La UE obligará a las empresas a contar con escudos contra los ciberataques

El aumento de la ciberdelincuencia obliga al Gobierno a revisar sus estrategias

La Unión Europa desarrolla una nueva estrategia de ciberseguridad que busca avanzar en la **protección de las infraestructuras europeas** frente a las cada vez mayores y más sofisticadas amenazas cibernéticas. Cada vez es mayor la normativa que obliga a las empresas a velar por su ciberseguridad de una manera eficaz, requiriendo la implantación de medidas preventivas que dificulten o eviten la producción de incidentes de seguridad.

El Consejo de Ministros del 20 de julio formalizó cuatro contratos suscritos con proveedores informáticos, con carácter de emergencia, en relación con la g**estión del ransomware sufrido por el Ministerio de Trabajo y Economía Social.** El importe de adjudicación de dichos contratos sumaba, en total, un millón de Euros. Hace algunas semanas los ministros eran testigos de cómo otro ransomware afectaba a los sistemas informáticos de un hospital belga, lo que obligaba al aplazamiento de las intervenciones quirúrgicas, con el consiguiente riesgo para las vidas humanas.

Las ciberamenazas se han convertido en uno de los principales obstáculos para la prosperidad de Europa, afirma Digitaleurope, a la vez que los afectados por las brechas de datos comienzan a organizarse para poder exigir indemnizaciones a los responsables de las empresas que sufren algún tipo de ciberataque, especialmente por las consecuencias derivadas de la publicación inconsentida de sus datos. Este tipo de situaciones van a ser cada vez más habituales, especialmente a la vista de los datos aportados por el Comité Económico y Social Europeo, que prevé un número de dispositivos conectados a nivel mundial cercano a los 25.000 millones en el año 2025, de los cuales una cuarta parte estarán en Europa.

La amenaza sobre los pagos del Sepe acelera el plan nacional de defensa cibernética

Aumentar los niveles de conectividad supone ampliar la superficie de exposición a las ciberamenazas, lo que provoca un lógico incremento de la probabilidad de sufrir incidentes de seguridad, recuerda Francisco Pérez Bes, Socio de Derecho digital en Ecix Group y antiguo Secretario General del Instituto Nacional de Ciberseguridad de España (Incibe).

Efectivamente, en el año 2021 se prevé que **el 74% de las empresas de todo el mundo podría sufrir un ciberataque.** Sin embargo, sólo el 32% de las empresas europeas han desarrollado políticas de ciberseguridad, alerta este experto. En cuanto a las pérdidas provocadas por la ciberdelincuencia, se estima que Europa sufre un mayor impacto económico que Estados Unidos, cuantificándose en un 0,84% del PIB de la Unión Europea, frente al 0,78% de Norteamérica, según afirma el último informe del Centro de Estudios Estratégicos e Internacionales.

Las pérdidas económicas provocadas por un ciberataque son enormes. Sólo en **Estados Unidos se considera que en 2020 se pagaron 350 millones de dólares en rescates de ransomware,** aunque este tipo de incidentes provoca pérdidas adicionales, consistentes en robo de información comercial, de datos personales o el daño reputacional. Recientes informes muestran que la contratación de una póliza de ciberseguro es sólo una pequeña parte de los gastos de preparación ante las amenazas cibernéticas (se calcula que un 5%), mientras que la auditoría y la formación son los factores más importantes que determinan los costes.

En lo que al teletrabajo se refiere, la crisis de la Covid-19 ha acelerado la transformación digital de las empresas, y de sus modelos de trabajo, lo que llevó a que en el año 2020 el 40% de los trabajadores de la Unión Europea continuasen desempeñando sus funciones en modalidad a distancia. En ese escenario, datos de Eurofund afirman que, en ese mismo año, el 40% de los usuarios de la Unión Europea experimentaron problemas relacionados con la seguridad, mientras que más del 12% de las empresas se vieron afectadas por algún tipo de ciberataque.

La amenaza de retraso en los pagos de prestaciones del Servicio Público de Empleo Estatal (Sepe) tras el ciberataque contra el organismo ha obligado al Gobierno a acelerar la nueva estrategia nacional de ciberseguridad. En concreto, el Ejecutivo trabaja ya en una nueva ley sobre el 5G, que reforzará la seguridad de las redes para evitar estos ataques y vigilará a los proveedores de estos servicios.

El Gobierno ha impulsado los trabajos del nuevo plan de defensa cibernética nacional. El Ejecutivo prevé aprobar en breve, según fuentes de Moncloa, la **nueva Ley de Ciberseguridad 5G**. elEconomista ha tenido acceso a los borradores con los que trabaja la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, dirigida por Roberto Sánchez. El texto incluye la protección de la seguridad nacional y exigirá reforzar la ciberseguridad de las redes 5G y de los servicios que se presten a través de ellas. Además, impedirá que solo haya un proveedor de estos servicios. La norma obligará a un mercado diversificado de suministradores, evitando la dependencia de proveedores poco confiables y posibles injerencias de terceros en dicha cadena de suministro, como ha ocurrido en el caso del Sepe según las informaciones del CNI.

Esta nueva norma someterá a los suministradores de esta tecnología a estrictos controles de seguridad, al objeto de garantizar su fiabilidad técnica y su independencia de injerencias externas.

La nueva amenaza que plantea el 5G

La tecnología 5G amplía las amenazas sobre una amplia gama de servicios esenciales para el funcionamiento del mercado interior y el ejercicio de funciones sociales, económicas y vitales. Afectará a sectores como la energía, el transporte, la banca o la sanidad. De hecho, los expertos afirman que la organización de los procesos democráticos, como las elecciones, también se basará cada vez más en las infraestructuras digitales y las redes 5G. La consultora Mckinsey estima que la previsión de crecimiento de la actividad económica que puede provocar el desarrollo de las redes 5G y 6G llegará los 3 billones de euros.

Fuente: El Economista