Las 10 claves para entender la nueva Ley de Ciberresiliencia

Multimedia

La empresa de ciberseguridad y ciberinteligencia S2 Grupo destaca que una de las máximas de la nueva Ley de Ciberresiliencia de la UE será la implantación del llamado 'security by design'. Se trata de algo "absolutamente necesario para la ciberprotección" que, sin embargo, "va a suponer un contexto difícil" para muchas empresas

En este contexto, desde S2 Grupo, especializada en ciberseguridad y ciberinteligencia, se ha destacado en un comunicado que con esta medida "se combatirá uno de los grandes problemas de la mayor parte de los dispositivos" que no habían sido diseñados pensando en patrones de ciberseguridad. Esto, según los expertos de la compañía, hacía que tuvieran muchos puntos vulnerables desde los que un atacante podría acceder a las redes locales.

"Además de la necesidad que supone crear productos ciberseguros desde la fase más incipiente de diseño, las empresas han de tener en cuenta que el incumplimiento de los requisitos que establece esta ley está sujeto a multas de entre 10 y 15 millones de euros o hasta el 2 o 2,5% de su volumen de negocio anual", ha declarado José Rosell socio-fundador y CEO de S2 Grupo.

Esta normativa ha contemplado un periodo de adaptación de 3 años y según han señalado los expertos de S2 Grupo, estas son las 10 claves sobre la nueva Ley de Ciberresiliencia:

1. Afectará a todos los dispositivos conectados a la red o a otros dispositivos.
2. Se establecen normas de ciberseguridad para el diseño, desarrollo y producción de productos con elementos digitales, obligaciones para los operadores económicos y normas sobre vigilancia del mercado y ejecución.
3. Establece una serie de requisitos esenciales para los procesos de gestión de vulnerabilidades establecidos por los fabricantes para garantizar la ciberseguridad de los productos digitales durante todo su ciclo de vida. Los fabricantes deberán informar sobre las vulnerabilidades e incidentes.
4. Los Estados miembros designarán una autoridad notificadora que establecerá los procedimientos necesarios para la evaluación y notificación de los organismos de evaluación de la conformidad y el seguimiento de los organismos notificados.
5. Tiene como principal objetivo que los consumidores tengan suficiente información sobre la ciberseguridad de los productos que adquieren y usan.
6. Obliga a los fabricantes a proporcionar soporte de seguridad y actualizaciones de software para resolver las vulnerabilidades identificadas.
7. Los fabricantes, importadores y distribuidores tendrán la obligación de incorporar requisitos esenciales de ciberseguridad en el diseño, desarrollo,

producción, entrega y mantenimiento de dispositivos digitales. Deberán entregar sus productos sin vulnerabilidades "conocidas" y con una protección "segura" por defecto.

8. Los fabricantes tendrán que informar activamente de las vulnerabilidades e incidentes de sus productos. Deberán dar soporte de actualizaciones frente a vulnerabilidades durante la vía útil de sus productos con un mínimo de 5 años y que se gestionen y mitiguen con eficacia.
9. Todos los riesgos de ciberseguridad deberán estar documentados.
10. Los productos con elementos digitales deberán contar con instrucciones claras y comprensibles y deberán disponer de una evaluación de conformidad.

"Estamos en un contexto de digitalización en el que toda clase de empresas u organizaciones requieren de asesoramiento específico en ciberseguridad, no solo para cumplir con la legislación, sino para ofrecer servicios y productos que no pongan en riesgo la continuidad de sus negocios o la ciberseguridad de sus clientes, conocer las implicaciones de la ley en su actividad, diseñar las medidas que deben adoptar para adaptarse correctamente a la Ley de Ciberresiliencia e implementarlas de forma eficiente", ha explicado José Rosell.

"Por otro lado, que un producto sea seguro hoy no garantiza que lo siga siendo en el futuro porque el avance continuo de las capacidades tecnológicas y las actualizaciones del software descubren cada día nuevas vulnerabilidades. Por este motivo, la evaluación de dispositivos deberá realizarse de forma periódica como un proceso de mejora continua, como un eslabón esencial más del proceso de negocio", ha concluido el CEO de S2 Grupo.