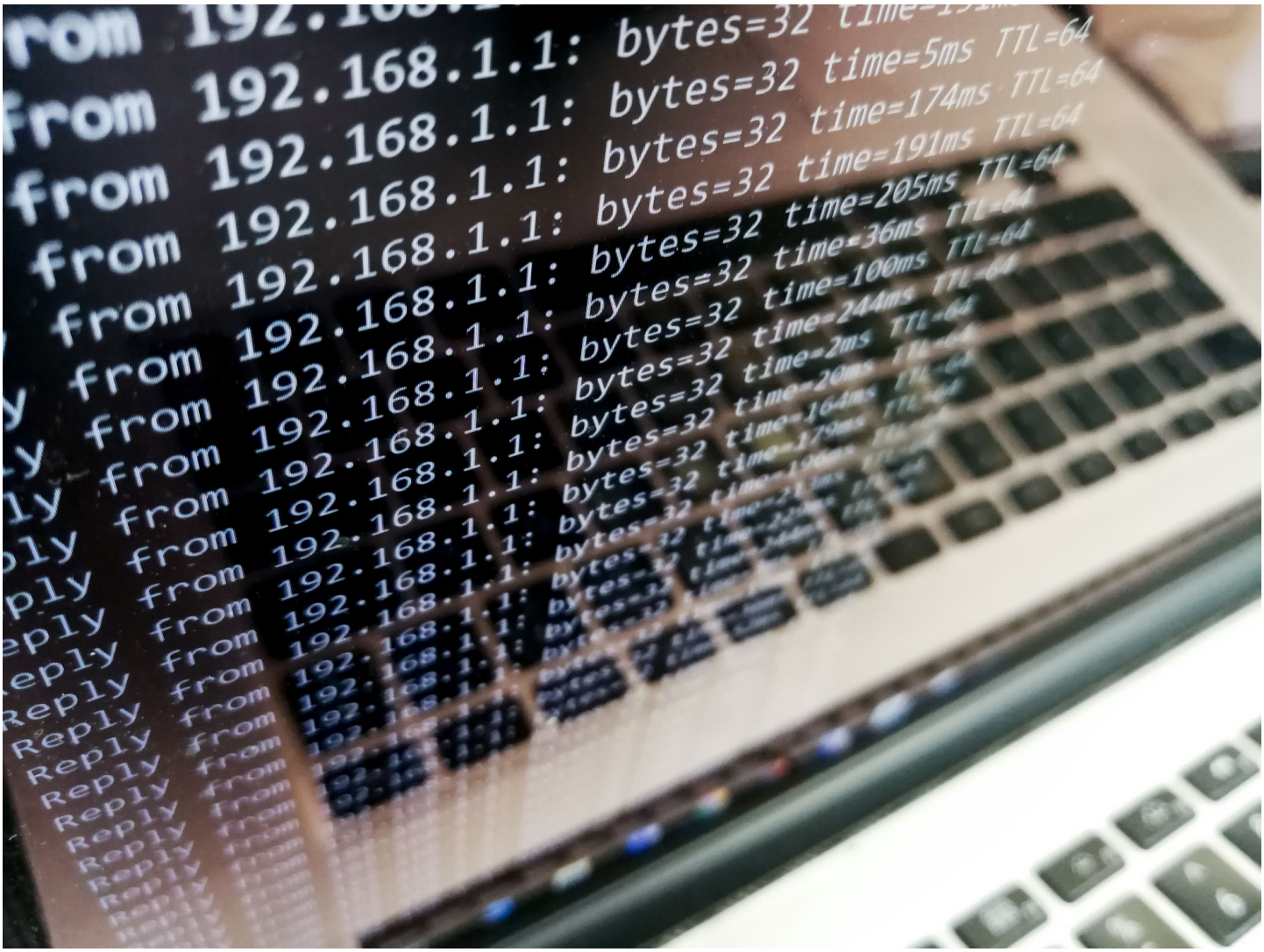
ATAQUES INFORMÁTICOS >

Las empresas se ponen en guardia: aumenta el riesgo de ciberataques tras la invasión de Ucrania

La Administración, las infraestructuras críticas y los servicios esenciales están en el punto de mira tras las sanciones a Rusia



En 2021, se produjeros 40.000 ciberataques diarios.
AUDRIUS MERFELDAS (GETTY IMAGES/ISTOCKPHOTO)

IRENE RUIZ DE VALBUENA

Madrid - 16 ABR 2022 - 05:45 CEST

En 2021, se produjeron 40.000 ciberataques diarios, un 125% más que el año anterior, según la empresa de soluciones de seguridad, Datos101. Si bien es cierto que en los últimos años el número de ciberataques no ha dejado de crecer, existen determinados factores, como la pandemia o la extensión del teletrabajo que, según los expertos, han contribuido a que el crecimiento en 2021 haya sido tan exponencial. Ahora, en plena guerra entre Rusia y Ucrania, ese riesgo se ha incrementado de nuevo y hace unas semanas la ministra de Defensa, Margarita Robles, anunció que el nivel de alerta ante ataques en el ciberespacio se elevaba a 3 de los 5 grados posibles.

La prevención sigue siendo la principal defensa frente a la amenaza de los ciberataques, y es ahí donde los abogados tienen un papel fundamental, concretamente en la adaptación de las organizaciones al marco regulatorio protector. Estas más de 50 normas se encuentran recogidas en el Código de derecho de ciberseguridad, estructurado en ocho grandes bloques, entre los que están, seguridad nacional, infraestructuras críticas o protección de datos.

Los sujetos obligados de estas normativas, salvo las más generales, como el Reglamento general de protección de datos, son, como señala Jesús Yáñez, socio de ciberseguridad de ECIJA, la Administración pública y sus proveedores, las infraestructuras críticas y los servicios esenciales. Estas entidades son precisamente el principal objetivo de los ciberataques dirigidos que surgen en respuesta a las sanciones impuestas a Rusia, afirma Jesús Iglesias, socio de Clyde & Co. Y es que, desde que se inició la invasión de Ucrania, han sufrido este tipo de ataques compañías de infraestructuras críticas como Iberdrola, entidades públicas como la Policía Nacional o la Agencia Tributaria, tecnológicas como Microsoft y Apple, así como la gran mayoría de bancos españoles (BBVA, Santander, Caixabank, Sabadell Liberbank), entre otros.

Sin embargo, no son el único blanco de la ciberdelincuencia. Los ciberataques generalizados siguen produciéndose a gran escala y atentan contra todo tipo de empresas, desde pymes a multinacionales. “En Rusia, hay organizaciones que se dedican al cibercrimen y aprovechan cualquier conflicto para incrementar los ciberataques”, explica Cristina Cajigos, ejecutiva de cuentas de Grupo Paradell Technologies, consultora especializada en riesgo digital y corporativo. En cuanto al móvil por el que se realiza un ataque cibernético, Yáñez admite que, puede ser tremendamente variado, “desde un rescate económico al acceso a información secreta, o una venganza de un extrabajador que sabe que las medidas de seguridad de su antigua empresa son mínimas”.

Cumplimiento normativo

Por todo ello, cada vez más empresas cuentan con un programa de cumplimiento normativo en ciberseguridad, a través del cual, como explica Natalia Martos, fundadora de Legal Army, se identifican los riesgos y vulnerabilidades y se valoran las probabilidades de que se produzca un ciberataque. “Se hacen test, se instalan controles de los que se verifica su eficacia, se crea un repositorio de evidencias y se generan medidas mitigadoras de riesgos”, describe Martos.

Un control que, como indica Yáñez, también implica evaluar a los proveedores tecnológicos de la empresa en materia de seguridad e incluso, exigirles medidas efectivas por contrato. “Hay que negociarlas con ellos, negociaciones que ya adelanto no son fáciles, pero sí necesarias. Ello no sólo nos

ayudará a evitar posibles brechas, sino que además servirá para demostrar nuestro compromiso y diligencia en esta materia", advierte.

Para Cajigos también hay que prestar especial atención a la sensibilización y formación sobre los riesgos por parte de los empleados. "El 90% de los ciberataques en las pymes viene por un fallo humano que está fuertemente vinculado a la concienciación y al clima laboral", afirma. De hecho, los más frecuentes son aquellos en los que se emplea ingeniería social, que como define Yáñez, no explotan las vulnerabilidades técnicas, sino que engañan al usuario haciéndole creer que está introduciendo sus credenciales de acceso en sitios legítimos, que en realidad no lo son. Se trata de los supuestos de suplantación de identidad corporativa o de sus representantes, con el objetivo principal de defraudar a terceros y obtener un beneficio económico. "Uno de los más comunes es el de la falsificación de facturas, mediante el cambio del número de cuenta donde debe realizarse el pago", avisa iglesias.

Como resultado, las empresas a las que se les suplanta su identidad, comenta Martos, "sufren terribles consecuencias, ya que sus clientes suelen ser objeto de robos y extorsiones que, inicialmente, pudieran parecer de su responsabilidad". Por ello, la consejera delegada de Legal Army recomienda que la entidad víctima deje constancia de todos los datos del ciberataque y se ponga inmediatamente en contacto con las unidades especializadas de las Fuerzas y Cuerpos de Seguridad del Estado para contenerlo y, en última instancia, tras un proceso de investigación forense, intente averiguar quién está detrás. "Algo que es realmente complejo por la falta de trazabilidad de las acciones en el mundo cibernético", reconoce.

Por su parte, Cajigos añade como pasos a seguir para mitigar el daño, detectar el origen del ataque, así como las vulnerabilidades para poder solucionarlas, e informar a la Agencia de Protección de Datos en caso de perder datos críticos. Eso sí, insiste en la prevención como aspecto clave. "Si preparas la infraestructura para la detección de intrusiones, tienes backups descentralizados con los datos críticos, un plan de recuperación de desastres y un plan de continuidad de negocio, el tiempo de reacción será más corto y el impacto del ciberataque mucho menor", concluye.

Seguros específicos

Contratar un seguro de ciberriesgos, según Jesús Iglesias, socio de Clyde & Co, "ayuda a que las empresas puedan responder y gestionar adecuadamente un ciberataque, y reduce los perjuicios financieros, legales o reputacionales derivados". Estas pólizas, explica el abogado, suelen incluir servicios de gestión de respuesta a incidentes y proporcionan un panel de diferentes proveedores, como técnicos, asesores legales, o empresas de relaciones públicas, que intervendrán si se da el caso. También es habitual que cubran las multas administrativas que puedan imponer las autoridades de protección de datos, el reembolso de los pagos de rescate realizados en caso de extorsión cibernética, o la posible responsabilidad civil del asegurado derivada del incidente.

Más información

Los ciberataques se multiplican desde la invasión de Ucrania y se hacen más frecuentes, diversos y complejos

RAÚL LIMÓN