CUADERNOS DE SEGURIDAD

Núm. 313 • JULIO-AGOSTO 2016 • 10 euros

PUNTOSEGURIDAD.com

¡MÁS DE 6.000 VISITANTES!

CUATRO AÑOS SUPERANDO EL RÉCORD
DE ASISTENCIA A SECURITY FORUM

Y además: Seguridad en hoteles | Seguridad en el transporte

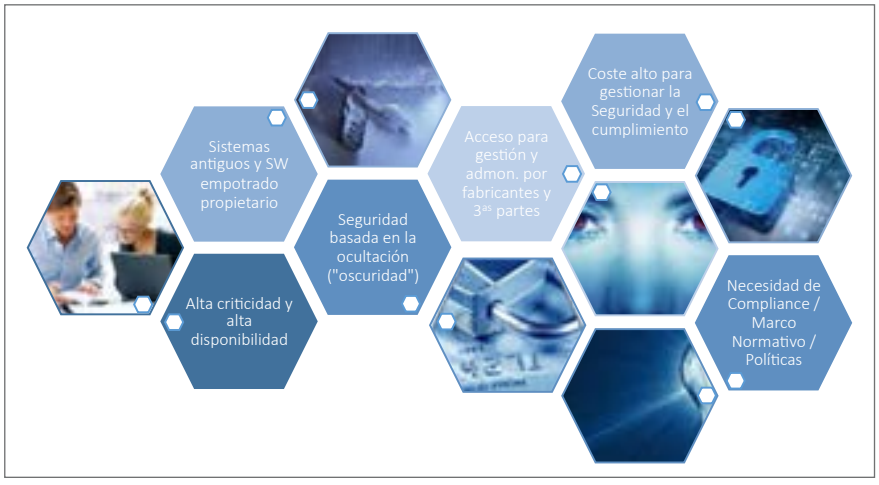
MARTA DOMÍNGUEZ JIMENO Y ENRIQUE DOMÍNGUEZ FERNÁNDEZ. INNOTEC SYSTEM

¿Protege su organización de forma eficiente sus infraestructuras críticas?

Por su enorme transcendencia, las infraestructuras críticas o estratégicas de una organización deben tener asegurada su disponibilidad y correcto funcionamiento. Lo contrario podría derivar en una pérdida de control sobre el proceso, con los riesgos que ello implicaría tanto en la seguridad del sistema como incluso en la seguridad física de las personas o el entorno. La seguridad en entornos industriales, por tanto, requiere de una atención y medidas de protección especiales, que contemplen la gestión integral de la seguridad (abarcando la doble dimensión física y virtual), y teniendo en cuenta que las ciberamenazas representan un riesgo con una probabilidad mucho más alta que el asalto físico y con un menor riesgo para quien lo comete[1].

En sentido general, cuando utilizamos los conceptos de infraestructura crítica o estratégica, estamos pensando en la función que ésta desempeña o el servicio que presta. Es decir, son determinadas funciones las que, a nuestro juicio, merecen el calificativo de esenciales y, a partir de ahí, mediante el estudio de las instalaciones, las redes y los procesos de trabajo por los que se desarrollan estas funciones, podremos determinar si alguna de las infraestructuras sobre las que operan reúne las características precisas para ser considerada de una manera especial[2]. Es decir que, en el ámbito empresarial, su funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre la operación de la organización, sus servicios esenciales y, por ende, de su continuidad en el tiempo.

Fig. 1 Desafíos en Seguridad OT.



En los últimos años, los operadores de infraestructuras críticas han centrado una buena parte de sus esfuerzos en el cumplimiento de las nuevas legislaciones impulsadas desde las diferentes instituciones nacionales o comunitarias. Por ejemplo, en España, según establece la Ley 08/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, el operador designado como crítico deberá elaborar un Plan de Seguridad del Operador (PSO) y un Plan de Protección Específico (PPE) por cada una de las infraestructuras críticas de las que sea propietario o gestor. Hasta la fecha se han nombrado 93 operadores críticos y se han identificado a más de 300 infraestructuras críticas de sectores como la energía, la industria nuclear, el sistema financiero, el transporte y el agua.

Por otro lado, cada vez son más numerosas las amenazas e incidentes de ciberseguridad en entornos industria-

les, por lo que no es suficiente con las típicas estrategias y controles de seguridad IT. Medidas como la protección perimetral clásica («burbuja») se han demostrado insuficientes en un entorno enormemente distribuido y en cuyo perímetro, cada vez más difuso, no sólo están los sistemas corporativos, sino sistemas distribuidos en sedes remotas, sistemas de control industrial, accesos de proveedores, etc.

Por ello es necesario aplicar el pensamiento lateral y ponerse en lugar del atacante, analizando nuevas formas de proteger nuestros activos, dificultando no sólo penetrar en nuestra infraestructura, sino evitando que el atacante se mueva horizontalmente por la misma para encontrar nuevos vectores de ataque y persistencia.

Como los organismos biológicos complejos, no sólo tenemos que establecer barreras de protección contra las amenazas externas, sino también establecer sistemas adicionales de protección que impidan que dichas amenazas penetren en nuestros sistemas más críticos. También contamos con sistemas inmunológicos que responden a los incidentes, reduciendo la amenaza, su capacidad de extenderse por nuestra infraestructura y preparándonos en caso de que un agente similar vuelva a atacar nuestro organismo.

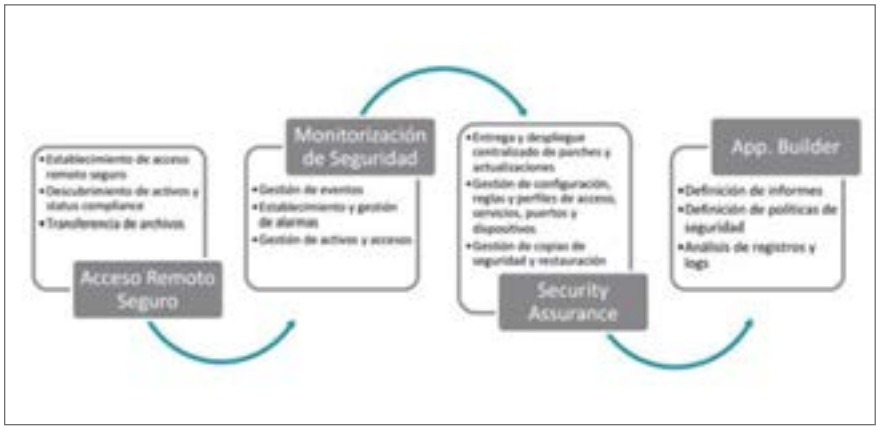


Fig. 2 Provisión y Gestión Centralizada de Seguridad OT.

> «En la protección de infraestructuras críticas es preciso aplicar el pensamiento lateral y ponerse en el lugar del atacante»

Adicionalmente, en entornos industriales, es importante tener en cuenta nuevas necesidades más allá de la clásica triada de confidencialidad, integridad y disponibilidad, siendo imprescindible mantener intactas las capacidades de operación, observación y control de los sistemas OT (Operational Technology).

Por todo ello, queda claro que la seguridad en entornos industriales y en especial infraestructuras críticas requiere de una atención y medidas de protección especiales.

Principales desafíos en Seguridad OT

Por su enorme criticidad, los sistemas OT deben garantizar una muy alta disponibilidad, estando siempre listos para realizar su función, hasta en las circunstancias más adversas. Sin embargo, las infraestructuras críticas a menudo cuentan con sistemas antiguos («legacy») y software propietario empotrado.

Hasta la fecha las empresas del sector industrial han basado su seguridad IT/OT en la separación física y la ocultación («Seguridad a través de la oscuridad»). Además, la poca información / conocimiento que se tenía sobre los sistemas OT ha provocado que, a menudo, los equipos de seguridad vayan «a ciegas», sin demasiada información sobre los entornos. Esto ha llevado a que las soluciones de seguridad ICS se hayan ido desarrollando a medida, según iban surgiendo las necesidades en las organizaciones, lo que las ha convertido en un recurso costoso y complejo de mantener.

Las infraestructuras OT requieren la gestión del acceso a las mismas, habitualmente mediante el uso de sistemas propietarios, para mantenimiento y otras tareas, tanto por parte del operador de la infraestructura, como por fabricantes y otras terceras partes. Por este motivo surge la necesidad de gestionar de manera centralizada la seguridad de sedes remotas y/o aisladas. **Fig. 1**

Ante la necesidad de afrontar la ciberseguridad en su infraestructura crítica / entorno industrial, surgen preguntas que nos hacen plantearnos hasta qué punto lo estamos logrando de una forma real y efectiva:

1. ¿Somos capaces de conocer de forma sencilla y automatizada nuestro inventario de activos a lo largo de nuestras plantas, así como conocer qué nuevos sistemas se añaden?
2. ¿Sabemos el nivel de securización de dichos activos (parcheado, firmas, logs, bastionado…) en función de su criticidad?
3. ¿Podemos sincronizar de forma automática y centralizada los parches de los fabricantes (Vendor Qualified Parches) y verificar su instalación?
4. ¿Detectamos anomalías, fallos no intencionados o comportamientos maliciosos (malware) en las comunicaciones SCADA / ICS?
5. En caso de incidente en un sitio remoto, ¿es capaz el equipo de seguridad de recibir una alarma precisa sobre los dispositivos afectados? ¿Podemos acceder remotamente de forma segura y granular para el diagnóstico y cierre del incidente?
6. ¿Podemos monitorizar y gestionar globalmente todo lo anterior mediante un cuadro de mandos en tiempo real?

> «En entornos industriales es imprescindible mantener intactas las capacidades de operación, observación y control de los sistemas OT»

Para solucionar estas casuísticas, InnoTec System, a través de sus alianzas con empresas líderes en la seguridad de OT, ofrece una solución para la provisión y gestión centralizada de seguridad OT, a través de un acceso remoto seguro.

Para la protección de sus sistemas OT, InnoTec propone un enfoque de Seguridad a 5 niveles:

- **Identificación**: Descubrimiento e inventariado automatizado de dispositivos.
- **Protección**: Entrega y despliegue automatizada de parches y actualizaciones (AV, S.O. y dispositivos).
- **Detección**: Recolección y gestión de registros de seguridad, junto con análisis de incidentes.
- **Respuesta**: Acceso remoto seguro dispositivo a dispositivo.
- **Recuperación**: Backup y restauración. **Fig. 2**

Fotos: ***Innotec***

[1] Palabras del Secretario de Estado de Seguridad, Francisco Martínez, al presentar el nuevo Plan de Protección de Infraestructuras críticas el pasado 8 de marzo.

[2] Así lo señala el Centro de Protección de Infraestructuras Críticas, CNPIC, dependiente de la Secretaria de Estado de Seguridad, del Mº del Interior.