Cyber-Physical Risks: When Data Attacks Meet Physical Safety Meeting Kit – Spanish

QUÉ ESTÁ EN RIESGO

Antes, un ciberataque solía significar contraseñas robadas o una bandeja de entrada de correo electrónico bloqueada, pero esos días ya quedaron atrás. Hoy en día, los atacantes pueden infiltrarse en una fábrica y bloquear un robot, anular un sistema de seguridad o apagar la calefacción y la refrigeración del edificio. Cuando los mundos digital y físico se conectan, cada contraseña débil se convierte en un riesgo potencial de lesiones, y todos los trabajadores se encuentran en primera línea.

CUÁL ES EL PELIGRO

Ciberataques en la Planta

La mayoría de los ataques ciberfísicos comienzan con un simple clic en un enlace de un correo electrónico común. Desde la red de la oficina, los atacantes se desplazan lateralmente hacia los sistemas operativos. El malware que se inicia en una computadora portátil puede llegar a los controladores de las máquinas en cuestión de horas.

Sensores y Alarmas Manipulados

- Lecturas falsificadas de gas, temperatura o presión
- Alarmas silenciadas que deberían haber detenido la línea
- Falsas alertas que provocan evacuaciones innecesarias

Acceso Remoto y Robots sin Seguridad

Los proveedores y contratistas a menudo se conectan a los sistemas de la planta a través de computadoras portátiles, tabletas y VPN que se dejan abiertas. Las carretillas elevadoras, los vehículos guiados automáticamente (AGV) y los robots colaborativos reciben sus comandos a través de la red y pueden ser redirigidos en el peor momento. Es posible que los trabajadores cercanos no reciban ninguna advertencia antes de que un vehículo cambie de rumbo.

COMO PROTEGERSE

La seguridad cibernética en la planta de producción es responsabilidad de todos.

Presta Atención a los Equipos que Funcionan de Manera Anómala

- Reinicios inesperados o reinicios sin explicación
- Puntos de ajuste o temporizadores que cambian por sí solos
- Alarmas que no coinciden con las condiciones reales

Trata Cada Inicio de Sesión Como si Fuera una Cerradura

Utiliza contraseñas seguras y únicas en cada sistema, y nunca compartas tus credenciales con tus compañeros de trabajo, aunque sea más rápido. Habilite la autenticación multifactorial siempre que sea posible, incluso en las tabletas de la planta y los paneles HMI. Un inicio de sesión marca la diferencia entre una máquina controlada y una comprometida.

Esté Atento al Phishing en los Dispositivos de la Planta

Las tabletas HMI, los quioscos compartidos y las terminales de despacho son objetivos principales porque se encuentran en la intersección entre la oficina y la planta. Si un mensaje parece sospechoso —remitente inesperado, lenguaje urgente, enlace extraño— no haga clic en él y no lo ignore. Denúncielo para que puedan advertir al resto del equipo.

Bloquee los Soportes Extraíbles

Las memorias USB y los dispositivos personales son una de las vías de ataque más comunes a las redes de la planta. Utilice únicamente unidades aprobadas por la empresa en los sistemas de la planta, y nunca conecte algo que haya encontrado en el estacionamiento o que le haya dado un proveedor sin inspeccionarlo. Trate los soportes desconocidos de la misma manera que trataría los productos químicos desconocidos.

Si Ocurre: Actúe Rápido

- Detenga la máquina utilizando la parada de emergencia física
- Aíslela de la red si puede hacerlo de forma segura
- Informe inmediatamente al departamento de TI y a la supervisión
- No intente volver a iniciar sesión ni «arreglarlo» usted mismo

CONCLUSIÓN

La línea que separa un teclado de un interruptor de emergencia es más delgada que nunca. Cuando los ataques cibernéticos llegan al mundo físico, quienes velan por la seguridad de las operaciones son los mismos que se dan cuenta cuando algo anda mal. Mantente alerta en línea, mantente alerta en el lugar de trabajo: ahora ambos turnos son uno solo.