Protección de datos: Cómo poner la seguridad cibernética al servicio de LGPD

Ilustración: pch.vector, freepik

por: **Fernando Zamai**

La Ley General de Protección de Datos (LGPD), una especie de versión brasileña del Reglamento General Europeo de Protección de Datos (GPDR), entró en vigor el 18/9. La Ley considera datos confidenciales cualquier información que permita la identificación, directa o indirectamente, de una persona física que se encuentre viva y considera como datos personales: nombre, DNI, CPF, sexo, fecha y lugar de nacimiento, teléfono, domicilio, ubicación vía GPS, retrato. en fotografía, registros sanitarios, ingresos de tarjetas bancarias, etc.

Esto convierte a las organizaciones que operan en suelo brasileño en guardianes de esta información confidencial y la pone en la mira de una multa que puede llegar a los 50 millones de reales. En octubre, casi dos meses después de la entrada en vigor de la ley, las primeras decisiones sobre la LGPD ya estaban ganando publicidad. La Justicia ha estado considerando, principalmente, el intercambio indebido de datos y, en consecuencia, la falta de protección de los datos personales.

LGPD alcanzó a un mercado que prácticamente no estaba preparado para esta nueva realidad. En medio de la pandemia y con la creencia de que la fecha volvería a posponerse, las empresas aún están adaptando los procesos administrativos, operativos y legales. También se ha vuelto urgente un análisis en profundidad de la infraestructura de ciberseguridad para un uso efectivo de la tecnología que busca proteger la base de datos de los clientes.

Hablando de infraestructura tecnológica, la pandemia COVID-19 obligó a las empresas a poner a buena parte de sus empleados a trabajar desde casa, es decir, con acceso remoto a servidores corporativos y sin las protecciones tradicionales entregadas a las organizaciones. Esto aumentó la tasa de vulnerabilidad, lo que hizo que 2020 supere el récord de crecimiento anual de phishing, ransomware y otros riesgos cibernéticos.

La vida digital se ha vuelto más intensa y el anuncio de un ataque de ransomware puede incluso ser una cortina de humo para desviar la atención de algo que ya ha ocurrido y espera el momento adecuado para negociar inescrupulosamente el pago de "rescate" para evitar la divulgación parcial o total en entornos oscuros de los datos "secuestrados" de su cliente.

Entonces, ¿cómo puede la tecnología ayudar a las organizaciones a adaptarse a la LGPD? ¿Cómo preservar su imagen frente a los clientes, ya que, siendo los guardianes de la información, son vulnerables a los ciberataques?

La respuesta está en la infraestructura de ciberseguridad. Ha llegado el momento de realizar una revisión generalizada y en profundidad de los recursos disponibles internamente. Es necesario saber qué parte de la infraestructura de ciberseguridad está realmente en uso y qué tan efectiva es para protegerse contra los ataques. El control hoy es igual a costo, una cifra que puede ser alta dependiendo de la sanción que apliquen los jueces en las sentencias que consideren la LGPD.

Realice un Helth Check, sin cargo, de su infraestructura de ciberseguridad. Nuestro equipo de especialistas accede de forma remota a su base a través de Webex y realiza un informe en horas. Su red privada virtual (VPN) no puede exponerse. Por ello, recomendamos controles avanzados integrados con el servicio de inteligencia internacional Talos, para que no solo tenga dominio del entorno de TI que soporta datos protegidos por LGPD, sino que también cuente con un canal seguro en caso de problemas. Comuníquese con un especialista de Cisco