

El hecho es que no parece haber un flanco libre de huecos, y de hecho, así es. Como se puede apreciar en el recuadro *Elementos que disparan los riesgos*, el negocio de una empresa, así como sus sistemas de información, pueden ser vulnerables ante amenazas del mercado, financieras, operativas y de recursos humanos, entre otras.

Los objetos están más cerca de lo que parecen

El primer paso para efectuar un análisis de riesgos es entender la naturaleza misma de este proceso. De acuerdo con Gonzalo Espinosa, jefe de seguridad de la información en Cadbury Schweppes e instructor del módulo de análisis de riesgos en el diplomado de seguridad informática del Tec de Monterrey y la Asociación Latinoamericana de Profesionales en Seguridad Informática (ALAPSI),

el riesgo se puede definir como la probabilidad de que una amenaza aproveche una vulnerabilidad, o la ausencia de controles, para impactar al objeto de la información en cualquiera de sus tres características: integridad, confiabilidad o disponibilidad.

Ahora bien, no es posible eliminar por completo los riesgos en seguridad, pero "si los controles funcionan correctamente, la amenaza será contenida o mitigada", dijo Espinosa. En este sentido, un control se refiere a la solución específica para cada vulnerabilidad, ya sea que se trate de un marco de trabajo (como COSO, ITIL o Cobit), proceso, aplicación o tecnología, que ayude a las organizaciones a alcanzar sus objetivos y estrategias de negocio, evitando o minimizando los impactos. Los controles pueden ser preventivos, correctivos o de protección.

Así, el análisis de riesgos es el punto de inicio que debe cumplir cualquier procedimiento de administración de la seguridad de IT basado en estándares internacionales de seguridad, ya que deberán identificarse cuáles son las vulnerabilidades potenciales de seguridad de los procesos de la organización, para poder definir los planes de mitigación.

El análisis de riesgos permite identificar las amenazas que pueden poner en peligro a los activos de la organización determinando las vulnerabilidades del sistema ante estas amenazas así como estimando el impacto que tendría en la organización la materialización de las mismas. Por lo mismo, "este proceso debe realizarse por los ejecutivos del negocio, responsables de cada área, y no por el departamento de tecnología, que solo será un facilitador de los objetivos del negocio", de acuerdo con Espinosa.

Asimismo, son los responsables de cada área quienes pueden asignar adecuadamente un valor al nivel de la amenaza, ya sea baja (no hay riesgo de importancia, en valores financieros, imagen de la empresa o continuidad de los procesos), media (ataques conocidos en Internet pero que no tienen como objetivo a la compañía), o alta (ataques dirigidos y todos los riesgos que impliquen daño financiero, operativo o de imagen).

Una vulnerabilidad debe considerarse severa en cuanto a su impacto si permite a un atacante remoto violar la protección de seguridad de un sistema, o que tome control total del mismo.

De frente hasta topar con pared

Hasta aquí, todo pinta bien. El profesional de sistemas o el de seguridad de la información puede asistirse de metodologías ya probadas en la industria, así como de herramientas de gestión –como el Balance Scorecard– para evaluar, junto con un equipo de ejecutivos responsables del negocio, los riesgos a los que está expuesta la información y qué tipo de controles implementar.

Sin embargo, en la práctica no siempre hay finales felices. De acuerdo con Mario Farías Elinos, coordinador del grupo de investigación de la Escuela de Ingeniería de la Universidad La Salle, aún habrá que salir bien librados de la toma de decisiones. "Puede haber problemas cuando los responsables se inclinan por lo estético o convencional en vez de lo seguro o funcional", dijo. Por ejemplo, en la parte céntrica de la capital de México no se deben colocar sites de cómputo en una planta baja o sótano, debido a los riesgos de inundación, y aún así hay organizaciones que lo hacen.

Además, el mismo proceso de análisis de riesgos puede caer en alguno de diez errores comunes, a saber: dificultad excesiva para identificar amenazas, vulnerabilidades y sus consecuencias; un pobre entendimiento de las amenazas y sus capacidades; habituarse a una situación existente; ignorar las defensas exitosas; malinterpretar datos estadísticos; ignorar el problema del tiempo; subestimar la interdependencia y la complejidad del análisis; tener un enfoque netamente reactivo; generar una confianza excesiva al interior, o tener un foco inadecuado sobre los riesgos de negocio de alto nivel.

Reglamentos para escoger

Farías, quien se ha especializado en temas de seguridad como el análisis de riesgos, y ha estado involucrado en este tipo de procesos en La Salle, considera que en general los servicios de análisis de los consultores se centran sobre un foco en específico, y hay muchas metodologías distintas. Algunas cubren ciertos enfoques que otras no, y viceversa, de modo que la aplicación de los análisis queda a conciencia de los consultores o del líder de proyecto y puede haber algún hueco.

"La metodología que mejor se maneja es CMM (Capability Mature Model), pues no depende tanto de criterios individuales sino de abarcar las mejores prácticas", opinó. Añadió que lo más importante en estos procesos es tener una visión completa, tanto del área de tecnología en relación al negocio, como de la misión y objetivos de la empresa.

En lo que respecta a los entregables, antes y después de dictaminar las vulnerabilidades de la organización, es importante documentar todas las decisiones de la gerencia. De acuerdo con Espinosa, el dictamen debe contener los riesgos a los que la organización está expuesta, así como aquellos a los que no está expuesta. De esta forma, la gerencia tendrá mayores elementos para tomar decisiones acertadas.

Encienda sus motores

Bien. Ya se han identificado las amenazas del mercado y las vulnerabilidades de la organización que, en conjunto, pueden representar un riesgo para la empresa. ¿Ahora, qué hacer con la información resultante?

El análisis de riesgos es apenas una parte de la administración de riesgos, que consiste en un proceso continuo de evaluación, monitoreo y control de las vulnerabilidades de la organización con respecto a los retos a los que se enfrenta. La administración de riesgos incluye el análisis del riesgo, el análisis del costo-beneficio (impacto de la amenaza contra inversión en mecanismos de protección), la selección de protecciones, el desarrollo de la estrategia de seguridad, la prueba de la seguridad y su evaluación, la implementación de las protecciones y la revisión continua y cíclica del sistema.

El objetivo de la administración de riesgos es llegar a una de las cuatro opciones que plantea el acrónimo META: mitigarlos, evitarlos, transferirlos o asumirlos. No es posible eliminar los riesgos, pues siempre habrá una ventana de oportunidad abierta para los atacantes, pero una gestión adecuada permitirá a las compañías reducir tanto esa brecha que posiblemente al atacante le resulte más caro y le tome mucho más tiempo tratar de explotar la vulnerabilidad que el beneficio que pudiera obtener si logra penetrar los controles.

Por lo anterior, la administración de riesgos debe enfocarse al futuro, en la medida de lo posible, descalificando los elementos inciertos de riesgo y considerando a los que pueden tener impacto más nocivo. Este razonamiento parte de la premisa básica de que, no es justificable para el negocio la protección a alto costo de una vulnerabilidad cuando el impacto de la amenaza puede ser bajo, mientras que deben buscarse los mejores mecanismos de prevención y control para proteger aquellos huecos de seguridad que podrían representar un impacto muy severo a la organización en caso de ser vulnerados.

Este escenario exige, en cierto modo, que la persona responsable de conducir un análisis de riesgos "entienda tanto los detalles técnicos de sistemas operativos, bases de datos, switches y demás, así como las necesidades de la empresa, sus procesos de negocio y el entorno (físico, político, social,

económico)", considera Farías. Un profesional con este perfil podrá elaborar el análisis de riesgos adecuado para su organización.

Factores que disparan los riesgos

En lo que respecta a las tecnologías de información, los administradores deben tomar en cuenta su nivel de exposición y el impacto asociado a los siguientes riesgos:

- De mercado: factores que van más allá del control de la gerencia, como los intereses y el tipo de cambio. Los sistemas de información basados en IT pueden verse afectados por las inversiones, las tasas de interés proyectadas y el flujo de dinero estimado, de acuerdo al tipo de cambio
- Financieros: Incluyen la incertidumbre sobre los ingresos proyectados, los pronósticos de ventas, el plan de gastos, etcétera
- Operativos: Aquí se incluyen las obligaciones contractuales, la identidad de empleados críticos, planes de expansión de negocios, el desempeño real de los procesos contratados, retrasos en los procesos y pérdida de empleados clave, entre otros

Elementos de riesgo

Los riesgos que amenazan la información se pueden clasificar en internos y externos.

Los primeros incluyen el sabotaje, huelgas, fraude, destrucción (voluntaria o involuntaria) de datos y recursos, y el robo de material, recursos o información, ya sea en forma de programas o datos, impresos o digitales.

Los riesgos externos incluyen factores naturales (sismo, incendio, inundación, tormenta, etcétera), humanos (robo, sabotaje, motines sociales, fraude, espionaje) y materiales (descomposturas y daños a los equipos, fallas de energía, entre otros).

Tipos de riesgo

- De seguridad: Cumplimiento de los usuarios del sistema con las políticas, estándares, procedimientos y reglas.
- De tecnología: Utilizar tecnología de punta que aún no ha pasado por un periodo de pruebas en el mercado puede implicar riesgos de seguridad.
- Organizacionales: Factores que no concuerdan con la estructura orgánica y las estrategias del negocio. Se puede encontrar información sobre la alineación de los objetivos a través de un business scorecard en www.bscol.com
- De comunicación: Incapacidad de comunicar o de escuchar efectivamente, lo que conduce a errores de interpretación y acciones inapropiadas.