

C Columna **El "clásico" de la ciberseguridad**



Por Arturo Torres.
 FortiGuard Labs..

En unos meses Canadá, México y Estados Unidos se convertirán en los epicentros de la pasión futbolística mundial. Sin embargo, mientras las selecciones afinan sus tácticas y los aficionados preparan sus camisetas, hay otro partido que ya ha comenzado a jugarse de manera silenciosa, veloz y constante: el clásico de la ciberseguridad.

Un evento de esta magnitud es para los ciberatacantes, lo que para los jugadores sería el llegar a la final: una oportunidad máxima de éxito. En este 2026, el panorama digital en la región se encuentra en un punto donde la innovación tecnológica y la prevención de fraudes serán factores de gran importancia.

Cuando hablamos del Mundial, pensamos en goles, festejos y turismo, pero desde una perspectiva de ciberseguridad, este hito es una inmensa red de datos. Cada aficionado que entre a un estadio llevará consigo un dispositivo móvil, consumirá datos, realizará pagos electrónicos y buscará redes Wi-Fi para compartir su experiencia. Esta hiperconectividad es una maravilla de la innovación, pero también expande la posible superficie de ataque a través de fraudes y estafas.

Los ciberatacantes son oportunistas y utilizan la inge-

niería social, buscando engañar a las personas apelando a sus emociones y ¿qué emoción podría ser más fuerte para un fanático que el deseo de formar parte de algún partido entre sus equipos favoritos?

Uno de los fraudes más comunes será el phishing temático a través de correos electrónicos o mensajes de WhatsApp con ofertas increíbles de boletos o paquetes de viaje VIP. Estos mensajes, hoy potenciados por la inteligencia artificial (IA), carecen de errores ortográficos y utilizan logotipos e imágenes que son realmente similares a los oficiales con el objetivo de que, en la emoción del momento, el usuario haga clic en un enlace malicioso y entregue sus datos bancarios o sus contraseñas.

También veremos el auge de las estafas de transmisiones en vivo. Los aficionados que no puedan asistir al estadio buscarán opciones para ver los partidos en línea y aparecerán diversos sitios web que ofrecen streaming gratuito a cambio de descargar un pequeño archivo o registrarse con una tarjeta de crédito solo para verificación. En la mayoría de los casos, lo que el usuario está descargando es un virus que tomará control de su dispositivo.

Para el sector empresarial,

este evento deportivo representa una oportunidad de oro, pero también una importante responsabilidad. Desde las grandes cadenas hoteleras hasta los pequeños comercios que aceptarán pagos digitales, todos son parte de la cadena de suministro del país. Una empresa que sufre un ciberataque durante el torneo no solo pierde dinero o datos, sino que pierde la confianza de un mercado internacional que nos está observando.

En este sentido, la implementación de soluciones tecnológicas avanzadas ya no es un lujo. Las empresas deben entender que el cibercrimen hoy es una industria automatizada. Por ello, la respuesta debe ser igualmente tecnológica a través del uso de IA o sistemas unificados en la nube para la detección de amenazas, teniendo una integración total que proteja desde la computadora de la oficina hasta el teléfono móvil del empleado que trabaja vía remota.

Las inversiones en tecnología y ciberseguridad durante este periodo estarán contribuyendo a la creación de un ecosistema digital robusto que atraerán más inversiones incluso después del Mundial.