Protección de la cadena de suministro

DOI: 10.29236/sistemas.n164a2

A medida que las cadenas de suministros lineales tradicionales son más flexibles, digitales y conectadas, el número de enlaces externos que una organización tiene con otras, como el volumen y las fuentes de datos que fluyen a través de esas conexiones, crecen exponencialmente.
Así también lo hace el número de riesgos potenciales y vulnerabilidades.

Juan Mario Posada D.

En este mundo digital estamos tan seguros como el más débil de los eslabones en la cadena de suministros (Olson, 2020). Esto ha hecho que la protección de la cadena de suministro se convierta en uno de las preocupaciones con mayor crecimiento en los negocios modernos.

La pandemia impulsó las tendencias de aumento en la interoperabilidad, interconexión, eliminación de fronteras, aumento de volúmenes

de los datos y fuentes de información. Además, las organizaciones están redoblando la apuesta por la digitalización para su agilidad y capacidad de respuesta y estar mejor preparadas para hacer frente a los impactos de la crisis y sus consecuencias.

Para gestionar las crecientes amenazas que son inherentes al entorno de negocios, las organizaciones necesitan integrar los principios de seguridad en toda la red de la cadena de suministro. Esto incluye hacer de la ciberseguridad una prioridad no sólo dentro de la empresa, sino también a través de todas las organizaciones asociadas conectadas. También incluye el desarrollo de soluciones de trazabilidad para mejorar la visibilidad de la red. Estas deben ser consideraciones centrales en el diseño de cualquier cadena de suministro inteligente. Es acá donde toman gran relevancia esos factores que influencian la dinámica del entorno de seguridad digital, identificados por Accenture Cyber Threat Intelligence en su reporte anual (Accenture, 2020):

1. Entorno geopolítico comprometedor.
2. Los ciberdelincuentes se adaptan, apresuran y diversifican.
3. Aumento de motivos para el *ransomware.*
4. La mejora de la higiene del ecosistema está empujando las amenazas hacia arriba en la cadena de suministro.
5. Las vulnerabilidades en la infraestructura de la nube exigen soluciones costosas.

¿Cuál es la solución?

Como en muchos otros desafíos de la transformación digital de los negocios, la solución empieza por pensar en la seguridad desde el diseño como elemento fundamental de los procesos de la cadena de suministro.

Para reforzar la ciberseguridad de las cadenas de suministro, las empresas deben construir herramientas de soluciones de seguridad para cubrir las posibles vulnerabilidades. Para la mayoría, esto debería incluir una combinación de gestión de activos; supervisión de la seguridad; revisión y gestión de contratos legales; evaluación de la postura de seguridad del vendedor/proveedor; y la autenticación para el acceso al sistema.

Las empresas deben avanzar hoy hacia una base de datos central que recoja y compruebe la data. Hoy blockchain es una gran oportunidad en ese sentido, ya que integra eventos logísticos en la cadena de suministro y, a través de códigos QR únicos en los productos, pueden, por ejemplo, comprobar la autenticidad y obtener el detalle de la ruta del producto.

Las organizaciones deben buscar ahora ampliar sus estrategias y procesos de seguridad. Para esto, deben trabajar en conjunto con sus

proveedores para aumentar la visibilidad, comprender las amenazas y su potencial aplicabilidad e impacto en su organización. De esa forma se podrá avanzar hacia una estrategia que mitigue los riesgos. Para esto, National Institute of Standars and Technology (NIST) (s.f.) sugiere contemplar algunos principios guía:

- Desarrollar las iniciativas bajo el supuesto de que los sistemas serán vulnerados que permite responder no sólo a la pregunta de cómo prevenir sino también cómo recuperarse.
- La ciberseguridad nunca es un problema exclusivo de tecnología pues contempla a las personas, los procesos y el conocimiento empresarial. Cada vez son menos las infracciones originadas en fallas tecnológicas y más las derivadas de errores humanos.
- Seguridad es Seguridad, los adversarios aprovechan las brechas de la seguridad física para lanzar los ciberataques y viceversa.

Referencias

Accenture. (2020). Securing the supply chain. https://www.accenture.com/cr-en/insights/consulting/securing-the-supply-chain

National Institute of Standards and Technology (NIST). (s.f.). Best Practices in Cyber Supply Chain Risk Management. Supply Chain Best Practices (p. 3). National Institute of Standards and Technology (NIST).

Olson, E. (2020). Why you need to urgently rethink supply chain security. Accenture Business Functions Blog. https://www.accenture.com/us-en/blogs/business-functions-blog/why-you-need-to-urgently-rethink-supply-chain-security

Thomas, A. R. (2010). Supply Chain Security, International Practices and Innovations in Moving Goods Safely and Efficiently. Praeger.

Juan Mario Posada Daza: *Líder de los servicios de ciberseguridad en Accenture Colombia. Con más de 15 años de experiencia en áreas relacionadas con Ciberseguridad, Auditoría de TI y Gestión de Riesgos en empresas del sector financiero, energía, consumo masivo y telecomunicaciones. Ha trabajado anteriormente en firmas de consultoría como Deloitte e EY, donde estructuró y fortaleció las prácticas de servicios de consultoría en Ciberseguridad, seguridad de la información y privacidad.*