Inycom
innovation technologies

CONSTRUYENDO LA CIBERSEGURIDAD INDUSTRIAL VECTORES DE ATAQUE

- Industria 4.0
- Ciberseguridad
- Eficiencia Operacional
- Continuidad de Negocio
- Tratamiento de Datos
- Disponibilidad e Integridad

Aitor Lejarzegi
ICS Network Specialist & Industry 4.0 Business Dev.
Responsible Industrial Cyber Security for Inycom
aitor.lejarzegi@inycom.es
@cybergudari

4.0

CONSTRUYENDO LA **CIBERSEGURIDAD INDUSTRIAL**

Fuente de Información: Kaspersky Lab

A día de hoy, la ciberseguridad es ya un **elemento fundamental en la Industria**. Un proceso necesario que continuamente se mejora, se construye por fases con el objetivo claro de que siempre permanezca presente y adecuadamente controlado con un sistema profesional de gestión. La **mejora continua de la vigilancia** define el mejor objetivo.

En los sistemas que controlan un proceso industrial, otro factor importante es tener visibilidad de los riesgos asociados y para conocer este dato, es imprescindible realizar una auditoria o un estudio de vulnerabilidades. Contamos con que antes, necesariamente, **la concienciación** haya comenzado en la dirección de la empresa.

La auditoría nos aporta la situación real de la seguridad, será la foto de los agujeros que debemos cerrar .Una vez lo tengamos, ya con los ojos bien abiertos, daremos comienzo al desarrollo de una nueva arquitectura por fases. Entre otros, buscamos cerrar las brechas de seguridad, ofrecer una mayor **eficiencia operacional, monitorizar los riesgos en tiempo real y mantener de manera proactiva la continuidad de negocio**.

Sin embargo, es importante centrar adecuadamente el estudio de vulnerabilidad para evaluar los **vectores de ataque específicos del entorno**. Identificar los vectores de ataque es **una necesidad**.

Nivel 4 > ERP (Enterprise Resource Planning)

Nivel 3 > MES (Manufacturing Execution System)

Nivel 2 > SCADA (Supervisory Control and Data Acquisition)

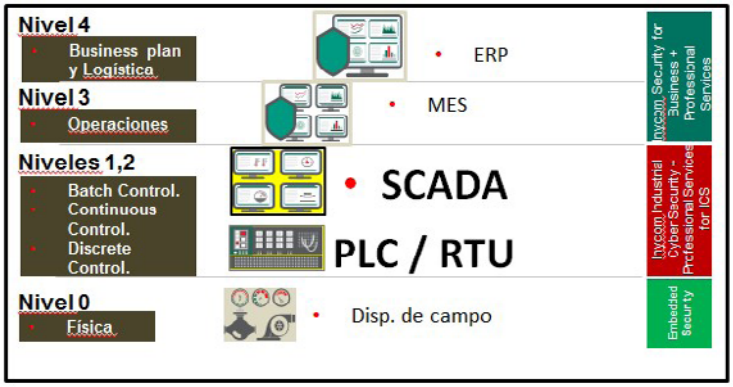
Nivel 1 > PLC/RTU (Programable logic Controller, Remote Terminal Unit)

Nivel 0 > Disp. Campo (field devices, sensores, válvulas, bombas...)

Distinguimos además **vectores de ataque y seguridad** entre:

1. Infraestructura física
2. Infraestructura lógica
3. Equipo final

SEGURIDAD POR NIVELES



FUENTE: Kaspersky Lab

La seguridad se construye por niveles y cada nivel de seguridad debe servir para proteger diferentes elementos activos

VECTORES DE ATAQUE EN **INFRAESTRUCTURAS INDUSTRIALES**

Los **vectores de ataque de la infraestructura física** son los relacionados con todos aquellos elementos pasivos, los cuales pasan por el correcto diseño y arquitectura física de la red, que son los responsables de la calidad de las comunicaciones en la planta industrial.

La construcción de la infraestructura física se consigue entre otros, mediante la implantación de estándares de la industria de telecomunicaciones. Algunos importantes, son el estándar de 'cableado estructurado" o el estándar de 'etiquetado".

En la fase de construcción de la seguridad industrial, comenzamos estudiando la infraestructura física para pensar en la seguridad que mantenemos para la infraestructura lógica en nuestras comunicaciones.

La protección de lo que consideramos la **infraestructura lógica** de nuestra planta, la diseñamos y aplicaremos en diferentes etapas. Por un lado, se distingue la etapa de los **servicios en la red** y por otro lado, la capa del **equipo final**. Cada una de ellas se origina según los diferentes vectores de ataque.

Dentro de los distintos niveles de seguridad que mencionábamos anteriormente, nos situamos en el **Nivel 1** y en el **Nivel 2**, es decir la parte de control y la parte de supervisión del proceso productivo.

FUENTE: Kaspersky Lab

Los vectores de ataque de la infraestructura lógica son los Niveles 1 y 2 de seguridad

MITIGAR LOS RIESGOS EN **SERVICIOS DE RED** EN LA INDUSTRIA

En la capa de protección de servicios de red, algunos de los vectores de ataque en una red industrial incluyen:

- Integradores y subcontratas o terceros en la red de control.
- Las conexiones desde la planta al ERP/MES o las conexiones a internet.
- Conexiones remotas o no autorizadas a la red de control de proceso.
- Ataques en la red al dispositivo PLC/RTU que controla el proceso.
- Reconfiguraciones no autorizadas a un dispositivo PLC.
- Envíos de órdenes de control no autorizados.
- Tipos sofisticados de ataques intencionados en la red

Estos riesgos se pueden mitigar empleando las necesarias soluciones de seguridad. Las soluciones que **Inycom ofrece** incluyen:

Control de la Integridad de la Red de control

1. Identificar activos en la red
2. Identificar comunicación legítima en la red
3. Detección de nuevos dispositivos

Control de la integridad del PLC

1. Control de cambios del programa del PLC
2. Control de órdenes remotas al PLC (MARCHA / PARO / PAUSA, etc.)

Detección de anomalías en la Red

Ataques en la Red y órdenes peligrosas que pueden afectar al SCADA, al HMI, a la detección del PLC en la red, etc.

Análisis semántico de órdenes de Control de Proceso

Detectando órdenes al PLC en la Red que pueden afectar en la disponibilidad del proceso (ordenar cambiar valores de parámetros cruciales en el proceso)

¿CÓMO PROTEGER EL **EQUIPO FINAL**?

En la protección del **Equipo Final** se habla del sistema **SCADA, del HMI** o equipo con el que vemos el proceso y con el que trabaja directamente el operador. El nivel de seguridad del que hablamos es el **Nivel 2**, relacionadas con la seguridad durante la supervisión.

Los vectores de ataque que vemos son:

- Software vulnerable (SCADA, Sistema Operativo, terceros)
- Conexiones a internet o a ERP/MES
- Uso no controlado de software
- Uso de dispositivos móviles no autorizados
- Dispositivos extraíbles como USB/SATA, etc.
- Subcontratas e integradores
- Cadena de suministro

Los equipos HMI son muy delicados en recursos y muchas veces extremadamente críticos en el control del proceso industrial. **La disponibilidad e integridad de los datos es nuestra mayor preocupación** y lo tenemos presente a la hora de aplicar esa seguridad.

Inycom ofrece soluciones para proteger a un equipo final (HMI) de manera segura y sin que afecte nunca al correcto funcionamiento del proceso.

La protección SCADA o de equipo final de Inycom incluye características como:

Un Software especialmente diseñado según las necesidades de sistemas de control industrial, con las siguientes características

- Un consumo de recursos optimizado
- Una Actualización adaptada (firmas, etc), Políticas
- Envío de alertas de seguridad al operador de SCADA (HMI)
- Comprobaciones de la compatibilidad de SCADA

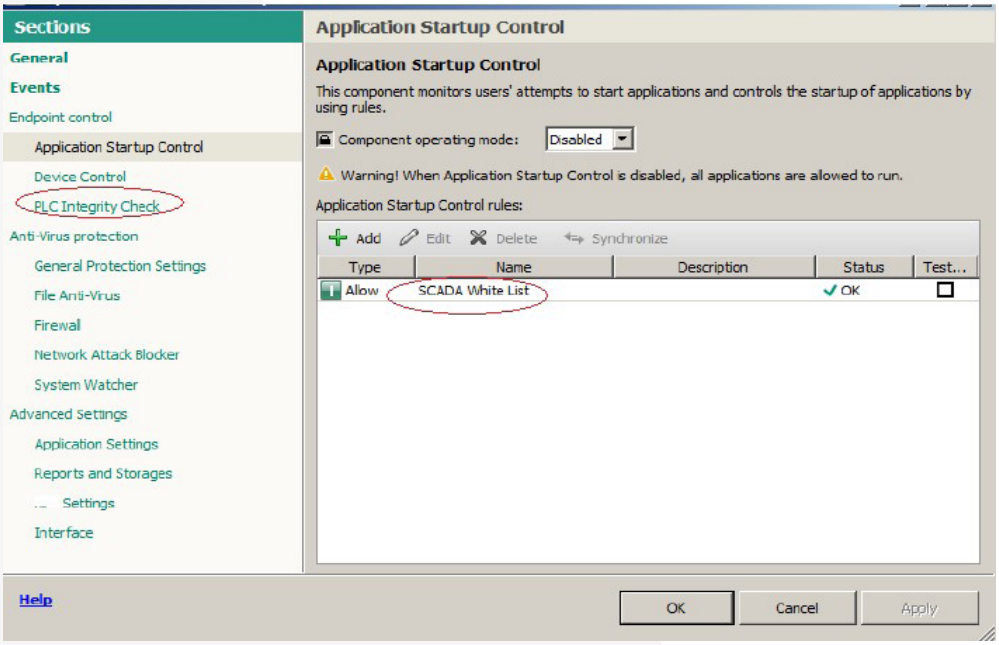
Control de integridad (listas blancas, listas negras) mediante

- Control de inicio de aplicaciones
- Control de dispositivos externos

Comprobación de integridad del PLC con

- Protección AntiVirus proactiva basada en firmas
- Evaluación de vulnerabilidad
- Integridad SIEM

PARAMETRIZACIÓN DE UNA SOLUCIÓN QUE PROTEGE LA INTEGRIDAD DE PLC/SCADA



Inycom ofrece soluciones para proteger a un equipo final (HMI, SCADA) de manera segura y sin que afecte nunca al correcto funcionamiento del proceso

SOLUCIONES INYCOM PARA
LA INDUSTRIA CON FUTURO

GESTIÓN PARA PROTEGER **EN PROFUNDIDAD**

En conclusión, es necesario conocer por un lado, la diferencia entre niveles de seguridad y por otro lado, de conocer también las distintas etapas que nos encontramos durante la fase de construcción de la seguridad industrial, con el objetivo de proteger en profundidad.

Una buena gestión durante este proceso de construcción es determinante. No te pierdas el próximo WhitePaper en el que hablaremos sobre los servicios de **Vigilancia** necesarios para mitigar riesgos y también, del **Centro de Operaciones de Seguridad (SOC, 24hx7) de Inycom**. Un SOC diseñado para la protección de la industria conectada.

#IndustriaDeFuturo

Todas las novedades en nuestra web
y nuestras redes sociales

+34 902 500 001
industriadefuturo@inycom.es

Inycom

>>INNOVACIÓN<<

COMPROMETIDOS CON SU FUTURO

GANADOR PREMIO A LA EXCELENCIA EMPRESARIAL EN ARAGÓN 2006
GRANDES EMPRESAS

AENOR ER-0532/1998 Empresa Registrada UNE-EN ISO 9001
AENOR SI/014/2009 Seguridad Información UNE-ISO/IEC 27001 DataCenter INYCOM
AENOR STI-0002/2014 Gestión Servicios TI UNE-ISO/IEC 20000-1
AENOR GA-2009/0053 Gestión Ambiental UNE-EN ISO 14001 O.C. ZARAGOZA

CMMI DEV/2 Exp. 2016-06-20 / Appraisal #20592
ITIL
PMP

www.inycom.es