|Comunicado de prensa

Según estudio, en Costa Rica el 48,5% de personas realizan compras por un medio electrónico

MEDIDAS DE SEGURIDAD QUE DEBEN IMPLEMENTARSE EN E-COMMERCE EN TEMPORADA ALTA

- Es fundamental que hagan monitoreos de ataques o pentesting a sus sistemas informáticos internos.

Costa Rica, 25 de noviembre de 2022

De cara a una de las épocas del año más esperadas por muchas personas -donde los comercios ofrecen ofertas especiales y descuentos- hace que los consumidores no puedan dejar pasar por alto estas oportunidades y compren los regalos de navidad para sus seres queridos en cualquier tipo de tienda; ya sea físicas o en línea, sin tomar en cuenta muchos aspectos de seguridad.

Es por esta razón que, Grupo EULEN Costa Rica - empresa que brinda servicios de ethical hacking y vulnerabilidades, vigilancia digital, gestión de la ciberseguridad y continuidad- hace un llamado a las empresas a que inviertan en sistemas de protección para asegurar la identidad de sus clientes y detectar vulnerabilidades que pueden ser aprovechadas por hackers maliciosos y ejecuten un secuestro de datos estratégicos.

De acuerdo a un estudio que realizó el Centro de Investigación Observatorio del Desarrollo (CIOdD), de la Universidad de Costa Rica (UCR), las personas que realizan compras por un medio electrónico en Costa Rica, representan el 48,5% de la población. Donde el medio favorito para hacer estas compras es el celular (65,3%), seguido de la computadora (32,8%) y por último la tableta (1,8%).

"Las empresas deben tener un protocolo muy riguroso en temas de ciberseguridad. Como sistemas actualizados libres de virus; concientización en los empleados sobre la correcta utilización de los sistemas corporativos; utilizar redes seguras para comunicarse con los clientes; incoportación de VPN's; incluir la información de los compradores en los análisis de riesgos anuales y realizar cambios de contraseñas periódicas", explicó Fernando Gamboa, asesor Ejecutivo de Grupo EULEN Costa Rica.

Está claro que los comercios deben manejar los datos sensibles de los clientes de manera correcta y segura. Por eso, como principales medidas de seguridad para garantizar la protección de estos datos, las compañías deben manejar -como mínimo- de dos a tres respaldos de la información privada; ya sea en fuera de la empresa o en una nube informática.

"Además, cada colaborador debe ser muy cuidadoso con el manejo de la información y ser conciente de la responsabilidad que tiene; ya que un gran porcentaje de los hackeos son producidos por descuidos o errores humanos", añadió Gamboa.

También, las personas que tienen accesos a este tipo de data, se deben identificar cada vez que tengan acceso, contar con una red segura y privada es vital y muy importante que los colaboradores no utilicen los equipos del trabajo para fines personales.

Realizar pentesting cada cierto tiempo. Es decir, provocar ataques al propio sistema informático con la intención de encontrar debilidades de seguridad y todo lo que podría tener acceso a ella, y en caso de topar con algún problema, se corrije con un "parche" y así se evita un posible hackeo. Para esto se recomienda invertir en un proveedor de ciberseguridad para que se adelante a cualquier oportunidad que exista de robar información.

Estas medidas son necesarias acatarlas para que las empresas anticipen posibles ataques, tomando en cuenta que dentro de las principales estrategias de los hackers está la suplantación de identidad, el *phishing* por correo electrónico y ahora por mensajería SMS, robo de tarjetas de crédito y el *ransomware* o también conocido como el secuestro de datos a cambio de dinero.

Por último, el experto indica una serie de señales que son claves para reconocer que un sitio web no es muy seguro:

- Recibir publicidad agresiva o *pop-ups* insistentes de una empresa.
- Recibir solicitudes de información inesperada o sospechosa. Un sitio web seguro nunca pedirá datos personales o información sensible sin sentido, y de manera recurrente.
- Visualizar el URL de la página y verificar si aparece el candado de seguridad en la barra de dirección.
- Recibir anuncios con errores gramaticales o faltas de ortografía muy evidentes, o prometiendo descuentos imposibles y remedios milagrosos.
- Solicitudes de datos personales, como estados de cuenta, números de PIN o contraseñas.

Para más información:
José Pablo Araya
jose.araya@upgradecomunicacion.com
http://www.upgradecomunicacion.com
Tfn. 506 8886-7470
Upgrade Comunicación