Retos de Ciber-seguridad

Cybersecurity in Supply Chain, escrito por Sumit Vakil y publicado por la empresa resilinc, nos da una gran perspectiva de lo que significa el concepto de ciber-seguridad en las cadenas de suministro modernas. En el mundo de hoy, los negocios y los sistemas globales están cada vez más interconectados y cada una de las organizaciones tiene diferentes grados de protección y control sobre el acceso a su información.

Debemos aceptar que la información es lo que impulsa a las cadenas de suministro, compartir información con los múltiples socios, ha creado una vulnerabilidad sin precedentes considerando el elevado impacto que ésto puede tener sobre la continuidad del negocio.

Por ejemplo, en la actualidad los proveedores no solo tienen acceso físico a las instalaciones de las empresas, sino también pueden acceder a datos confidenciales, en algunos casos extremos, los productos que se proveen son basados en propiedad intelectual del cliente. Los empleados de la organización, mantienen un constante intercambio de información con personal de los proveedores y se tiene amplia confianza sobre la seguridad asociada con la información proveniente de éstos. Difícilmente alguien abrirá un anexo de un correo electrónico proveniente de un desconocido, pero seguramente lo hará si proviene de un proveedor.

Tomemos en cuenta que todo empleado tiene almacenada información, de diferentes niveles de confidencialidad, en sus computadoras o dispositivos móviles y ésta puede quedar expuesta a cualquier intruso y no solo eso, su dispositivo puede utilizarse como acceso a otro tipo de información.

Además de todo esto, recordemos que nuestros proveedores tienen a su vez proveedores, que pueden también tener acceso a los sistemas compartidos, por lo cual la pérdida de un equipo o el acceso ilegal de cualquier miembro de la red, puede ser una llave de acceso para los sistemas internos de todos los que la comparten y causar múltiples daños, que van desde la introducción de virus, hasta le instalación de "malwares"

Muchos de los desarrollos comerciales están basados en las mismas plataformas tecnológicas, por lo cual el acceso a uno de estos sistemas, puede abrir la puerta a múltiples aplicaciones más, sin un gran esfuerzo extra.

Las grandes empresas aplican inspecciones a sus proveedores en temas de materiales, servicios, posición financiera, seguridad y recientemente también incluyen un aspecto de seguridad en el manejo de datos y tecnología de información, sin embargo, la frecuencia en los cambios tecnológicos hace que el análisis inicial pierda rápidamente valor y pocas empresas solicitan que se actualice esta información.

Bajo la digitalización y la famosa Industria 4.0, muchos equipos productivos y de medición están conectados a las redes y prácticamente nadie valida que estos sistemas operen de forma segura, por lo cual pueden ser una puerta de acceso a los sistemas gerenciales.

Para poder enfrentar este gran reto de ciber-seguridad, las compañías deben tener un rol más proactivo que implique el monitoreo de las prácticas de seguridad de sus socios de negocio bajo un proceso similar a este:

- La fuerza de la seguridad de una empresa la marca el eslabón más débil. Esto implica que las medidas de seguridad se le deben de aplicar a todos los que tengan algún tipo de acceso a los sistemas de la empresa, sin importar su tamaño o importancia.
- Pedir a cada proveedor que informe sobre sus procesos de protección en aspectos de tecnología de información. Se debe usar un breve cuestionario estándar que permita hacer comparativos y evaluar al proveedor.

Ing. Jesus Campos Cortés
CPIM CIRM, C.P.M, PMP, CQIA, CEI, CSCP, CPSM, CPF, PLS, CS&OP, PRINCE2, CA-AM, CLTD
jcamposc@crmmexico.com
http://jesuscampos.mx/otras-publicaciones/

- Considerando que algunos incidentes de seguridad se generan por “bugs” en los softwares. La compañía debe pedir a los proveedores una lista de los softwares que utiliza y la versión a la que corresponden.
- Implementar analítica en los datos recolectados con la finalidad de identificar vulnerabilidades en los procesos de los proveedores.
- Aplicar procesos de “acciones correctivas” con los proveedores que presentan ciber-vulnerabilidades.
- Apoyarse en expertos externos para realizar auditorías integrales.
- Implementar sistemas de monitores 7 x 24 para incidentes o vulnerabilidades de seguridad detectados.
- Desarrollar indicadores para conocer la salud de la ciber-seguridad de los proveedores mediante reportes trimestrales.
- Motivar a los proveedores a mejorar sus prácticas asociadas con la ciber-seguridad
- Evitar el uso de canales no seguros para el intercambio de información relevante, como el correo electrónico.
- No almacenar información delicada en equipos individuales, apoyarse en soluciones tipo SaaS.
- Adquirir seguros para protegerse contra pérdidas ocasionadas por ciber-ataques.

Aplicar esta serie de acciones, reducirá la exposición de la compañía. La mejor defensa contra este tipo de riesgos es la constante vigilancia.

Para redondear estas ideas, un artículo de Barry Hochfelder llamado “The Risks of Eluding Risk”, nos arroja estadísticas relevantes sobre el tema de riesgo, por ejemplo:

- 66% de las empresas tienen un responsable de riesgo en su empresa, pero prácticamente todas ignoran el tema asociado con el riesgo en la cadena de suministro.
- 100% de los ejecutivos participantes de una encuesta, reconocieron a los seguros como un método efectivo de mitigación de riesgo, pero el tema no estaba en su interés y reconocen un alto desconocimiento de su adecuada utilización.

El autor considera que entre las razones por la cuales las empresas no toman los pasos apropiados para mitigar el riesgo se encuentra el dejar todo para el último momento y que invertir en “evitar”, no demuestra fácil y claramente un ROI.