"TODO SISTEMA ELECTRÓNICO PUEDE SER ATACADO"

David González, responsable del departamento de ciberseguridad industrial de IK4-IKERLAN, analiza las amenazas a las que se exponen las empresas vascas

Empresas, instituciones y usuarios de internet demandan una mayor protección. Por estos motivos, IK4-IKERLAN ha trabajado en los últimos años en el desarrollo de tecnologías y productos en colaboración de sus clientes.

¿Qué visión general tiene de la ciberseguridad?

La ciberseguridad es un concepto muy amplio y tiene distintas implicaciones en función del ámbito en el que se trate. En IK4-IKERLAN nos centramos en la ciberseguridad industrial, y nuestra especialización está en el desarrollo de producto electrónico seguro. Al hablar de ciberseguridad en general pensamos en ataques informáticos a ordenadores ya sea en empresas o en el ámbito doméstico, pero cualquier sistema electrónico, si no está adecuadamente protegido, puede ser objeto de ataques locales o remotos (si se conecta a la red), y hoy en día los sistemas electrónicos están presentes en todos los ámbitos de nuestras vidas.

Nuestra visión de la ciberseguridad es la de ayudar a nuestros clientes a desarrollar productos más seguros para proteger, entre otras cosas, la integridad y disponibilidad de la información que gestionan y de las funciones que ofrecen a sus usuarios.

¿En qué se diferencia la ciberseguridad industrial respecto a otras áreas?

La ciberseguridad industrial está principalmente enfocada a la protección de sistemas electrónicos integrados en distintos procesos, bien en una planta industrial o en sectores más cercanos para todos como el transporte (automóviles, trenes, ascensores) o la energía.

Por ejemplo, prácticamente todos los sistemas electrónicos cuentan con un software y si personas ajenas a estos productos pueden acceder al mismo, podrían disponer de información confidencial sobre su funcionamiento (extrayendo información de valor sobre su diseño) o bien podrían modificarlo y hacer que el sistema funcione de forma distinta a la que fue diseñado, poniendo en riesgo a sus usuarios.. ¿Os imagináis que alguien ajeno a vuestro taller habitual modifica el software que lleva vuestro coche sin que vosotros lo sepáis?, ¿Qué garantía os daría montaros en él? En IK4-IKERLAN estudiamos las posibles vulnerabilidades que puede tener un producto electrónico y establecemos soluciones para evitar que personas ajenas al producto puedan acceder al mismo y modificarlo.

NECESARIO

"Todavía tenemos un camino largo por recorrer, aunque el nivel de concienciación ha crecido"

LIDER EN I+D

"Nuestra experiencia de más de 40 años transfiriendo tecnología a las empresas vascas nos avala"

¿En qué se especializa IK4-IKERLAN?

Nos enfocamos claramente en la industria, y en los riesgos asociados a la digitalización. En la unidad de TEIC (Tecnologías de la Electrónica, Información y Comunicación) de IK4-IKERLAN somos 150 investigadores desarrollando producto en toda la cadena de valor desde el sensor hasta la nube, diseñando para nuestros clientes sistemas embebidos, soluciones de conectividad, o plataformas digitales. Y lo más importante, trabajamos la ciberseguridad de todos nuestros desarrollos desde la etapa de diseño.

Nuestra experiencia de más de 40 años transfiriendo tecnología a la industria vasca nos avala como agente tractor en la digitalización de nuestras empresas. Prueba de ello es nuestra estrecha colaboración con empresas como Orona y CAF.

David González es responsable del área de ciberseguridad industrial de IK4-IKERLAN.

¿Cuál es el nivel de alerta?

La visión que tenemos de la seguridad en IK4-IKERLAN va más allá de los ciberataques. De hecho, lo que muchas de las empresas nos transmiten es que algunos de los riesgos que más preocupan además de los ataques remotos a través de Internet, son los ataques que se realizan localmente, cuando el atacante tiene acceso físico a los dispositivos. Por suerte, en Euskadi hay centros tecnológicos y empresas muy competitivas en el ámbito de la cibeseguridad, y tratamos de buscar la complementariedad con otros agentes. El papel de IK4-IKERLAN es fundamental ya que tenemos mucha experiencia y una gran especialización en el desarrollo de sistemas electrónicos seguros, mientras otros centros o empresas trabajan en actividades complementarias como la detección de amenazas o la gestión de incidencias.

¿Cree que hay suficiente concienciación entre las empresas?

En general, creo que todavía tenemos camino por recorrer. El nivel de concienciación ha crecido mucho en los últimos años, y prácticamente todas las empresas con las que colaboramos están trabajando para que sus productos y servicios sean más seguros. También es verdad que el punto de partida es muy distinto en función del sector, ya que en algunos casos la ciberseguridad no había sido un requisito hasta hace poco, y por lo tanto queda mucho trabajo por hacer.

¿Dejan algún tipo de señuelo para detectar a los hackers?

No, es cierto que hay empresas que se dedican a implementar este tipo de estrategias, pero como he dicho anteriormente en IK4-IKERLAN nos centramos en desarrollar productos seguros. Lo que sí hacemos es establecer mecanismos que nos permitan obtener la mayor cantidad de información posible tras una incidencia.

¿Es la ciberseguridad más una inversión que un gasto?

Sí, por supuesto, pero hay que determinar muy bien qué nivel de inversión es adecuado en cada caso. El coste de las medidas de seguridad puede variar en un espectro muy amplio, y en IK4-IKERLAN tratamos de ayudar a las empresas a definir y realizar la inversión más adecuada para lograr la mayor efectividad posible en sus productos.

¿Cómo se enfoca la formación siendo un área tan cambiante?

Creo que este es uno de los mayores retos que tenemos. Para empezar, la demanda actual de ciberseguridad es bastante reciente, y la oferta formativa aunque se está reforzando de manera significativa, todavía es incipiente. Además, tenemos la dificultad de que las asignaturas de ciberseguridad hasta ahora solo se han impartido en los grados de informática, y no es fácil encontrar ingenieros que combinen conocimientos electrónicos y de seguridad.

La solución que estamos adoptando es completar en IK4-IKERLAN la formación de los alumnos que quieran especializarse en el tema, por ejemplo, mediante tesis doctorales con universidades de referencia.

Más información: **www.ikerlan.es**