AÑO 25 / NÚMERO 106 / NOVIEMBRE - DICIEMBRE 2022

CONTACT FORUM

¡Alcancemos la **equidad** en nuestras comunidades!

Construyendo el **talento diverso** del futuro

IMT

4 recomendaciones para reforzar la seguridad de los activos empresariales

Erik Moreno

Director de Ciberseguridad de Minsait, una compañía de Indra en México

En el entorno de amenazas de hoy, la interrogante no es si una empresa podría ser blanco de un ciberataque en un momento dado, sino de cuándo lo será. Su seguridad está bajo el riesgo constante de ser vulnerada, sin importar su tamaño o el sector en el que opere.

La superficie de ataque crece continuamente debido a sistemas vulnerables, prácticas de protección pobremente diseñadas y ejecutadas, el aumento constante de dispositivos personales, así como por la migración a la nube y la implementación del trabajo remoto.

Una encuesta de IDC señala que más de una tercera parte de las organizaciones de todo el mundo han experimentado algún ataque o brecha de *ransomware* que logró bloquear el acceso a sus sistemas o datos. Esto les representó un desembolso importante de recursos, además de poner en riesgo la continuidad de su negocio y afectar su reputación.

Si bien muchas organizaciones trabajan constantemente en optimizar su estrategia de defensa, se estima que más de la mitad (56%) no cuenta con un plan de respuesta a incidentes de ciberseguridad, y que sólo un 30% cree que su plan es efectivo.

Acciones clave

Por ello, las organizaciones llevan a cabo constantemente acciones para reforzar su ciberseguridad y minimizar cualquier riesgo a los que pudieran estar expuestas.

Para apoyarlas en esa tarea, comparto cuatro recomendaciones que les servirán de guía para la protección efectiva de sus recursos y activos, al tiempo de apuntalar la confianza de clientes y socios, así como robustecer su reputación corporativa.

1.- **Implementar una estrategia de seguridad basada en riesgos.** Comúnmente, las organizaciones orientan su estrategia de ciberseguridad hacia la adopción de tecnologías de última generación, pero con frecuencia no toman en cuenta los activos de información críticos, las "joyas de la corona", que hay que cuidar y proteger en primera instancia.

   El primer paso, por tanto, es identificar esos activos para hacer una evaluación precisa de los riesgos a los que están expuestos. Las transacciones financieras, por ejemplo, podrían estar expuestas a fraudes y desvíos, mientras que en un entorno industrial el riesgo radicaría en que las operaciones se vieran comprometidas.

   Al diseñar una estrategia de seguridad basada en riesgo, las organizaciones podrán no solamente tener visibilidad total de sus activos, sino también de tener bases sólidas para justificar la inversión en tecnología de ciberseguridad.

2.- **Proteger la cadena de suministro.** Los autores de amenazas han comenzado a penetrar a las redes y sistemas de una organización atacando primero a su ecosistema de proveedores. Si bien es una ruta más larga, está probando ser efectiva.

   ¿La razón? Muchos proveedores carecen de los controles de seguridad y no tiene el mismo nivel de madurez que las empresas más grandes, a lo que se suma un pobre cumplimiento con las normativas de protección.

   De ahí la importancia de colaborar con socios que cuenten con políticas de ciberseguridad robustas, y evaluar constantemente su postura en este rubro para minimizar la exposición de los recursos empresariales a las amenazas informáticas.

3.- **Aplicar controles de acceso y la gestión de identidades.** En esencia, se trata de determinar quién tiene acceso a qué, al tiempo de establecer mecanismos efectivos de autenticación y protección de la información, tanto en entornos de nube como locales.

   Endurecer el acceso y gestionar las identidades es hoy un requerimiento ineludible ante la creciente digitalización, la virtualización de sistemas, el trabajo remoto, el cómputo en la nube y el *edge computing*, entre otras tendencias.

   Asimismo, contribuirán en gran medida a prevenir la fuga de datos, proteger la información confidencial, vigilar estrechamente quién se mueve al interior de la red, e identificar y responder cualquier actividad sospechosa oportunamente. Asimismo, reducirán el riesgo de afectar la reputación de la empresa y perder la confianza de sus clientes.

4.- **Proteger la tecnología operativa (OT).** Las amenazas no son exclusivas de la tecnología de la información (IT), afectan también a la tecnología operativa (OT), donde puede afectarse la infraestructura estratégica y crítica de industrias como manufactura, transporte, petróleo y gas, electricidad e hidráulica, entre otras.

   En OT, la disponibilidad de la tecnología debe ser constante (24x7) para soportar las operaciones de una empresa o los servicios provistos a clientes o ciudadanos. Por lo tanto, los sistemas OT necesitan estar siempre disponibles y protegidos contra cualquier incursión por parte de atacantes y *software* malicioso como *ransomware* o DDOS.

Si hay algo seguro es que los atacantes no les darán tregua a las organizaciones y continuarán buscando formas de penetrar a sus redes y sistemas, buscando impactar sus activos de información críticos y obtener beneficios económicos al mismo tiempo.

En el mercado existen empresas que pueden ayudarlas a desarrollar e implementar una estrategia de ciberseguridad efectiva, acorde a su actividad y nivel de riesgo, y manteniendo un alto nivel de protección en un entorno cada vez más conectado y digitalizado.