Ciberseguridad y protección de la privacidad: ¿quién es el responsable?

En muchas organizaciones, la lógica dicta que el aspecto de la ciberseguridad se atribuye directamente al CISO (Chief Information Security Officer). A menos que exista una responsabilidad colectiva por la seguridad cibernética y la privacidad, los datos no están seguros y si las cosas salen mal, es responsabilidad de todos.

En algunas organizaciones, la alta dirección no siempre se toma en serio la seguridad de TI y la privacidad de los datos. Con demasiada frecuencia se descuidan, muchos de estos temas son tareas que pueden delegarse al CISO o al DPD (responsable de protección de datos) y olvidarse. Si la gerencia continúa viéndolo de esta manera, entonces no es de extrañar que este tipo de actitud se esté extendiendo en las organizaciones y que el personal de todas las categorías tampoco se tome estos temas en serio.

Por lo tanto, hay algunos consejos para superar estas vulnerabilidades de seguridad:

1. Opte por dispositivos encriptados

Si la decisión de comprar unidades USB, SSD o dispositivos IoT no cifrados se basa únicamente en el precio, independientemente de si son seguros o tienen cifrado de hardware, entonces esos dispositivos no cifrados crean una vulnerabilidad cibernética. Toda la organización corre el

riesgo de sufrir una filtración de datos.

2. No olvide las contraseñas

Si el personal no sigue las reglas básicas de ciberseguridad y es descuidado con las contraseñas o los archivos adjuntos de correo electrónico, está poniendo en riesgo la seguridad de toda la organización. Los ciberdelincuentes se dirigen activamente a contraseñas débiles o conocidas y utilizan tácticas de phishing para comprometer la seguridad de sus víctimas. Estos son algunos de los vectores de ataque más comunes para los incidentes cibernéticos.

3. Respete el uso de datos privados

El GDPR estipula que los datos personales solo se pueden recopilar con el consentimiento del interesado para un propósito específico. Si una empresa recopila o comparte datos ilegalmente, expone a todos a multas y litigios importantes. La ciberseguridad y la confidencialidad de los datos son, por

tanto, temas que no deben pasarse por alto. Por el bien y la seguridad de todos, es preferible utilizar unidades USB seguras, SSD o dispositivos de IoT, respetar las normas de higiene de TI o utilizar los datos de los clientes de forma adecuada. El cambio de cultura es la clave Para cambiar las mentalidades y garantizar que los empleados tomen en serio la ciberseguridad y la confidencialidad de los datos en una organización, en todos los niveles jerárquicos, es imperativo cambiar la mentalidad cultural. Hay muchos incentivos para que las empresas hagan esto. Es obvio que los clientes estarán felices de hacer negocios con organizaciones que creen que se ocuparán de sus datos y que serán más reacios a hacer negocios con aquellas que no lo hagan. Por lo tanto, mantener la confianza del cliente y evitar cualquier incidente de ciberseguridad que pueda socavar esta confianza debe ser una prioridad para todos. Además, existen diferentes palancas para que las empresas se tomen en serio la protección de datos.

Para empezar, el RGPD. Esta norma prevé una multa máxima de 20 millones de euros o el 4% de la facturación mundial anual, la más alta de las dos, por cada incidente identificado. El costo de arreglar un incidente puede ascender a millones de dólares y si se trata de un ataque de ransomware, los ciberdelincuentes podrían exigir un rescate de varios millones de dólares más. También existe el riesgo de ser demandado por aquellos cuyos datos se han visto comprometidos. Como si tales sanciones contra una organización no fueran suficientes, también están surgiendo sanciones contra las personas. De hecho, un informe de la firma de analistas Gartner predijo que los directores ejecutivos pronto podrían ser personalmente responsables de los ataques cibernéticos.

Los ciudadanos y los clientes quieren con razón que las empresas protejan sus datos con los más altos estándares posibles. Por tanto, es cada vez más lógico preocuparse, tanto colectiva como individualmente, de que cada uno pueda ser considerado responsable en caso de violación de datos. Pero la

prioridad número uno siempre debería ser centrarse en la protección de datos.

Conclusión

El GDPR ha tenido un gran impacto en todos nosotros y en nuestra privacidad, pero la tecnología está evolucionando más rápido que la ley y no es fácil para las empresas mapear el ecosistema digital en el que operan. Pese a esto y dentro de las herramientas disponibles para las empresas, asumir la responsabilidad y tener los planes de contingencia diseñados para tal efecto, resulta crucial.

Si se subestima, el tema de la privacidad puede representar un costo en términos de sanciones, así como un riesgo para la imagen y reputación de la empresa, provocando una pérdida de confiabilidad frente a la competencia. El GDPR reitera a todos, ya que todos procesamos y somos portadores de datos personales, que nuestra privacidad está protegida solo si estas herramientas son «reales», es decir, hechas a medida y adecuadas para el contexto.

Hace hincapié en el fondo y no en la forma, suprime listas preestablecidas de medidas de seguridad, como tal no recorta a situaciones específicas. Los formularios de divulgación y los formularios de consentimiento llenados previamente no son aceptables. Por tanto, el impacto del RGPD quiere ser una garantía para la protección de la privacidad de todos nosotros.

Leer también: ¿Cómo configurar la gobernanza multicloud? ; Informática forense, qué es, definición, significado ; El rol de la seguridad en la transformación digital ; tendencias en ciberseguridad para personas y empresas.