Directiva NIS2
Un nuevo paradigma de ciberseguridad en la Unión Europea

Por Joan Roda, Vocal de ADSI

En un contexto global donde las amenazas cibernéticas evolucionan a un ritmo sin precedentes, la Unión Europea ha dado un paso firme hacia el fortalecimiento de su resiliencia digital con la entrada en vigor de la **Directiva (UE) 2022/2555**, conocida como **NIS2**. Esta normativa, que sustituye a la Directiva NIS original de 2016, busca armonizar y reforzar las medidas de ciberseguridad a nivel comunitario, abordando las debilidades detectadas en la aplicación de la primera directiva y adaptándose al nuevo entorno de amenazas.

La **Directiva NIS (Network and Information Security)** fue la primera legislación de la UE en materia de ciberseguridad. Aunque representó un avance significativo, su implementación dejó brechas relevantes: falta de coherencia entre Estados miembros, requisitos poco claros y una cobertura limitada en cuanto a sectores afectados. Además, el aumento de ataques como el ransomware, las campañas de desinformación o los incidentes de cadena de suministro (supply chain attacks) evidenciaron la necesidad de un marco más robusto y actualizado.

La NIS2, adoptada en diciembre de 2022 y con plazo de transposición hasta **octubre de 2024**, responde a esta necesidad redefiniendo las obligaciones de seguridad, ampliando el ámbito de aplicación y estableciendo sanciones más contundentes. Esta directiva forma parte integral de la **Estrategia de Ciberseguridad de la UE para la Década Digital**.

Puntos clave de la Nueva Directiva NIS2

Ámbito de aplicación

Un cambio importante es que ahora más organizaciones entran dentro de la directiva.La NIS2 separa entre entidades clave (como las de energía, transporte, salud, gobierno o soporte digital) y las importantes (como los que hacen productos críticos, correos, empresas de residus o servicios digitales).Se calcula que más de 160,000 negocios estarán bajo esta Directiva, cuando anteriormente eran solo unas 15,000 con la NIS original.

Reglas claras y de cumplimiento forzoso

A diferencia de la anterior Directiva, donde cada país decidía quién debía seguir las reglas, la NIS2 tiene normas claras, como el tamaño y lo vital del servicio que ofrecen.Esto ayuda a que todo sea más parejo en la Unión y evita que cada quien haga lo que quiera.

Obligaciones mes severas en la ciberseguridad

Las organizaciones englobadas en la Directiva deberán poner en marcha medidas básicas de seguridad digital, como; manejar los riesgos y tener políticas de seguridad para los sistemas de información, manejar los incidentes y seguir funcionando, tener buena higiene digital y capacitar al personal, usar bien la criptografía y la autenticación de múltiples factores y asegurar la cadena de suministro, algo clave tras lo que pasó con SolarWinds.

Aviso de incidentes

La notificación de incidentes es más estricta. Las organizaciones deberán comunicar cualquier problema grave al **CSIRT nacional o a la autoridad** en 24 horas desde que lo detecte, y proporcionar un informe completo en cinco días.Además, deben avisar a los usuarios si el problema puede impactarles gravemente.

Régimen sancionador

La NIS2 aplica sanciones ejemplares, con multas de hasta 10 millones de euros o el 2% de las ventas anuales en todo el mundo. Se incluye como responsables a los jefes de las empresas y deben participar i gestionar los riesgos de seguridad digital.

Qué significa para el sector de la seguridad?

La **NIS2** representa un giro radical para los expertos en seguridad y los líderes en las empresas europeas. Inicialmente, exige que la ciberseguridad se integre en la estrategia central de las compañías, superando la respuesta reactiva y adoptando un enfoque de gestión proactiva de riesgos. Esto conlleva más inversión en tecnologías para detectar y responder, evaluaciones frecuentes, simulaciones de ataques cibernéticos y planes de mejora constante.Además, proteger la cadena de suministro digital supone un reto importante.Las empresas deben evaluar la seguridad tanto de sus sistemas como la de sus proveedores y socios tecnológicos, fomentando una cultura de responsabilidad compartida en todo el entorno digital.El rol del CISO y los equipos de ciberseguridad se vuelve más crucial, liderando el cumplimiento de la NIS2, coordinando con las autoridades y participando en decisiones estratégicas del negocio.A la vez, aumenta la demanda de talento especializado y formación continua, justo cuando el sector sufre una falta constante de expertos cualificados.

Retos y roles

La implementación de la NIS2 tiene sus desafíos.El primero es la verdadera armonización entre los países miembros, ya que, pese a que la directiva fija requisitos comunes, su aplicación puede variar, creando dudas para las empresas internacionales.Luego, muchas pymes, sobre todo las que ahora entran en la categoría de

"entidades importantes", no tienen los recursos o la experiencia para cumplir con los nuevos estándares.

Como resumen o conclusión final, podemos decir que la **Directiva NIS2** es un gran avance en la política de ciberseguridad europea.Al establecer normas más estrictas, extender su alcance y crear un marco más unificado, la UE deja claro que la ciberseguridad es clave y esencial para asegurar que la economía y la sociedad digital funcionen de forma segura.

Para los que trabajan en este campo, la NIS2 no solo es un desafío legal, sino una ocasión para liderar el cambio, fortalecer la cultura de seguridad y ser figuras clave en la protección del entorno digital europeo.Estar preparados, colaborar y anticiparse serán claves para triunfar en esta nueva fase. ■