Juegos online, en alerta por ciberataques

Los usuarios de **juegos online quieren disfrutar de descargas rápidas y divertirse sin interrupciones**. Para satisfacer estas expectativas, los proveedores del contenido tienen que hacer frente a una gran cantidad de desafíos técnicos. Akamai ayuda a los usuarios en tener experiencias seguras en el sector del juego.

Hugo Werner, vicepresidente Regional de Akamai Latinoamérica, asegura que cada día las empresas de **juegos online se exponen a nuevas amenazas y vulnerabilidades**, como las interrupciones por ataques Distribuidos de Denegación de Servicio (DDoS) y otros tipos de ciberataques.

“Los recientes ataques de mayor resonancia son sólo los más conocidos, pero se producen incontables incidentes que no trascienden. Por desgracia, pueden producirse ciberataques contra cualquiera, no solo contra grandes empresas, y suelen resultar más costosos de lo que en un principio se piensa”, explica.

Es posible que el mayor costo para una empresa no sea el económico, pero, de todos modos, puede ser devastador. De hecho, **las empresas identificaban el daño a su reputación** como la peor consecuencia de los ciberataques.

Werner agrega que en un sector intensamente competitivo como el de los juegos online, donde la marca es fundamental y la experiencia del usuario es primordial, las interrupciones del servicio debidas a ataques DDoS pueden resultar especialmente nocivas.

“Para los jugadores, cada milisegundo cuenta y un ataque solo necesita ralentizar un servidor, no sobrecargarlo totalmente, para hacer estragos en la experiencia de juego. Por desgracia, los atacantes necesitan recursos mínimos para infligir estos tipos de daños”, agrega.

Es posible **alquilar botnets DDoS por unos pocos dólares a la hora**, y perpetrar ataques constantes. Al contrario que en los sectores financiero, salud o retail, a los ciberatacantes del sector de los juegos a menudo no les motiva el dinero, sino que sencillamente se trata de jugadores descontentos que buscan sus 15 minutos de fama o sacar ventaja a sus rivales. Aun así, los ataques pueden causar daños importantes, ya que las interrupciones del servicio que producen frustran a los jugadores existentes y alejan a los potenciales.

Riesgos

Los riesgos aumentan más todavía durante los eventos a gran escala, como los lanzamientos de nuevos títulos y los torneos de deportes electrónicos. Las interrupciones no solo dañan la reputación, sino que también echan a perder millones de dólares de inversión en marketing y promociones.

Debido a la escala y la complejidad de las ciberamenazas a las que se enfrenta el sector, las empresas de juegos adoptan, cada vez más, la práctica recomendada de **utilizar defensas**

distribuidas en la nube para proteger sus activos y sus servicios online. Para las empresas que ya emplean una infraestructura en la Nube, las defensas basadas en este entorno son la opción más natural.

Un sistema de ciberdefensa basado en la nube (ya sea independiente o complemente una solución local) permite a las empresas reducir el gasto de capital y el gasto operativo en materia de seguridad. Asimismo, dado el mayor tamaño, duración y frecuencia de los ciberataques, las defensas distribuidas en la nube son la mejor y, a veces, la única manera de neutralizar las amenazas y de minimizar las interrupciones para los jugadores legítimos.

Aun así, no todas las **defensas en la Nube** son iguales. Muchos servicios no disponen de **capacidad para gestionar los ataques más grandes a nivel de internet** e incluso pueden limitar contractualmente el tamaño de los ataques contra los que ofrecen protección. Cuando los proveedores citan una cifra de capacidad de red, ese número no refleja el tamaño del ataque DDoS que son capaces de gestionar correctamente.

Por lo general, el tráfico legítimo consume gran parte de la capacidad de una red, y el resto de la capacidad se reparte entre varios centros de datos. Si la tolerancia a los fallos y la resistencia no se integran en el sistema de manera inteligente, un número relativamente pequeño de ataques DDoS regionales puede bloquear fácilmente un centro de datos o región, lo que podría provocar la interrupción del servicio para los usuarios finales.

Las mejores soluciones proporcionan varios perímetros de defensa que se integran para supervisar y ofrecer protección proactiva contra una amplia variedad de amenazas.