Guía informativa sobre Ciberseguridad

EY Law | Mayo 2022

Click para ingresar

EY Law

Como consecuencia de los ataques cibernéticos realizados recientemente en varias instituciones de Costa Rica, EY Law emite esta guía informativa sobre los temas más relevantes a tomar en consideración para garantizar la seguridad de su empresa.

Instamos a todos nuestros clientes de la región Centroamericana y el Caribe a reforzar sus medidas de seguridad y a diseñar e implementar protocolos de seguridad cibernética en función de los temas que han sido objeto de consultas recurrentes de nuestros clientes:

¿Cuáles serían las posibles implicaciones para una empresa en caso de una posible publicación de su información contenida en una Institución Pública, en este caso Hacienda en Costa Rica?

Esta respuesta está asociada a la determinación de cuál es la información que se ha secuestrado producto del Hackeo. En el peor escenario, la consecuencia sería la filtración de información sensible en el aspecto financiero de la empresa. Por ejemplo, listado de clientes, proveedores, cifras económicas (impuestos y declaraciones, pagos, costo de producto, seguros, contratos naviera,) representantes legales, correos, direcciones, informes de fiscalización, actividad, transacciones sin facturación electrónica, archivos xml., compras mensuales, DUAS, importadores, valores aduanales, compradores, gastos varios(cánones, regalías), descripciones de productos y en general el secreto de empresa que salvaguarda el interés económico que encierra para el negocio.*

¿Consecuencias directas?

Entre las consecuencias directas de una exposición de este tipo de información, encontramos disminución de la capacidad de la compañía, exposición a la competencia, riesgo reputacional, posible extorsión por parte de terceros.

* No obstante, hay que considerar que en el caso particular del Ministerio de Hacienda y otras Instituciones Públicas, lo anterior es meramente especulativo, ya que no han confirmado qué han hackeado, a quiénes y qué bases de datos específicas de la Administración Tributaria se vieron afectadas. Se había confirmado que era información referente a los históricos de Aduanas y correos electrónicos, pero hasta conocer las conclusiones del peritaje, no se puede asegurar el tipo de información afectada.

¿Debería la empresa informar a sus proveedores o socios comerciales sobre la posibilidad de haber sido víctima durante el Hackeo?

La respuesta es sí. Es recomendable que todas aquellas partes que se encuentran presentes en la cadena de servicio estén enteradas sobre el tema y sus riesgos. No obstante, debe considerarse que mientras no exista una confirmación real arrojada en los resultados del análisis forense que esté realizando la Institución sobre la información secuestrada, solamente se podrán realizar estrategias para evitar una fuga adicional y conocer el impacto y alcance del ataque, el cual es fundamental para la toma de decisiones. Es por lo anterior, que lo recomendable es que las relaciones continúen, pero siempre en alerta sobre cualquier movimiento atípico en cuentas, sistemas, bases de datos, etc. Debe hacerse la salvedad de que no se conoce la información afectada. La comunicación es clave para evitar complicaciones para todas las empresas, estos son los momentos en que cada compañía de manera individual debe protegerse para salvaguardar a las demás y sus relaciones con terceros. De esta forma, se evitan males mayores y se minimiza el riesgo de alguna afectación interna y a los consumidores de sus productos o servicios.

¿Recomiendan que nos acerquemos a los ejecutivos de los bancos donde la empresa tenga sus cuentas para asegurar que las contraseñas estén a salvo?

Sí, lo más recomendable es hablar con los personeros de los bancos y conocer los mecanismos de ciber seguridad (protocolos, seguros internacionales, alarmas de movimientos atípicos) que se están implementando para garantizar la no exposición de las cuentas. En caso de que se considere no ser suficiente, el cambio de contraseñas es posible. Sin embargo, ese cambio en este momento podría entrabar aún más los procesos aduanales ya afectados (en el caso de Costa Rica). Es por lo anterior, que resulta esencial diseñar un plan de buenas prácticas empresariales y de Ciberseguridad que complemente las relaciones con las entidades financieras.

Medidas de Ciberseguridad

Algunas de las estrategias

Software y Bases de datos

- Mantener todo el software actualizado. Realizar análisis de vulnerabilidades.
- Implementar segmentación de red y filtrado de tráfico de data.
- Remover aplicaciones no necesarias u obsoletas.
- Limitar el acceso a los recursos de red.
- Cifrar bases de datos. Podrían seudonimizarse o anonimizarse también.
- Implementar soluciones y protocolos de detección y respuesta a amenazas.
- Utilizar sistemas de prevención de pérdida de información.
- Implementar procedimientos para identificar cambios no autorizados en los sistemas de redes.
- Implementar Firewalls y proteger los Routers.
- Actualizar los sistemas de red.
- Revisar los accesos del dominio. Limitarlos.
- Capacitar sobre los usos de la Intranet.
- Autenticar los ingresos a cuentas empresariales.
- Cambiar las contraseñas periódicamente, pero de manera controlada y a solicitud de la empresa. El cambio masivo de contraseñas y de manera desorganizada podría generar desconfianza y levantar sospechas sobre todo si se ha realizado en el plazo del último mes del acto.

Personal y Hardware

- Capacitar al personal en temas sobre ciberataques- Temas de Virus (Malware en general), Ransomware y Phishing.
- Mantener un inventario actualizado de activos tecnológicos esenciales para el adecuado funcionamiento de la organización.
- Realizar respaldos de forma periódica.
- Asegurar los respaldos de la organización. Se recomienda implementar medidas físicas para proteger los servidores.

Para más información puede contactar a:


Fernando Vargas W | Socio EY Law
Fernando.Vargas.Winiker@cr.ey.com


Margarita Guido | Gerente EY Law
margarita.guido.gomez@cr.ey.com


Nadia Chaves | Gerente EY Law
Nadia.Chaves.Zuniga@cr.ey.com

EY | Construyendo un mejor mundo de negocios

EY existe para construir un mejor mundo de negocios, ayudando a crear valor a largo plazo para sus clientes, su gente y la sociedad en general, así como también para construir confianza en los mercados de capitales.

Por medio de datos y tecnología, los equipos diversos e incluyentes de EY, ubicados en más de 150 países, brindan confianza a través de la auditoría y ayudan a los clientes a crecer, transformarse y operar.

El enfoque multidisciplinario en auditoría, consultoría, legal, estrategia, impuestos y transacciones, busca que los equipos de EY puedan hacer mejores preguntas para encontrar nuevas respuestas a los asuntos complejos que actualmente enfrenta nuestro mundo.

EY se refiere a la organización global y podría referirse a una o más de las firmas miembro de Ernst & Young Global Limited, cada una de las cuales es una entidad legal independiente. Ernst & Young Global Limited, una compañía del Reino Unido limitada por garantía, no proporciona servicios a clientes. Para conocer la información sobre cómo EY recaba y utiliza los datos personales y una descripción de los derechos que tienen las personas conforme a la ley de protección de datos, ingrese a ey.com/privacy. Las firmas miembro de EY no ofrecen servicios legales en los casos en que las leyes locales lo prohíban. Para obtener mayor información acerca de nuestra organización, ingrese a ey.com.