MURCIA INDUSTRIA 4.0

Tú formas parte de la Cuarta Revolución Industrial

Ciberseguridad

Descripción

La ciberseguridad representa un eje fundamental de actuación en la industria. El ciberespacio se ha convertido en una parte integral de nuestra vida.

Organizaciones y entidades de todos los ámbitos (sanidad, financias, educación, etc.) utilizan redes de comunicación para recopilar, procesar, almacenar y compartir grandes cantidades de información digital. A medida que se recopila y se comparten más datos, la protección de esta información se vuelve más importante para nuestra seguridad nacional y estabilidad económica. En este contexto, la ciberseguridad se define como la capacidad de proteger los sistemas de red, las infraestructuras y los datos contra el uso no autorizado y sus posibles daños (a nivel personal, corporativo y de estado).

Dos puntos estratégicos de la ciberseguridad son la seguridad en las comunicaciones y el uso apropiado de las herramientas de las que disponemos hoy en día para hacer frente a las ciberamenazas.

Confidencialidad, integridad, disponibilidad, autenticación y no repudio representan los pilares de un entorno seguro. Para alcanzar estas características es necesario aplicar un conjunto de tecnologías entre las que se incluyen técnicas criptográficas, métodos de autenticación, cortafuegos, redes privadas virtuales, sistemas de detección de intrusos, monitorización y auditoría, entre las más destacadas. Así, conocer la idiosincrasia de la ciberseguridad facilitará la labor de los expertos en la nueva revolución industrial.

Beneficios de su incorporación en la empresa

La Industria 4.0, una industria altamente automatizada, conectada e inteligente, no sólo debe hacer frente a los problemas clásicos sino que ahora se enfrenta a amenazas cada vez más sofisticadas en el ámbito del ciberespacio dirigidas a la infraestructura crítica y los dispositivos inteligentes que se emplean. El coste de sufrir un ciberataque puede ser muy elevado, por ejemplo, el ciberataque WannaCry le costó al gobierno británico más de 100 millones de euros. Estadísticas recientes muestran que más del 50% por ciento de las PYMES experimentaron algún tipo de ciberataque en 2018.

Al mismo tiempo, una gran mayoría de empresas asumen no estar preparadas en lo referente a su capacidad para proteger y mitigar un ciberataque. Por ello, es fundamental proteger los sistemas de red, las infraestructuras y todos los datos contra el uso no autorizado y los posibles daños (a nivel personal, corporativo y de estado). Sin embargo, no será posible protegernos si no existe una formación previa que permita conocer y dar respuesta de primera mano a preguntas básicas como: ¿qué debemos proteger?, ¿cuáles son las amenazas?, y por último, ¿cómo protegernos? La formación en este ámbito será básica para lograr que todos los actores (empresarios, emprendedores, trabajadores, clientes, etc.) sean partícipes del éxito.

Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Unión Europea
Región de Murcia
info REGIÓN DE MURCIA

Ejemplos de aplicación en empresa de la tecnología

La Industria 4.0 es inherentemente propensa a vulnerabilidades que los atacantes pueden explotar para acceder a las redes de destino. Por ejemplo, supongamos un sistema de tratamiento de aguas que es atacado y en consecuencia, se produce la caída completa del sistema, dejando a una región sin suministro de agua. En concreto, una vez que los atacantes consiguen acceder a la red de la empresa, podrían llegar a la red de control de la misma y hacerse con el control de los sistemas SCADA.

Así, si consiguen controlar una bomba y forzarla a que vaya cambiando de estado (apagado-encendido), al final la bomba se romperá por el uso incorrecto, derivando al final dejar sin suministro a una parte de la población. Los dispositivos de Internet de las Cosas (IoT, Internet of Things) son otro claro ejemplo.

Dispositivos IoT con un bajo nivel de seguridad que se utilicen para controlar el sistema de riego de una explotación agrícola, podrían hackearse. En este caso, los atacantes podrían por ejemplo simplemente apagar los dispositivos de forma que se deja sin riego por falta de datos de entrada (los que capturan los sensores de los dispositivos IoT) al sistema.

Por todo ello, es necesario un enfoque integrado de la seguridad. Cualquier entorno inteligente seguro debe tener una base sólida que utilice la detección y prevención de intrusiones, listas blancas de aplicaciones, monitorización de la integridad, segmentación, parches virtuales, análisis avanzado de espacios aislados, aprendizaje automático, análisis de comportamiento, antimalware, detección de riesgos, evaluación de vulnerabilidades, firewall de próxima generación, tecnologías anti- phishing, protección contra spam o fugas de datos, entre otros.

Coste de incorporación en la empresa

La inversión que cada empresa debe realizar para protegerse de las ciberamenazas dependerá directamente del tipo y características del negocio. Por ejemplo, la pérdida de datos sensibles de los clientes de una empresa, no sólo significa perder los datos en sí sino una pérdida de credibilidad que a su vez repercutirá negativamente en el futuro de la empresa. De forma orientativa, serían los siguientes:

- **La complejidad de la arquitectura de red** establecida o a establecer (cantidad de equipos de hardware involucrados). El coste medio de un firewall ronda los 1.200 €.
- **Licencias de software de seguridad** (antivirus, antispyware, etc.) (algunas licencias también cuentan con actualizaciones). El coste suele rondar los 100 euros por anualidad, aunque dependerá del número de equipos a proteger. También existen soluciones de tipo open source aunque se requiere de cierta experiencia para su instalación y configuración.
- **Personal de la empresa** o tercerizado especializado en brindar seguridad en la empresa y en la realización de evaluación de riesgos de seguridad. El salario medio en España se encuentra aproximadamente entre los 30.000-45.000 €.
- **Herramientas software de auditoría y monitorización** (AlienVault, IBM Qradar, HP ArcSight, Splunk, etc). Estos programas combinan detección y gestión de vulnerabilidades, detección de anomalías, monitorización de seguridad, visualización, capacidad de respuesta a incidentes, etc. El precio de la licencia suele comenzar en 1000 euros por mensualidad, aunque existen opciones más económicas para PYMES.
- Otra alternativa es la **contratación de Security as a Service** (SaaS o SecaaS). Se trata de un modelo basado en la nube para ofrecer soluciones de seguridad. En este caso existen multitud

de opciones siendo necesario contactar con el proveedor para analizar los costes.

En definitiva, a diferencia de otras tecnologías de la Industria 4.0, el coste de incorporación en la empresa de medidas de ciberseguridad dependerá totalmente de las características técnicas de dicha empresa, del tipo de servicio que proporcionan y del impacto que los riesgos en los que pudiera incurrir la empresa podrían causar.