Once claves para evolucionar hacia una Organización Protegida

En la era de la transformación digital, la ciberseguridad avanza a pasos agigantados para responder al aumento de los ciberataques

Fuente: LA RAZON

11. Gestión del riesgo digital. La progresiva digitalización de las organizaciones y sus procesos ha incrementado exponencialmente el número de amenazas existentes, introduciendo nuevos vectores de riesgo. La clave está en contar con las capacidades para identificar y gestionarlos, alineado con la estrategia de negocio.

10. Riesgo de fraude. Es fundamental prevenir cualquier tipo de fraude que pueda afectar a una organización con herramientas y ejercicios proactivos, y detectar comportamientos y acciones inadecuadas de clientes o empleados a través de la implantación de soluciones modulares para procesos transaccionales o de comercio electrónico, complementado con el control por agentes expertos.

9. Soluciones de firma digital para securizar los procesos empresariales. La digitalización de los procesos requiere completar las transacciones con una firma digital de forma ágil, eficiente en tiempo y costes, y con plenas garantías legales. Una solución en la nube facilita la integración con aplicaciones, asegurando el archivo y la recuperación.

8. Alta digital de clientes o Digital Onboarding. Llevar a cabo su incorporación a través de tecnología de identificación y uso de elementos biométricos que les proporcione un entorno seguro para realizar sus operaciones. Estas transacciones digitales deben iniciarse con procesos de registro de identidades en tiempo real y en cualquier lugar que garanticen y protejan al usuario desde el inicio de la relación.

7. Gestión de la identidad digital. Controlar los derechos de a qué servicios y qué perfiles tiene cada persona en una organización es esencial. La inteligencia artificial en los procesos de perfilado junto con soluciones de múltiple factor de autenticación y acceso (sign-on) unificado, además de la protección de las cuentas privilegiadas y del acceso a los datos, permiten garantizar un entorno de confianza para los usuarios de sistemas de información.

6. Detección de amenazas y respuesta efectiva. Identificar los activos digitales es crucial para una organización y supone el primer paso para gestionar sus puntos vulnerables y detectar posibles amenazas con el objetivo final de responder de manera eficaz a los ciberincidentes y maximizar así la resiliencia del negocio.

5. Implementar un Plan de Ciberseguridad. Con las prioridades, los responsables y los recursos que se van a emplear para mejorar el nivel seguridad en la organización, y con los proyectos técnicos, organizativos y de contenido legal, coordinado mediante una oficina técnica.

4. Definición de una arquitectura robusta de seguridad. En el mundo TI, la protección de entornos multicloud, seguridad de las aplicaciones, desarrollo seguro de software, y gestión de las alertas de servicios son clave en la implantación de soluciones.

3. Planes de continuidad de negocio. Definir e implementar las estrategias de respaldo y recuperación frente a desastres son esenciales para evitar la pérdida de datos y reducir los tiempos de inactividad provocados por amenazas externas, indisponibilidades de red, errores humanos y otras interrupciones del servicio.

2. Concienciar a empleados y usuarios sobre la seguridad de la información y la protección de los activos críticos. Ellos son la primera línea de defensa ante un ciberataque –el 90% se inician a través de técnicas de ingeniería social– y su concienciación y formación son una necesidad para las organizaciones y un requisito legal.

1. Cumplimiento legal y regulatorio. El entorno regulatorio y legislativo resulta bastante complejo y condiciona muchas de las acciones a poner en marcha, por lo que es necesario contar con especialistas que combinen conocimientos técnicos y legales que proporcionan flexibilidad para adaptar las soluciones de seguridad a diferentes sectores y plataformas, minimizando los riesgos derivados por incumplimiento (económicos por sanciones, operativos, reputacionales…).

La hoja de ruta prevé identificar riesgos, poner en marcha acciones de protección, determinar una estrategia para detectar posibles ataques, contar con especialistas para poder reaccionar eficazmente y disponer de capacidades para recuperarse de los mismos. Para afrontarlo con éxito, SIA, compañía líder en ciberseguridad a través de la que Minsait, la compañía de Indra especializada en digitalización, presta servicios en este ámbito, plantea once claves para minimizar el riesgo y maximizar la protección de los negocios:

Esta situación requiere de planes y medidas de protección frente a las amenazas que plantean lo que SIA denomina las cuatro fuerzas de la digitalización (normativa y marco regulatorio, transformación de sistemas TI, adopción del internet de las cosas y soluciones industriales, e interacción digital creciente entre las personas) y evolucionar hacia un nuevo modelo: Organización Protegida Digitalmente.

Si bien muchas compañías han centrado sus esfuerzos e inversiones en acciones contundentes frente a los ciberataques para garantizar la continuidad de su actividad, el margen de mejora es alto. Según el informe Ascendant de Madurez Digital en Ciberseguridad 2021 de SIA y Minsait (ambas, compañías de Indra), el 56% de las organizaciones tiene aún como asignatura pendiente contar con una estrategia de ciberseguridad bien definida.

FUENTE: LA RAZÓN