



¿QUÉ PREOCUPA?

... LA INVERSIÓN EN SEGURIDAD

Recuerdo que algunos años atrás, conversando con un veterano y prestigioso responsable de seguridad con más de 40 años de experiencia, le pregunté si pensaba que la gestión de la seguridad era un asunto más de TI o de Negocio. Me miró sorprendido y me respondió: "de Negocio, por supuesto". Hoy día, no podría estar más de acuerdo con esta afirmación.

En el entorno cambiante de la seguridad de la información, donde cada día surgen nuevas amenazas, se publican decenas de vulnerabilidades y se construyen innovadoras soluciones tecnológicas, implementar un nivel de seguridad acorde a las necesidades

volver la vista hacia el mundo tradicional de la gestión empresarial, donde el objetivo de cualquiera de las áreas es obtener un beneficio para la organización. Dicho beneficio puede estar relacionado con el aspecto económico, la imagen, la estrategia corporativa o el cumplimiento normativo, pero en último caso ha de poder ser expresado en términos objetivos y cuantificables.

Cualquier estrategia de gestión de la seguridad por la que se opte requiere una inversión económica o humana y, al igual que cualquier otra, la inversión en seguridad debe ser rentable. Probablemente más de uno de ustedes, estimados

de las TIs: es seguro o no es seguro; nos han *hackeado* o no; si no hubo un incendio el año pasado, entonces no fue rentable el extintor. Debemos entrar de lleno en el incierto mundo de la probabilidad y la gestión de riesgos, en el cual, las amenazas no se eliminan, se mitigan. Invertir bien en seguridad significa conseguir el mayor beneficio posible dentro de la ecuación formada por el impacto (o coste) de los incidentes, amenazas existentes, probabilidades de materialización de las amenazas, contramedidas de seguridad y coste de las mismas.

Hay que seleccionar los indicadores económicos que queremos evaluar, buscar el método de análisis de riesgos que más se ajuste a nuestras necesidades y adaptar ambos a nuestra organización. No existe un método infalible, pero en mi opinión, un buen punto de partida es comenzar por el famoso retorno de la inversión (ROI), que se define como la diferencia entre el ahorro y el coste de la inversión. Si lo trasladamos a la seguridad, el retorno de la inversión en seguridad (ROSI) sería el ahorro en incidentes de seguridad menos el coste de las contramedidas. El ahorro en incidentes de seguridad se puede expresar como la diferencia entre la pérdida anual esperada (ALE) y la pérdida anual esperada modificada por las contramedidas de seguridad (mALE), donde la pérdida anual esperada (ALE) equivale al riesgo anualizado: impacto (o coste) de un incidente multiplicado por la probabilidad de ocurrencia en un año. Nuestro objetivo es obtener el mayor ROSI posible, aumentar la inversión o disminuirla no son las únicas decisiones factibles: en ocasiones se puede conseguir un incremento significativo simplemente reubicando la inversión, desinvirtiendo en los aspectos de menor rentabilidad para mejorar

La estimación del impacto de un incidente de seguridad es una tarea que atañe principalmente a Negocio, no a Seguridad.

de nuestra organización se convierte en una tarea, cuando menos, compleja. Si dejamos que la estrategia de seguridad sea dirigida por las necesidades tecnológicas, corremos el riesgo de perder de vista el verdadero objetivo, y a menudo nos encontramos inmersos en una frenética carrera entre amenazas y contramedidas que se aleja cada vez más de la realidad empresarial.

Merece la pena que nos detengamos en el significado de "seguridad acorde a las necesidades de nuestra organización". ¿Cuáles son las necesidades de nuestra organización respecto a la seguridad? Si planteamos esta pregunta a 10 directivos probablemente obtengamos 10 respuestas diferentes. ¿Cómo podemos acertar, nosotros, los profesionales de la seguridad, cuando hasta el concepto clave de nuestro trabajo es incierto? Quizás, en esta tesitura, nos puede ayudar olvidarnos de los virus y *hackers*, y

lectores, pensará que en la frase anterior algo falla: ¿"seguridad" e "inversión rentable"? ¿juntos?, ¿no es seguridad un centro de costes con el que no queda más remedio que vivir? En mi opinión, no. La inversión en seguridad debe de servir para que la organización obtenga un beneficio, al menos, superior al coste. El problema, muchas veces, radica en la dificultad de medir el coste y, sobre todo, el beneficio obtenido. La complejidad del asunto queda claramente reflejada cuando nos planteamos el ejemplo de un extintor de incendios: ¿es rentable un extintor?, ¿cómo evaluar la rentabilidad de algo que raramente se usa? Y lo que es aún peor, ¿cómo evaluamos la rentabilidad de un componente que nunca se debería utilizar si todo está bien planificado?

Llegados a este punto, es necesario deshacernos de la visión binaria tan habitual en el mundo

en puntos donde el retorno es superior.

Se ha de elegir la aproximación más adecuada –se puede afrontar el análisis por proceso de negocio, por activo de información, por grupo de sistemas de información, por proyecto, etc.– y aplicarlo en un ámbito realista bien acotado. Teniendo en cuenta que el punto de partida es Negocio, cada organización puede definir sus tipos de impacto y probabilidad, relacionando un significado cualitativo con una expresión cuantitativa –p.e., podemos definir que un impacto es crítico si amenaza la subsistencia del negocio, y equivale a una pérdida superior al 8% de los ingresos, o que una probabilidad es alta si se estima en 2 veces al año–.

La estimación del impacto de un incidente de seguridad es una tarea que atañe principalmente a Negocio, no a Seguridad, mientras que la estimación de la probabilidad de ocurrencia considerando las componentes técnicas y organizativas que intervienen es una labor del especialista en seguridad. Por tanto, el análisis de la inversión en seguridad fomenta la colaboración entre los expertos de negocio y seguridad, aportando a los primeros una visión sobre posibles escenarios de amenazas a su negocio y a los segundos información sobre las verdaderas necesidades de la organización.

A menudo se objeta que el impacto de un incidente es muy difícil de evaluar ya que entran en juego costes directos (financiero) e indirectos (de imagen, legal, etc.), pero yo soy un firme defensor de que sí se puede estimar. A veces es sorprendente la efectividad con la que el departamento de Marketing puede valorar el impacto debido a pérdida de imagen o el Financiero cuantificar el quebranto económico cuando se interrumpe un proceso de negocio. De igual forma, el

cálculo de probabilidad se puede aproximar. Debe alimentarse de todos los datos disponibles: históricos internos, bases de datos externas, aspectos organizativos y de personal, particularidades técnicas, etc.

Si bien el análisis de la inversión no es sencillo, citando a Confucio, “es mejor encender una pequeña luz que quejarse de la oscuridad». El objetivo no es la precisión, sino la obtención de una serie de parámetros y medidas para que los responsables de seguridad y de negocio puedan tomar buenas decisiones. No sólo consiste en acertar en los nuevos proyectos y

ción (e inversión), pero a largo plazo, se convierte en el cuento del “pastor y el lobo”, y genera un descrédito progresivo de los responsables de seguridad.

Reaccionar, esperando a que ocurra un incidente de seguridad y una vez que esto sucede buscar soluciones (e inversión), permite que durante cierto tiempo se preste más atención a la seguridad, aunque rara vez sirve para solucionar el problema en conjunto. Se van poniendo parches costosos y se transmite una sensación de falta de control.

Planificar e invertir proactivamente con criterios objetivos,

¿Cuáles son las necesidades de nuestra organización respecto a la seguridad? Si planteamos esta pregunta a 10 directivos probablemente obtengamos 10 respuestas diferentes

adquisiciones, hay que optimizar los recursos existentes. Sin olvidar los escenarios de reducción de gastos, que deben ser tan cuidadosamente examinados como los de nueva inversión. Por tanto, evaluar la inversión de seguridad está claramente ligado a la gestión y estrategia de seguridad. Poner el discurso de seguridad en términos de coste/beneficio facilita la comunicación con el resto de áreas y desmitifica la función de seguridad, reduciendo el problema al tipo de decisiones que la Dirección toma cada día.

Me viene a la mente un artículo que leí hace no mucho, en el que se identificaban los tres tipos más comunes de estrategia de concienciación de seguridad: Asustar, Reaccionar o Planificar/Invertir proactivamente. La estrategia de asustar, avisando sobre los escenarios más negativos y preocupantes, en un principio puede parecer efectiva ya que se consigue aten-

aporta una mayor credibilidad y alinea las necesidades de seguridad con las de negocio, facilitando la comunicación con la dirección y el resto de áreas mediante un lenguaje común: el del retorno de la inversión.

Estoy convencido de que todos conocemos ejemplos de los tres tipos, decidir por cual queremos apostar, qué lenguaje vamos a emplear y con qué herramientas contaremos, es clave para el éxito. ¿Qué estrategia nos interesa más?

Por cierto, según la *American Society of Safety Engineers*, un extintor de incendios es rentable. De media, por cada 1\$ invertido se obtiene un retorno de 3\$. ■



>Daniel Barriuso Rojo

Responsable de Seguridad de la Información
CREDIT SUISSE ESPAÑA