Ciberdelincuentes buscan la mayor afectación a sus víctimas

# PROTOCOLOS DE SEGURIDAD MINIMIZAN IMPACTOS ANTE UN CIBERATAQUE

— Un plan integral debe incluir medidas de seguridad tradicional y ciberseguridad, que protejan mercancías e información sensible.

**Costa Rica, 18 de mayo de 2022.**

A raíz de los ataques cibernéticos sufridos en días recientes en diferentes instituciones de Gobierno, programas de importaciones y exportaciones e incluso plataformas de envíos y entregas de mercancías, es importante contar con mecanismos de ciberseguridad para proteger la información sensible, sea personal o empresarial, y seguridad física para el control de las mercancías y bienes, incluyendo su logística, tráfico, entrega, entre otros.

Las empresas, al ver impactadas sus exportaciones e importaciones, acumulan mercancía en bodegas y almacenes, afectando sus inventarios; por eso, se recomienda que tomen medidas de seguridad. Lo primero es revisar y analizar la red interna de cada empresa donde se encuentra almacenada toda la información acerca de los bienes y/o mercancías que tienen en inventarios, almacenadas o en tránsito. Lo segundo es reforzar la seguridad física de las instalaciones donde se almacene esta mercancía, ya que, al tener mayor cantidad de ésta por el paro en las importaciones y exportaciones, mayor es el riesgo de sufrir un ataque criminal de otro tipo, como robo o asalto.

“Uno de los objetivos de los ciberdelincuentes cuando efectúan un ciberataque es buscar el mayor impacto para la empresa o gobierno que es víctima, teniendo como fin extorsiones económicas a cambio de la devolución de la información secuestrada. En el caso de Costa Rica, uno de los impactos del ataque lo recibió el sistema donde se hacen las declaraciones aduaneras en línea (Tica). Esto afecta directamente las importaciones y exportaciones del país, y de las empresas”, explica Fernando Gamboa, asesor Ejecutivo de Grupo EULEN Costa Rica.

En el caso de las personas que realizan compras por plataformas digitales la recomendación es guardar los tiquetes de pago en línea, el número de referencia de la mercancía y estar en contacto constante con el proveedor, esperar a que el servicio vuelva a su normalidad y reclamar su mercancía.

El experto indica que dentro de la información sensible que empresas, instituciones y personas pueden ver vulnerada están las direcciones físicas, correos electrónicos, números de cuentas, depósitos bancarios, salarios, contratos comerciales y laborales, información médica, antecedentes de investigaciones administrativas o de otra índole, claves de seguridad, declaraciones fiscales o bancarias y otra información con valor sensible, permitiendo elaborar perfiles con información que no se considera pública.

“Recuperar o no los datos, va a depender de las medidas de ciberseguridad que mantengan las víctimas. Si hay respaldos de información adecuados, frecuentes y protegidos sí existe la posibilidad de rescatarlos, de lo contrario, entraría en juego la negociación con los delincuentes para recuperarlos o verse afectados por la no recuperación. Ante esta realidad, es vital contar con un plan de continuidad de negocio, donde se analicen, estudien y evalúen los riesgos de ciberseguridad y establezcan los procedimientos y protocolos de prevención de ataques o de reanudación de las actividades de la empresa luego de un ciberataque”, agregó Gamboa.

Un aspecto a considerar es que muchos de los datos secuestrados son ofrecidos y vendidos en la Deep Web. Esta web mantiene un 96% de la información de Internet global, a diferencia de la web visible; además, el anonimato y la libertad de expresión hacen que sea una red para la delincuencia en línea. El precio de la información que el ciberdelincuente le da a la información es acordado según el nivel de sensibilidad o privacidad de esta y el grado de afectación, ya sea operacional o de reputación para el gobierno o la empresa.

## Protocolos de seguridad: tradicional y en línea

Un plan de continuidad de negocios debe analizar dos escenarios: antes de sufrir un ataque (prevención) y la recuperación de desastres (atenuar efectos de un ataque y reanudar las operaciones normales de la empresa o gobierno). En el primero, se toma en cuenta la identificación de amenazas y procesos críticos de la empresa, se identifican y evalúan riesgos y se implementan medidas para no ser una futura víctima de los ciberdelincuentes, por ejemplo: protección a la red y sistemas de la empresa, almacenamiento seguro de información confidencial, políticas de uso de equipos, evaluaciones y simulacros, entre otros. Todo ciberataque tiene como elemento común; el error humano, al aceptar correos maliciosos o usar claves y correos en sitios web de alto riesgo, por lo que una campaña de sensibilización ciberseguridad a lo interno del personal es relevante.

Para la recuperación de desastres se debe identificar la información vital para la continuidad del negocio (ejemplo planillas, inventarios, información comercial) y definen la frecuencia y cantidad de respaldos para esta información sensible y donde se almacena, ya que, en caso de un ataque, la reanudación de las actividades vitales del negocio será más fácil. En este plan se mide el impacto económico para la empresa en caso de sufrir un ataque (se mide en el escenario más crítico imaginado), con el fin de determinar la estrategia de seguridad y sus acciones, y el presupuesto para ejecutarlo de cara a futuros ciberataques.

Finalmente, hay acciones para la protección de datos que pueden considerarse básicas, pero en realidad son determinantes a la hora de salvaguardar la información, entre ellas:

- Identificar la información y los datos que la empresa desea proteger por ser críticos, esto basado en el análisis de riesgos.
- Aplicar las medidas de protección de seguridad física (ubicación de los servidores principales, identificar personal con acceso a ellos y controlar el acceso), alarmas, controles biométricos o con tarjeta.
- Ciberseguridad: políticas de asignación de claves, equipos de cómputo, acceso a la red interna de la empresa, VPN para trabajar fuera de la empresa, uso de correos y un plan agresivo de sensibilización para el personal.

“La ciberseguridad no es al azar. Para estar seguros, se debe invertir en un plan integral que ayude a minimizar este tipo de ataques, porque estos eventos suelen tener impactos muy grandes para las empresas y personas”, detalló Gamboa.

---

EULEN Seguridad, lleva en Costa Rica 20 años al servicio de sus clientes con la misma vocación que al inicio de su actividad. Como empresa innovadora y flexible, se adapta a los nuevos escenarios y riesgos comprometiéndose para conseguir la excelencia en la prestación de servicios. EULEN Seguridad está especializada en vigilancia, soluciones de sistemas de seguridad, consultoría, Unidad de Inteligencia, aerovigilancia, transporte de fondos, Centro de Control de Seguridad Integral, Protección de infraestructuras críticas y seguridad integrada.

EULEN Seguridad tiene más de 45 años de trayectoria en España y es una empresa del Grupo EULEN, fundado en 1962 en Bilbao. La compañía está presente en 14 países y el volumen de ventas anuales supera los 1.600 millones de euros, con una plantilla global de más de 90 000 personas. En Costa Rica se desempeña como auxiliar de la Fuerza Pública y las policías municipales, según lo estipula la Ley de Servicios de Seguridad Privados (8395). Desde este rol estratégico EULEN Seguridad aporta las herramientas técnicas y el recurso humano experto para contribuir con los objetivos del Ministerio de Seguridad Pública.

**Para más información:**

Flor Monestel
flor.monestel@upgradecomunicacion.com
http://www.upgradecomunicacion.com

Tfn. +506 2506-3882 / +506 8873-2412.
Upgrade Comunicación