| **Comunicado de prensa**

Respalde la información crítica para que su negocio no pierda continuidad

PROTEJA SU EMPRESA CONTRA POSIBLES CIBERATAQUES

- Compañías deben desarrollar junto con expertos, una estrategia de ciberseguridad donde identifiquen los riesgos y amenazas para implementar medidas de protección.

- Estudio de Procomer identificó que siete de cada diez empresas costarricenses (73%) ha invertido o invierte actualmente en ciberseguridad, mientras que las restantes no lo han hecho nunca.

Costa Rica, 03 de febrero de 2023.

Las empresas costarricenses tienen oportunidades de mejora en materia de protección de información, ya que una gran parte de ellas invierte principalmente en lo básico, mientras otras del todo no asignan recursos e incluso algunas no saben qué es la Ciberseguridad.

Según el informe de la Promotora de Comercio Exterior (Procomer) "*Caracterización del uso y necesidades potenciales de ciberseguridad en empresas costarricenses"*, en 2020 en Costa Rica se detectaron unos 201 millones de ciberataques, especialmente de *Phishing* y algunos nuevos tipos de intentos de hackeo basados en Inteligencia Artificial (IA) y en el Internet de las Cosas (loT). Se estima que cada 10 segundos se registran pérdidas de casi USD$2 millones y en una hora hay casi 23.000 ataques a empresas e instituciones del país.

Para estas compañías que aún no conocen las consecuencias negativas que puede haber si son vulneradas, Grupo EULEN Costa Rica -empresa que brinda servicios de *ethical hacking* y vulnerabilidades, vigilancia digital y gestión de la ciberseguridad y continuidad- ofrece algunas sugerencias para blindar la información crítica.

Lo primero que se debe entender es que la información es el principal activo; por lo tanto, para mayor orden, se debe clasificar en pública, privada y confidencial, estas dos últimas muy buscadas por los *hackers*, ya que -dependiendo de la empresa- pueden incluir datos financieros o sensibles, contratos legales, bases de datos, información comercial, entre otros.

Por eso, para prevenir posibles amenazas, Fernando Gamboa, Jefe Comercial de Grupo EULEN Costa Rica, recomienda a las empresas lo siguiente:

- Identificar cuál es la información más importante de la empresa.
- Una vez identificada, se debe tener un respaldo en una nube que sea reconocida y cuente con certificaciones de alta seguridad.
- Los respaldos se deben hacer -automáticamente- cada cierto tiempo, para que, en caso de sufrir un robo de información, el negocio no se paralice y la reanudación sea en el menor tiempo posible.
- Manejar la información de los clientes bajo contratos de confidencialidad para ambas partes.
- Constante cambio de contraseñas en los principales servidores y contar con VPN's (redes privadas) para las personas que trabajan desde sus casas o lugares con conexión pública.
- Control de acceso adecuado donde se identifiquen las personas que manipulan esta información.

- Un buen proceso de reclutamiento del personal a cargo y lograr una continuidad en los colaboradores para evitar la rotación constante.
- Contar con una estrategia en ciberseguridad que integre posibles escenarios y acciones de respuestas inmediatas.

“Los *hackers* ambicionan estas informaciones para distintos fines, por ejemplo: para divertirse, mostrar vulnerabilidades, trabar el accionar de una empresa o extorsionar por dinero a cambio. Es por eso, que todas las empresas deben contar con un plan de contingencia para evitar que, en caso de ser robada la información, el negocio se pierda”, agrega el experto.

Plan de recuperación de negocio

En el comercio, es muy dado a que se dé el espionaje industrial, una práctica en la que, por medio de un *hacker*, una empresa consigue información sensible de la competencia. Este hecho ilícito es muy común, por lo que se aconseja a las compañías que cuenten con un plan de recuperación de negocio, que permita la reincorporación a las actividades en el menor tiempo posible.

“Al elaborar un plan de recuperación de negocios, se debe hacer un análisis de riesgos, identificar posibles amenazas y conocer cuáles serán las medidas de protección que se deben implementar según el caso presentado. Se debe tener un estimado de tiempo de cuánto puede tomar la empresa en volver a funcionar con normalidad y trabajar un protocolo pensado en los clientes”, finalizó Gamboa.

Tras existir una gran cantidad de ciberataques, en Costa Rica existe la Agencia de Protección de Datos de los Habitantes (Prodhab), cuyo objetivo principal es garantizar a cualquier persona el respeto del correcto uso de sus datos privados. Asimismo, orienta al ciudadano a ejercitar sus derechos y a las entidades públicas y privadas que manejan bases de datos, a cumplir con las obligaciones que establece la Ley N.°8968, de Protección de la Persona frente al Tratamiento de sus Datos Personales.

Para más información:

José Araya
jose.araya@upgradecomunicacion.com
http://www.upgradecomunicacion.com
Tfn. +506 2506-3882 / +506 8886-7470.
Upgrade Comunicación

Flor Monestel
flor.monestel@upgradecomunicacion.com
http://www.upgradecomunicacion.com
Tfn. +506 2506-3882 / +506 8873-2412.
Upgrade Comunicación