TRES CONSEJOS SOBRE CIBERSEGURIDAD

La ciberseguridad es una preocupación cada vez mayor entre los fabricantes, ya que cada semana se crean nuevas cepas de ransomware y otros virus de sistemas.

Cualquier empresa puede ser objetivo de un ataque cibernético. La mejor forma de prevenirlo consiste en planificar con antelación y prepararse para lo inesperado.

1

DISPOSITIVOS CONECTADOS

Las ventajas de los dispositivos móviles se pueden observar en la supervisión del estado, el mantenimiento predictivo y los análisis. Para los fabricantes que usan dispositivos conectados, las actualizaciones de seguridad periódicas y las auditorías informáticas deberían ser una prioridad si pretenden detectar y resolver fallos del sistema.

2

SISTEMAS TRADICIONALES

Por lo general, los sistemas informáticos industriales no se actualizan ni sustituyen con tanta frecuencia como la tecnología de consumo, lo que hace que los fabricantes sean vulnerables a ataques como Heartbleed o Shellshock.

Los sistemas más antiguos pueden tener instalado un software OpenSSL. Es posible que las vulnerabilidades de este software hagan que el sistema sea accesible a atacantes que pueden interceptar o robar datos.

Muchas empresas de software han divulgado actualizaciones críticas gratuitas para atajar estas vulnerabilidades. Todo lo que los fabricantes tienen que hacer es actualizar su software.

3

SISTEMAS DE PRODUCCIÓN AUTOMATIZADOS

Las redes y los sistemas corporativos no son lo único expuesto a riesgos. Los sistemas de control industriales también pueden ser objetivo de ransomware. Si un ataque bloquea los ordenadores de fabricación, podría suponer importantes costes de inactividad. Los fabricantes deben proteger los sistemas de producción automatizados mediante la protección celular, una forma eficaz de defensa frente a ataques por intermediario.

En la era de la Industria 4.0, los dispositivos conectados y los sistemas automatizados pueden ser objetivo de mayores amenazas. La mejor forma de prevenir un ataque consiste en planificar con antelación y prepararse para lo inesperado.