Estas acciones blindan sus ventas y aseguran datos de usuarios

COMERCIO ELECTRÓNICO DEBE FIJAR MEDIDAS BÁSICAS DE SEGURIDAD EN TEMPORADA DE COMPRAS

— Es fundamental que hagan auditorías de ataques o *pentesting* a sus sistemas informáticos internos.

Panamá, 24 de noviembre de 2022.

El protagonismo que tuvo el comercio electrónico o e-commerce en los dos primeros años de la pandemia del COVID-19, continúa en este 2022 y se prevé que continuará por un largo tiempo.

De acuerdo con el Digital Report 2022 "El Informe sobre las Tendencias Digitales, Redes Sociales y Mobile", en el mundo 6 de cada 10 usuarios de Internet en edad laboral compran en línea todas las semanas.

Esta tendencia motivó a muchas empresas -pequeñas, medianas y grandes- en varios países del mundo, incluyendo Panamá, a crear plataformas de E-Commerce para poner sus productos o servicios al alcance de los consumidores.

Más allá de la facilidad que le genera a los compradores y el incremento en las ventas que le representa a las empresas, estas deben reforzar la seguridad en estas plataformas para evitar ser presas fáciles de los ciberdelincuentes, sobre todo en temporada de compras de fin de año.

Según Antonio Pérez Díaz, durante esta época en que se realizan muchas compras en línea lo recomendable es que las empresas fijen medidas básicas de seguridad, por ejemplo, mantener los sistemas actualizados libres de virus y vulnerabilidades; concientizar a los empleados sobre la correcta utilización de los sistemas corporativos; utilizar redes seguras para comunicarse con los clientes; incluir la información de los compradores en los análisis de riesgos anuales; realizar copias de seguridad periódicas; entre otro aspectos de ciberseguridad.

"El no prestar suficiente atención a los sistemas de seguridad y a las barreras de seguridad, el no realizar actualizaciones continuamente ni auditorías a los sistemas, o el no revisar las configuraciones de seguridad y privacidad de los equipos con regularidad, les facilita el camino a los ciberdelincuentes. Por eso, se recomienda a las empresas que revisen sus banners de cookies, para confirmar que son los suyos y que no están siendo utilizados por los ciberdelincuentes para redirigir a los clientes o usuarios hacia sitios fraudulentos de robos de datos", indica Antonio Pérez Díaz, gerente general de Grupo EULEN Panamá.

Para el gerente de Grupo EULEN Panamá -empresa que brinda servicios de *ethical hacking* y vulnerabilidades, vigilancia digital y gestión de la ciberseguridad y continuidad-, es fundamental que las empresas hagan auditorías de ataques o *pentesting* -test de penetración que consiste en atacar diferentes entornos o sistemas con el objetivo de detectar y prevenir posibles fallos- a sus sistemas informáticos internos.

Igualmente recomienda a las empresas buscar la personalización de la experiencia de compra, adaptándola al perfil exacto de los clientes, analizando los perfiles de riesgo y el grado de exposición; de manera tal que puedan detectar más fácilmente a los

compradores que usan perfiles falsos para cometer fraudes y ataques a los sistemas que comprometan el negocio y su reputación.

Por otro lado, las compañías deben manejar los datos sensibles de forma correcta. Esto quiere decir que aquellos datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los datos genéticos, los datos biométricos tratados únicamente para identificar a un ser humano, los datos relativos a la salud, la orientación sexual de una persona o de índole económico, deben estar celosamente custodiados.

Finalmente, 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.

Para más información:
Melissa Novoa Tfn. 507 6090-2967
melissa@upgradecomunicacion.com Upgrade Comunicación
http://www.upgradecomunicacion.com