Gestión de riesgo de ciberseguridad y utilidad neta

Andrew Kling
Schneider Electric
www.schneider-electric.com.ar

En 2013, el entonces presidente de Estados Unidos, Barack Obama, instó al Instituto Nacional de Normas y Tecnología de su país (NIST, por sus siglas en inglés) que desarrolle un marco que se convertiría en una fuente de autoridad para las mejores prácticas de ciberseguridad [1]. Otros países del mundo cuentan con estándares similares o trabajan activamente en versiones locales. En algunos países, como Francia, estos estándares tienen fuerza de la ley [2].

Estos estándares de ciberseguridad facilitan una aproximación al tema de forma ordenada y estructurada que atienden los desafíos de la ciberseguridad. Dichas normas colaboran a traducir cuestiones de ciberseguridad basadas en términos vagos y atemorizantes en un análisis racional del riesgo, de tolerancia al riesgo y de formas de evitarlo.

Cambiando la discusión de un impreciso "miedo al ataque" a una discusión racional que pueda tomar su lugar tiene un impacto positivo hasta en el último eslabón de las organizaciones. Efectivamente, el tema de conversación pasa del miedo e incertidumbre en lo que respecta a la ciberseguridad a uno que define de manera más precisa los resultados posibles en caso de que los riesgos definidos por esos temores se hagan realidad.

Las defensas de ciberseguridad luchan por paliar las ciberamenazas dañinas en contra de las operaciones, instalaciones e individuos. Tales daños pueden tomar forma de una pérdida financiera, pérdida de la propiedad intelectual, pérdida de la privacidad y pérdida de la reputación. Todo afecta la capacidad de una organización de llevar a cabo su misión principal (en general, aunque no necesariamente, su beneficio financiero).

El riesgo de ciberseguridad es solamente uno de los factores dentro de la situación de riesgo general en la estrategia de gestión de riesgo de una organización. El riesgo de ciberseguridad, como cualquier otro riesgo, no se puede eliminar completamente, pero sí se puede gestionar a través de procesos informados de toma de decisiones. El objetivo de un programa de ciberseguridad es reducir la probabilidad y efecto de un ciberevento en las operaciones de una organización, instalación o individuo. Un proceso equilibrado, informado de toma de decisión que incluya la gestión de riesgo cibernético conducirá a un efecto positivo en el beneficio financiero de todo el negocio.

Andrew Kling
Andrew Kling tiene más de treinta años de experiencia en el desarrollo de software. Trabaja en la organización del desarrollo de sistemas de control industrial (ICS) en Schneider Electric desde el año 2001, asegurando que los requisitos de seguridad cibernética formen parte de cada proyecto que se ejecuta

El conjunto central de prácticas de ciberseguridad necesarias en nuestra industria son bien conocidas. Sin embargo, las barreras para su adopción aún existen. En gran medida, tales obstáculos se sostienen en un entendimiento impropio de los riesgos y de la capacidad de la organización para resistirlos. A pesar de la existencia de incentivos de gestión de riesgo y regulaciones, encontrar compañías que atiendan la ciberseguridad de forma acabada es aún raro. Es hora de mudar la conversación lejos de los miedos por un ciberataque a algo entendido por las altas gerencias: el beneficio financiero .

Conocer, entender el lugar de la ciberseguridad en su organización. Conocer, entender la capacidad de su organización a la tolerancia al riesgo. Tras conocer estas dos piezas de información, usted puede comenzar el camino a entender la diferencia entre en dónde está parado hoy en la gestión de riesgos cibernéticos y cuánto se puede acortar la brecha. Es ahí en donde una estrategia para mejorar el nivel de preparación de su empresa a la ciberseguridad a través de un programa de gestión de riesgo que alcance la totalidad.

- Localice la responsabilidad de la ciberseguridad en su organización, de modo tal que la toma de decisiones, la ejecución y la respuesta a los incidentes sean eficientes y exitosas. Este paso es para visualizar el flujo de trabajo de su gestión de riesgo. Especifique los objetivos de la gestión de riesgo de ciberseguridad.
- Establezca el valor de sus bienes para su organización, y posibles atacantes. Este paso es para calcular el tamaño del riesgo de seguridad.
- Modele un panorama de amenaza. Analice amenazas de seguridad específicas de su industria. Recuerde, la amenazas evolucionan constantemente, a la par de las nuevas habilidades, técnicas y herramientas.
- Determine en dónde podría integrar las funciones de riesgo de seguridad dentro de la infraestructura de su organización.

- Construya un plan de ciberseguridad de modo que su organización pueda responder a un ciberataque general. Analice las opciones del plan. Jerarquice los elementos del plan según su efectividad para reducir riesgos.
- Ejecute en base al plan para gestionar los ciberriesgos de su organización.
- Tenga en mente que los elementos del programa, tales como parches de errores ('*bug patching*') y monitoreo de amenazas, son continuos. Un plan de gestión de riesgo de ciberseguridad no es una acción de una vez, sino una operación continua.

Tenga un plan, actúe en base al plan, mida la efectividad de la ejecución del plan y, si es necesario, mejore el plan. Estas instrucciones son una aproximación simple a gestionar los riesgos cibernéticos con un efecto positivo en toda su compañía.

Referencias

[1] *http://www.nist.gov/cyberframework/*
[2] *http://www.ssi.gouv.fr/en/cybersecurity-in-france/*