¿Cuáles son los grandes retos de la industria de la ciberseguridad en España para los próximos años?

Dotar a las infraestructuras críticas que aportan servicios esenciales a la sociedad de soluciones digitales que les permitan identificar con todo detalle los riesgos de carácter ciberfísicos, poniendo foco principal en el área de tecnologías de la operación (OT). Estas herramientas ágiles deberán ir enfocadas al gobierno de la seguridad, gestión del riesgo en tiempo real, notificación de incidentes, pruebas de resiliencia, intercambio de información, privacidad, diagnósticos rápidos por sectores, estándares para cumplimento (ISO/IEC), orquestación de personas y tecnología a través de la automatización inteligente de procesos y presentaciones visuales globales de indicadores y tendencias.

Asimismo, es importante que todo el gobierno relativo a riesgos ciberfísicos en las infraestructuras críticas se transmita claramente a su cadena de suministro, donde los diferentes TIER deberán aplicar de manera ágil los requerimientos de los primeros para que todos los servicios y/o productos que presten estén libres de vulnerabilidades y amenazas.

Desde su punto de vista, ¿qué ciberamenazas predominarán durante este año?

Tendemos a separar las amenazas del mundo físico de las del mundo lógico y a tratarlas de manera independiente; pero la actual transformación digital ya ha comenzado a poner de manifiesto que una amenaza física puede explotar una vulnerabilidad de un sistema IT/OT y viceversa.

La concienciación que se está creando sobre la digitalización de las personas, procesos y modelos de gobierno de las *smart cities* e Industria 4.0 afecta de lleno a los servicios esenciales que prestan las infraestructuras críticas y otros sectores que, sin ser considerados infraestructuras críticas, son de vital importancia en nuestro día a día.

¿Cómo ayuda su empresa a los usuarios a protegerse de las amenazas o a cubrir sus necesidades de ciberseguridad?

RKL dispone de un equipo de profesionales formados y desarrollados durante los últimos 25 años en las cuatro áreas principales de la seguridad integral.

La Ley PIC y la Directiva Europea NIS exigen la implantación de planes estratégicos y específicos a las infraestructuras críticas designados por el CNPIC mediante el desarrollo de los planes de seguridad operativos y planes de protección específicos; pero en RKL Integral vamos mucho más allá, mediante la posibilidad del despliegue de servicios y soluciones operables.

En consultoría, estos servicios son la base del diagnóstico y planificación de la seguridad integral que ayuda a alinear objetivos estratégicos y operativos de nuestros clientes.

En ingeniería ofrecemos servicios profesionales para el diseño e implementación de soluciones de seguridad integral y TIC que permiten a nuestros clientes aplicar las mejores soluciones. También contamos con soluciones SaaS para la explotación, operatividad y certificación de los diferentes planes exigidos por la ley.

Y, por último, cabe destacar VES PaaS, un *software* desarrollado por RKL Integral en un proceso de I+D+i testado mediante pruebas de concepto (PoC) para operar en tiempo real los riesgos ciberfísicos de infraestructuras críticas.

Conseguimos que todos esos planes sean operativos, certificables y resilientes en un entorno de seguridad integral, donde los mundos físicos y lógicos estén cada día más unidos.

Más información en:
rklintegral.com

José María Sanz Yarritu

CEO Y FUNDADOR

Los riesgos ciber físicos de tu empresa son una prioridad.

Te ayudamos a identificar, proteger, detectar, responder y recuperar desde una perspectiva global de las amenazas físicas y lógicas que pueden impactar en tu empresa, profundizando en las Tecnologías de la Operación (OT).

Consultoría

Ingeniería

Automatización de Procesos

VES PaaS

RKL integral

+34 946 40 10 11
contacta@rklintegral.com
rklintegral.com

Safety&Security
Cyber Physical
Threat Management