Gestión de riesgo de ciberseguridad y cómo prepararse para enfrentarla

La amenaza más grande de la ciberseguridad: no comprender los riesgos

Por Andrew Kling, de Schneider Electric, *www.schneider-electric.com.ar*

Malentendido sobre ciberseguridad número uno: muchos negocios creen que el problema de la ciberseguridad no los afectará porque la gente no sabe si la compañía ha implementado o no un programa de ciberseguridad. Falso. Incluso los más inexpertos en Internet cuentan con varias herramientas para determinar el nivel de seguridad informática de una compañía.

Otro malentendido común es creer que sus ciberdefensas son lo suficientemente buenas sin haber dedicado tiempo ni esfuerzos para analizar esas defensas y comparar su efectividad con la tolerancia de riesgo de ciberseguridad de la empresa, definida en el plan de gestión de riesgo.

La ciberseguridad es una cuestión de gestión de riesgo integral que necesita ser considerada desde una perspectiva estratégica, económica y transversal a varios departamentos. Un buen lugar para empezar es definir la gestión de riesgo de la empresa como el "proceso general de gestionar la exposición de una organización a lo incierto, con un particular énfasis en identificar los eventos que potencialmente podrían impedir a la compañía alcanzar sus objetivos" (*Gordon & Loeb, 2005*). La gestión de riesgo de ciberseguridad es una parte del plan de riesgo general de la empresa. Es el proceso de gestionar eventos potencialmente dañinos debido a la falta de defensas de ciberseguridad efectivas y de resiliencia de ciberseguridad.[1]

No importan cuán bien controlen, las organizaciones podrían aún experimentar mayores interrupciones (por ejemplo, robo de códigos fuente o diseños de producto). La resiliencia de ciberseguridad representa la habilidad de una organización para adaptarse a tales perturbaciones, e incluso crecer al enfrentarlos..

Situar los costos de los cibereventos en contexto

Una pregunta crítica: ¿cuánto de un problema son los cibereventos? Primero, como se publicó en la revista académica de Oxford sobre de ciberseguridad (*Oxford Academic Journal of Cybersecurity* [2]), la investigación mostró una contradicción interesante. Por un lado, que los promedios totales de cibereventos muestran una tendencia, que los ciberincidentes son más frecuentes y por lo tanto

Sobre el autor

Andrew Kling tiene más de treinta años de experiencia en desarrollo de software. Ha trabajado en la organización del desarrollo de Sistemas de Control Industrial (ICS) en *Schneider Electric* desde el año 2001. Ha llevado al equipo de desarrollo de equipamiento para la automatización de procesos de *Schneider Electric* a la primera certificación "ISA Secure - Secure Development Lifecycle Assurance" para tres sitios de desarrollo en tres continentes. En esta responsabilidad ha mejorado la adopción del "Secure Development Lifecycle", asegurando que los requisitos de seguridad cibernética formaran parte de cada proyecto que se ejecuta.

más costosos (en total) para las organizaciones, especialmente cuando se involucra información personal en el incidente. Por otro lado, los costos reales de estos eventos en los reportes analizados les cuestan a la mayoría de las empresas menos de 200 KU$D, solo una fracción de los millones de dólares que comúnmente se leen en los titulares de los medios de comunicación. Y los ataques a los sistemas de automatización y control industrial (*Industrial Automation Control Systems* o IACS como se los conoce por su sigla en inglés) no se compara con los ciberataques a la población en general, a menudo motivados por cuestiones financieras. Estos sistemas IACS se utilizan para manejar la infraestructura crítica del mundo. Los impactos a estas infraestructuras son difíciles de medir, y cuando se intenta hacerlo éstas se acumulan en sumas impactantes.

Por ejemplo: el ciberataque a la red de energía de Ucrania en diciembre de 2015. Los sistemas de control fueron separados de las redes centrales de control con *firewalls* entre las redes administrativas (IT) y las redes de operaciones (OT) del sistema de distribución eléctrica. Sin embargo, los sistemas aún estaban comprometidos. Se cree que el ataque fue una represalia por un ataque físico de activistas pro-ucranianos en subestaciones de energía de territorios anexados a Rusia. En este caso, las reputaciones del gobierno y del proveedor de electricidad aparentemente sufrieron mayor daño del que se puede medir con un apagón relativamente menor de un par de horas. Un año después, otro ataque, otra vez en Ucrania, posiblemente para llevar a casa el mensaje político.

La investigación muestra un incremento en la cantidad de ciberincidentes. Pero los costos por incidentes por sí solos no reflejan la misma magnitud de las consecuencia, o la urgencia de atención. Proteger las infraestructuras críticas del mundo conlleva una responsabilidad significativa. Cita de la Comisión Europea – Infraestructura Crítica: "… es esencial para el mantenimiento de las funciones vitales de la sociedad. El daño a una infraestructura crítica, su destrucción o interrupción por desastres naturales, terrorismo, actividad criminal o comportamiento malicioso, quizá tenga un impacto negativo significante para la seguridad de la UE y el bienestar de sus ciudadanos".[3]

Mientras que el potencial de mayores daños parece estar agrandándose a medida que pasa el tiempo, la evidencia de que los impactos financieros son menores a lo esperado es un error de medición que resulta en malentender los verdaderos riesgos.

Las organizaciones carecen de un real incentivo financiero para aumentar su inversión en ciberseguridad. Pero la naturaleza del trabajo que se lleva adelante para proteger los IACS demanda un entendimiento más profundo de la misión de cada organización. Esto resultará en programas de ciberseguridad que hagan foco en mejorar aspectos más prácticos de sus programas de gestión de riesgo: prevención, preparación y respuesta.

Por lo tanto, se debe:

- Tomarse el tiempo necesario para entender la naturaleza de los riegos de ciberseguridad de hoy.
- Conocer la tolerancia a estos riesgos.
- Tener un plan para gestionar el riesgo.
- Elegir a un socio que ayude a encontrar una solución de ciberseguridad para los IACS. ❖

Referencias

[1] Cybersecurity Risk Management and Insurance, *https://www.actuaries.org.uk/documents/c8-cybersecurity-risk-management-and-insurance*, Ene. 6, 2014

[2] Examining the costs and causes of cyber incidents, Sasha Romanosky, *https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyw001/2525524/Examining-the-costs-and-causes-of-cyber-incidents*

[3] *https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en*