SMARTGRID

Las redes eléctricas representan probablemente la estructura conectada más grande e importante de cualquier país desarrollado.
En el caso particular de España puede decirse que en su mayoría están diseñadas y en funcionamiento desde mediados del siglo pasado, afirmación que a buen seguro es aplicable con carácter general a cualquier país.
Es por ello que la naturaleza de las instalaciones e infraestructuras que tradicionalmente han dado soporte a la red tenían un bajo nivel de exposición a ciberataques al no estar conectadas a redes corporativas o redes de datos fácilmente accesibles. Era suficiente la protección física de las instalaciones y un correcto mantenimiento de los equipos.

Desde finales de los años 90 se han producido cambios legislativos del mercado y un interés por la eficiencia que han propiciado la evolución tecnológica en diferentes puntos de la cadena de valor del suministro eléctrico (redes de transporte, operación del sistema eléctrico, equipos de medida, etc.).
Como consecuencia de ello estamos asistiendo al desarrollo de una red eléctrica más inteligente (Smart Grid) pero inherentemente más automatizada y más interconectada. Se espera que para 2018 en España todos los contadores de consumo sean smart-meters y en este nuevo escenario cobra especial relevancia el intercambio, procesamiento y almacenamiento de datos entre los dispositivos embebidos que controlan el comportamiento de los componentes de la red inteligente.

Hoy día existen ya herramientas capaces de identificar sistemas industriales visibles desde redes públicas y que presentan configuraciones débiles, se han publicado listas de vulnerabilidades de sistemas SCADA ampliamente implantados, se pueden encontrar incluso vídeos que instruyen sobre cómo realizar ataques de denegación de servicio sobre dispositivos que se comunican por PLC. No resulta difícil imaginar cuál será el siguiente paso y los operadores deben tomar medidas para estar preparados. El número de incidentes está creciendo y ya se han registrado intentos de ciberataques mediante apagones eléctricos como arma entre países en conflicto o mediante la identificación de patrones de consumo para detectar la presencia física de personas en su vivienda.

Como consecuencia de todo lo anterior, existe una preocupación creciente en los gobiernos para la protección de la red eléctrica y buena prueba de ello es la legislación sobre la Protección de Infraestructuras Críticas, entre las que probablemente se contarán algunas de las que dan soporte a las redes inteligentes.

VISIÓN DE INDRA

Los operadores afrontan el desafío de proteger y asegurar el suministro eléctrico frente a amenazas que hace tan sólo unos años ni siquiera existían o eran altamente improbables. Ya no sirve el tradicional enfoque de seguridad por oscuridad porque no existe un aislamiento estanco entre las redes corporativas y las redes de control industrial y tampoco sirve proteger simplemente el acceso físico a la instalación, Indra considera necesario un enfoque más global que integre la ciberseguridad para garantizar que los procesos de suministro eléctrico no se vean afectados en su correcto funcionamiento protegiendo al mismo tiempo las vidas de las personas que puedan verse afectadas por las consecuencias de un ciberataque (operarios de planta, dependientes de sistemas de soporte vital, control de tráfico, etc.) y previniendo el fraude a gran escala.

Este enfoque integral de la seguridad trasciende lo técnico y requiere también transformar la cultura de las organizaciones, concienciando al personal clave, definiendo nuevos "modos de hacer con seguridad" y asignando responsabilidades. Para ayudar a los operadores a abordar este reto y definir su plan de seguridad, Indra aporta su contrastada experiencia en los tres ejes fundamentales: seguridad física, ciberseguridad y, por supuesto, negocio. Se tendrá en cuenta la definición de la estructura organizativa, se identificarán amenazas y riesgos, y se propondrá un programa de trabajo para asegurar las instalaciones desde el punto de vista de la Seguridad Global. Indra desea ser un referente en este campo y por ello tiene presencia activa en diferentes grupos de trabajo, nacionales e internacionales, cuya misión es evolucionar la seguridad de la Smart Grid.

MEDIDAS PARA REDUCIR EL RIESGO

CÓMO QUIERO SER

Identificar el marco de referencia (legal y/o de buenas prácticas).

CÓMO SOY

Catalogar aquellos procesos que son críticos y los activos que los soportan.

Analizar los riesgos que afectan a los activos críticos.

Verificar qué vulnerabilidades técnicas están presentes en los equipos.

CÓMO ME TRANSFORMO

Trazar un plan de despliegue de las medidas de seguridad para mitigar los riesgos.

Adaptar la organización al nuevo "modo de hacer con seguridad".

Concienciar y crear cultura de seguridad.

CÓMO ME MANTENGO Y MEJORO

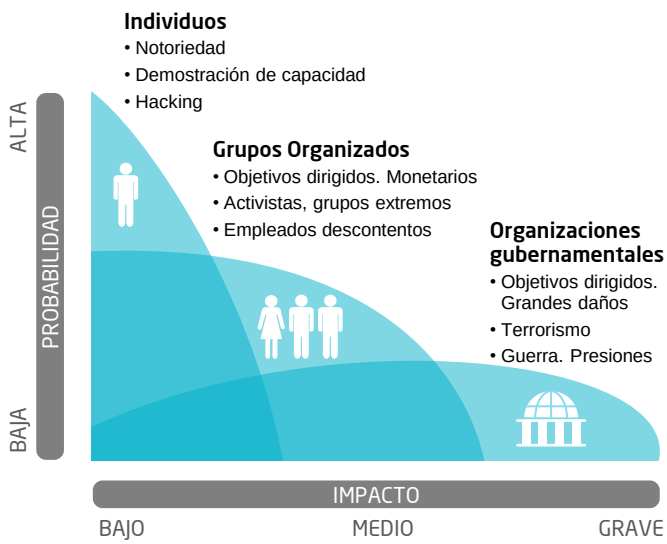
Gestionar los incidentes de seguridad.

Supervisar la eficacia de la seguridad realizando auditorías periódicas.

Asegurar la continuidad de los procesos críticos.

Incluir los requisitos de seguridad en cualquier proyecto desde el comienzo.

Colaborar activamente en grupos de trabajo y foros especializados.



PLAN DE SEGURIDAD GLOBAL

SEGURIDAD TIC
- Amenazas
- Vulnerabilidades
- Tecnologías
- Soluciones

INGENIERÍA & CONTROL
- Sistemas
- Entono
- Operación
- Requisitos

SEGURIDAD FÍSICA
- Documentación
- Personal
- Zonas restringidas

indra

Avda. de Bruselas, 35
28108 Alcobendas
Madrid (España)
T +34 91 480 60 00
F +34 91 480 60 31
indracompany.com