5 pasos de seguridad que el *retail* debe seguir en el Hot Sale

CIUDAD DE MÉXICO. 22 de mayo de 2023.- El comercio electrónico en el país ha tenido un crecimiento sin precedentes durante los últimos años. Tan solo durante 2022, las operaciones *online* en México para los comercios de *retail* alcanzaron $528.1 mil millones de pesos, experimentando un crecimiento del 23% de acuerdo con la AMVO.

Eso significa que hoy en día el comercio electrónico es una excelente oportunidad para los comercios de trasladar sus ventas al plano digital y elevar sus ingresos, crecer su fidelidad y ganar mucho más dinero. Pero también implica un alto riesgo en materia de ciberseguridad, con los ciberdelincuentes volviéndose cada vez más sofisticados y peligrosos en sus ataques.

Épocas como el Hot Sale, que este año se llevará a cabo del 29 de mayo al 6 de junio, se caracterizan por tener un alto índice de cibercrimen, ya que representan para los entes maliciosos una oportunidad muy grande de vulnerar y robar información para engañar a los consumidores, dado el alto interés por comprar que estas temporalidades generan.

Un ejemplo es lo sucedido en el mercado de Estados Unidos, en el que de acuerdo con un estudio de Sift los casos de cibercrimen se incrementan en un 61.5% durante el Black Friday y el Cyber Monday. En el caso del Hot Sale, los criminales saben que este evento, según la AMVO, genera más de 560 millones de visitantes a los sitios web de los comercios participantes, lo cual es sumamente atractivo para ellos.

Desde la perspectiva de Strike, las siguientes son las principales medidas de ciberseguridad que las empresas de *retail* deben seguir para cuidar su información y proteger sus sistemas durante el Hot Sale 2023, para evitar pérdidas por el cibercrimen y conseguir el éxito:

1. Evaluación de vulnerabilidades mediante *pentesting*: El *pentesting* es una técnica de seguridad que implica la evaluación activa de sistemas, aplicaciones y redes para identificar vulnerabilidades y determinar si pueden ser explotadas por atacantes externos.

Las empresas del sector *retail* deben realizar pruebas de *pentesting* previas al evento para identificar posibles vulnerabilidades en su infraestructura y sistemas. De ese modo, en lugar de ofrecer un sitio desprotegido a sus consumidores, podrán ‘cerrar ‘ esas puertas antes de que las encuentren los cibercriminales y tener una plataforma de ventas online segura.

2. Actualización de *software* y parches de seguridad: Los sistemas y aplicaciones desactualizados pueden ser una puerta de entrada para los *hackers*. Por lo tanto, las empresas deben asegurarse de mantener sus sistemas, aplicaciones y dispositivos al día con las últimas actualizaciones y parches de seguridad.

Para ello es importante acudir con especialistas en ciberseguridad que presenten soluciones enfocadas en atender las necesidades de la empresa, y no que ofrezcan la misma herramienta para todos sus clientes. Un asesoramiento puntual y la ayuda de *hackers* éticos en el proceso de detección de vulnerabilidades será la clave para que esas actualizaciones se lleven a cabo correctamente.

3. Configuración de *firewalls* y filtros de contenido: Un *firewall* es un sistema de seguridad que controla el tráfico de datos que entra y sale de una red, utilizando reglas y políticas de seguridad específicas para permitir o denegar el acceso al sistema por parte de usuarios no autorizados.

Las empresas deben configurar sus *firewalls* y filtros de contenido para estas temporalidades en las que el tráfico de usuarios se incrementa notablemente y alcanza niveles que no se ven en otras épocas del año, para proteger su infraestructura de posibles ataques de *malware* y *phishing*.

4. Entrenamiento de concientización en seguridad cibernética para empleados: Las empresas deben ofrecer a sus empleados un entrenamiento de concientización en seguridad cibernética, para educarlos sobre las amenazas informáticas y cómo protegerse de ellas. Esto incluye la identificación de correos electrónicos de *phishing* y la importancia de la autenticación multifactor.

5. Análisis de registros: Las empresas deben monitorear la actividad en su red en tiempo real y analizar los registros para detectar posibles actividades sospechosas.

Esto debido a que las estrategias de protección de datos implementadas al inicio del evento, pueden no ser suficientes conforme avanzan los días del Hot Sale tomando en cuenta lo rápido que evolucionan los cibercriminales en sus ataques.

El Hot Sale es una época en la que compran más de 12 millones de mexicanos debido a las ofertas y descuentos que encuentran. Pero también es un momento clave para los comercios ya que los precios bajos no son suficientes si no se tiene una plataforma segura. Ofrecer un sitio inseguro y una experiencia poco confiable, puede ser el parteaguas para perder la lealtad del consumidor, para quien la ciberseguridad y la protección de su información hoy en día es prioridad.

Sobre Strike

Strike es la plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas. Esto se realiza a través de tests de penetración - o pentests - llevados a cabo por su red global de hackers éticos, conocidos como “Strikers”, una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo estanco o independiente. Más información en: https://strike.sh/

Síguenos en nuestras redes sociales:
Instagram - @strikesecurity
Twitter - @strike_secure
LinkedIn - Strike

Contacto para prensa México
another
Ahtziri Rangel | PR Expert
+ 52 1 55 1395 6970
ahtziri.rangel@another.co