

El proyecto IDUNN, liderado por IKERLAN, sienta las bases para afrontar la nueva Ley europea de Ciberresiliencia

La ley establecerá las normas comunes de ciberseguridad para dispositivos conectados

La Comisión Europea ha publicado el primer borrador de esta novedosa norma, que pretende establecer una regulación común de ciberseguridad para los productos digitales y servicios asociados que se comercializan en la UE y que será la primera legislación 'Internet de las Cosas' o IoT del mundo.

Uno de los módulos desarrollados en el marco del proyecto IDUNN ayudará a hacer frente a esta novedosa normativa.

Liderado por Ikerlan, este proyecto europeo arrancó el pasado año con un presupuesto superior a los 5M€ con el objetivo de que todos los componentes que lleven software incorporado en la industria sean ciberseguros.

Participan también: Grupo S21Sec, Fagor Arrasate, el Clúster GAIA, Mondragon Assembly y Mondragon Goi Eskola Politeknikoa, junto a socios finlandeses y alemanes.

Con un presupuesto superior a los 5M€ y una duración de tres años el proyecto IDUNN, liderado por el centro tecnológico vasco IKERLAN, pretende crear un sistema de detección cognitiva (aplicación de inteligencia artificial que "aprende" por sí sola para interpretar nuevos ataques externos), que analice y haga frente a las nuevas ciberamenazas. Su objetivo es, por tanto, que las tecnologías operativas presentes en el sector industrial sean resistentes a los ciberataques de hoy y del futuro.

Se trata de un proyecto puntero en el ámbito industrial europeo, alineado en la estrategia de Euskadi de convertirse en región referente en ciberseguridad industrial. Sus socios consideran que tendrá un impacto crucial en la productividad de cualquier industria al poder hacer uso de cadenas TIC seguras. Desde el consorcio anuncian ahora que, además, uno de los módulos desarrollados en el marco de IDUNN por IKERLAN ayudará a las empresas a hacer frente a los requisitos de análisis de vulnerabilidades que traerá la nueva Ley europea de Ciberresiliencia.

La Comisión Europea ha publicado ya un primer borrador de esta ley que establecerá normas comunes de ciberseguridad para los productos digitales y servicios asociados que se comercializan en la UE. Los próximos pasos serán el paso de la norma por el Parlamento Europeo y el Consejo, que examinarán, debatirán y propondrán sus enmiendas. Una vez aprobada, la normativa se aplicará en dos fases.

Desde el proyecto IDDUN recuerdan que a medida que los diferentes sectores económicos se han vuelto más dependientes de las tecnologías digitales en la ejecución de sus negocios, las oportunidades que brinda la conectividad digital también exponen a las economías a las ciberamenazas.

Ante esta realidad, la cantidad, la complejidad, la escala y el impacto de los eventos de ciberseguridad también están creciendo. "Cuando todo está conectado, un incidente de ciberseguridad puede afectar a todo un sistema, interrumpiendo muchas actividades económicas y sociales. La Ley de Ciberresiliencia introduce normas para proteger los productos digitales que no están cubiertos por ninguna normativa anterior. De este modo, será la primera legislación ('Internet de las cosas o IoT) del mundo", recuerdan las entidades participantes en IDUNN.

Hay que tener en cuenta que productos de hardware y software son cada vez más objeto de ciberataques exitosos, lo que ha provocado un coste anual mundial estimado de la ciberdelincuencia de 5,5 billones de euros para 2021.

¿Cómo ayudará IDUNN a hacer frente a la nueva Ley europea?

Según informan desde el consorcio, IDUNN ayudará a hacer frente a las necesidades que marque la nueva Ley europea de Ciberresiliencia gracias a los desarrollos pioneros que se están realizando en el mismo por parte de IKERLAN. Más concretamente, se avanzará en una aplicación de un sistema de detección resultante de una colección de microservicios que procesan en tiempo real el conjunto de actividades anormales y sospechosas en la red de entornos industriales con el objetivo de detectar incidentes o amenazas.

"Esta aplicación realizará una detección automatizada. Las vulnerabilidades identificadas se clasificarán, en función de su gravedad, para que posteriormente se pueda realizar una evaluación de riesgos y la presentación de informes. Por ejemplo, el sistema de detección detectará los activos que puedan verse afectados por un posible ataque y su nivel de criticidad", explican.

Recientemente, los participantes en el proyecto se reunieron en Oulu (Finlandia) en una cita en la que se analizó la evolución del proyecto y el avance en la evolución de los diferentes módulos y que contó con la participación de representantes de todos los socios del proyecto.

Este proyecto ha sido financiado por el programa de investigación e innovación Horizonte 2020 de la Unión Europea mediante el acuerdo de subvención nº 101021911.

Datos de contacto:

Clúster GAIA Comunicación
943223750

Nota de prensa publicada en: [Gipuzkoa](#)

Categorías: País Vasco Ciberseguridad Otras Industrias

NotasdePrensa

<https://www.notasdeprensa.es>