24

Cómo afectan los ciberataques en los momentos de gran consumo

En los últimos años, los ciberataques se han convertido en uno de los mayores riesgos para las empresas, especialmente durante periodos de gran consumo como el Black Friday, Navidad o el inicio de rebajas, cuando el volumen de transacciones digitales se dispara. Estos picos de actividad representan un momento de vulnerabilidad crítica: los sistemas están más saturados, los equipos técnicos bajo presión y los ciberdelincuentes aprovechan el incremento de operaciones para lanzar ataques cada vez más sofisticados.

EL AUMENTO DE LOS CIBERATAQUES EN TEMPORADAS CLAVE

Estudios recientes revelan que en eventos de gran consumo la actividad maliciosa crece de forma notable. En noviembre de 2023, por ejemplo, se registró el mayor nivel de ciberdelincuencia del año, impulsado por el Black Friday y la cercanía de las festividades navideñas. Se estima que durante este tipo de periodos los ataques podrían crecer hasta un 20% adicional en 2024, lo que convierte al comercio electrónico en un blanco privilegiado.

La temporada de verano también muestra incrementos significativos, debido a la reducción de personal y la relajación de controles. Howden Iberia se ha documentado aumentos de hasta un 30% en incidentes durante estas fechas. El caso del fallo en la actualización de CrowdStrike, que afectó a sistemas de Microsoft y provocó cancelaciones de vuelos y pérdidas millonarias, evidenció la fragilidad del ecosistema digital.

EL RESURGIMIENTO DEL RANSOMWARE Y EL RIESGO REPUTACIONAL

El ransomware continúa posicionándose como una de las amenazas más persistentes y disruptivas dentro del ecosistema digital. Su evolución ha superado el mero cifrado de información: actualmente, los atacantes también exfiltran datos sensibles con el propósito de extorsionar a las organizaciones mediante la amenaza de divulgación pública.

Esta modalidad dual —cifrado y filtración— incrementa de forma significativa tanto el riesgo económico como el impacto reputacional, especialmente cuando las brechas se producen en momentos clave del calendario comercial. En estos casos, la pérdida de confianza por parte de clientes y socios puede traducirse en una caída sustancial de ingresos, además de posibles sanciones regulatorias.

Además, los ciberdelincuentes muestran un alto grado de profesionalización. La fragmentación de grupos, la colaboración entre actores maliciosos y el respaldo —explícito o implícito— de ciertos Estados hostiles han contribuido a elevar significativamente el nivel técnico y estratégico de las operaciones. Esta transformación ha dado lugar a estructuras más ágiles, coordinadas y difíciles de rastrear, capaces de ejecutar ataques complejos con precisión y rapidez.

CIBERATAQUES CON MOTIVACIÓN POLÍTICA

Más allá del objetivo meramente económico, cerca del 90% de los ciberataques registrados entre abril de 2023 y marzo de 2024 tuvieron motivaciones políticas, según un análisis de Howden basado en datos del CSIS. En un entorno de inestabilidad geopolítica, como las guerras en Ucrania y Oriente Medio o los intentos de manipulación en procesos electorales, los ataques a infraestructuras críticas y empresas privadas se han convertido en un campo de batalla digital.

Patricia Fernández Ramos
Directora de Cyber en Howden Iberia

LA IRRUPCIÓN DE LA INTELIGENCIA ARTIFICIAL GENERATIVA

La inteligencia artificial generativa está transformando profundamente el panorama de la ciberseguridad. Por un lado, esta tecnología democratiza el acceso a herramientas sofisticadas, permitiendo que actores con escasa experiencia técnica lleven a cabo actividades maliciosas con mayor facilidad. Por otro, habilita a grupos organizados para ejecutar ataques más rápidos, precisos y dirigidos contra infraestructuras críticas o activos de alto valor. Incluso actores estatales, respaldados por gobiernos, están incorporando estas capacidades para perfeccionar sus estrategias ofensivas.

No obstante, la IA generativa también está siendo aprovechada en el ámbito defensivo. Soluciones avanzadas de detección, análisis y respuesta ante incidentes están reforzando la resiliencia de las organizaciones, permitiéndoles anticiparse a las amenazas y responder con mayor eficacia ante posibles compromisos de seguridad.

EL PAPEL DEL CIBERSEGURO EN LA RESILIENCIA EMPRESARIAL

En un entorno marcado por amenazas digitales cada vez más sofisticadas, el ciberseguro se ha consolidado como un componente esencial dentro de las estrategias de gestión de riesgos. De acuerdo con el cuarto informe anual de Cyber elaborado por Howden, nunca antes se había observado una convergencia tan intensa de riesgos cibernéticos junto con un mercado asegurador estable y en expansión.

Más allá de la compensación económica tras un incidente, el ciberseguro desempeña un papel proactivo: promueve la adopción de buenas prácticas en ciberseguridad, incentiva la inversión en controles preventivos y fortalece la capacidad de respuesta ante eventos disruptivos. Sectores altamente expuestos como el financiero, sanitario, retail e industrial lideran la demanda de este tipo de cobertura, conscientes de su papel crítico en la continuidad operativa y la protección de activos digitales.

IMPACTO ECONÓMICO Y NECESIDAD DE PREPARACIÓN

Los ciberataques durante periodos de alta demanda, como el Black Friday o la campaña navideña, representan una amenaza creciente que combina oportunismo, sofisticación tecnológica y, en algunos casos, motivaciones geopolíticas. Las consecuencias pueden ser devastadoras: desde la interrupción de sistemas y cancelación de operaciones hasta pérdidas económicas significativas y daños reputacionales irreversibles.

Ante este escenario, el desafío para las organizaciones no se limita a la prevención. La capacidad de reacción rápida y eficaz ante un incidente se ha convertido en un factor crítico de supervivencia en la economía digital.

Entre las medidas más efectivas para mitigar el impacto de estos ataques destacan:

- La implementación de sistemas avanzados de detección y respuesta.
- El mantenimiento de protocolos robustos de copia de seguridad y recuperación.
- La formación continua del personal en buenas prácticas digitales.
- El refuerzo de mecanismos de autenticación y la segmentación de redes.
- La integración de planes de continuidad de negocio respaldados por ciberseguros.

En este contexto, el ciberseguro ha evolucionado de ser una herramienta de transferencia de riesgo a convertirse en un aliado estratégico. Su papel no solo es compensar económicamente tras un incidente, sino también elevar el nivel de preparación y resiliencia de las organizaciones frente a un entorno digital cada vez más hostil.

En un mundo donde la digitalización acelera las oportunidades de negocio y, simultáneamente, multiplica las amenazas, anticiparse a los atacantes ya no es una opción: es una condición indispensable para prosperar.