eBook

¿QUÉ RETOS PRESENTA ACTUALMENTE LA SEGURIDAD INDUSTRIAL?

Nextel S.A.
Ingeniería y Consultoría

¿QUÉ RETOS PRESENTA ACTUALMENTE LA SEGURIDAD INDUSTRIAL?

La seguridad de los sistemas de información es esencial para la continuidad de cualquier negocio y en **Nextel** somos plenamente conscientes de ellos. Por eso trabajamos para encontrar soluciones que garanticen la protección de las empresas con servicios, metodologías y sistemas de calidad, siempre certificados por las principales normativas internacionales. Nuestra atención se centra especialmente en la seguridad de los sistemas industriales, la llamada Industria 4.0 que engloba en su seno las siempre complejas infraestructuras críticas.

En los últimos años se han vivido ataques lo suficientemente importantes como para afectar no solo a la continuidad de negocio sino incluso a la buena imagen de grandes empresas, que hasta entonces eran consideradas prácticamente intocables por su envergadura y seguridad interna, como pueden ser multinacionales del sector de los seguros, bancos o incluso centrales nucleares.

A la amenaza cada vez más acuciante de vivir ataques como los sufridos por estas corporaciones, se añade el crecimiento sin control de la llamada Internet de las Cosas, que conecta a Internet muchos dispositivos que no han pasado los controles de seguridad adecuados, convirtiéndose en un peligro para todos en forma de ataques de Denegación Distribuida de Servicio o como puertas de entrada ilegal a las redes corporativas.

En esta telaraña de riesgos entremezclados y conectados, los datos se configuran como el valor más crítico a ser atacado en una organización normal. Pero todo se complica varios grados cuando no hablamos de la seguridad de una compañía de seguros sino de la seguridad de las máquinas: de la seguridad industrial de una empresa dedicada a la metalurgia, el petróleo o la construcción de palés.

En estos casos la protección tradicional no es suficiente y es preciso desarrollar un plan específico de seguridad tanto para la organización en general y sus oficinas como para su parque de maquinaria. Es necesario redefinir qué proteger y cómo hacerlo, teniendo en cuenta que aquí no hay sólo datos en juego, también la seguridad de las personas y del modelo productivo.

La llamada Industria 4.0 es la nueva revolución industrial que lleva a la digitalización de todos lo procesos de los sistemas industriales e introduce a las empresas en el mundo conectado prácticamente “de golpe”. Las

redes de sensores, los nuevos dispositivos y la comunicación de máquina a máquina (M2M) están cambiando completamente al panorama.

Así, hemos pasado de un entorno totalmente hermético, con el control en manos de un operador, a un mundo conectado a la red, que recibe información de miles y miles de sensores en los entornos de monitorización y la vierte en el accionamiento de los sistemas industriales. Antes, un operario podía controlar el estado de todos los procesos en curso, revisar y tomar acciones en consecuencia desde un panel de control aislado de la red.

Hoy, el operario puede acceder a este panel de control remotamente, desde múltiples ubicaciones, y recibir información en tiempo real procedente de las interfaces de todo tipo de dispositivos que informan de su estado. Este entorno, por estar conectado a la red, se convierte automáticamente en un entorno de inseguridad, donde cibercriminales atacan estos dispositivos para controlarlos remotamente y construir gigantescas "botnets".

El problema es doble porque, por un lado, estamos implantando en nuestro perímetro un conjunto de dispositivos conectados a la red. Y, a la vez, estos dispositivos tienen la problemática creciente de carecer de medidas de seguridad, cifrado y múltiples vulnerabilidades en su "firmware".

Sería el caso por ejemplo de las cámaras de vigilancia IP, que ya han sido usadas más de una vez para crear "botnets" después de que delincuentes tomasen el control masivo de las mismas. En el caso más conocido, el problema de seguridad estaba en el "firmware" de las cámaras, que creaba una puerta trasera que permitía la ejecución de un código remoto. Millones de dispositivos han sido infectados de esta forma y, a día de hoy, aunque exista un parche para esta vulnerabilidad sigue habiendo cámaras con esta puerta abierta.

Hemos visto también casos más graves, relacionados con infraestructuras críticas. El dispositivo vulnerable puede formar parte de la red de control de una subestación eléctrica. El atacante toma el control del dispositivo y ejecuta un ataque, llamado "lateral" porque sucede dentro de la red interna, para acceder a recursos de esta red, tomar el control y comprometer sistemas críticos. En este escenario, podría cortar el suministro eléctrico de pueblos, barrios, hospitales, señales de tráfico, etc.

Otro escenario a tener muy en cuenta como decíamos es la Internet de las Cosas industrial, una tecnología disruptora en el mercado, sin lugar a dudas, que en pocos años será un estándar en cualquier industria que quiera ser competitiva. Pero la seguridad de estos dispositivos y redes de sensores no está siendo lo estricta que debería y se están detectando importantes brechas de seguridad en cifrado de datos, contraseñas inseguras o de fábrica (porque no se siguió el procedimiento de buenas prácticas o simplemente porque no se pueden cambiar), la autenticación entre dispositivos o incluso deficiencias en su diseño físico.

EL COMPROMISO DE NEXTEL CON LA SEGURIDAD INDUSTRIAL

El équipo técnico de Nextel posee amplios conocimientos en el sector de los procesos industriales, dispositivos y sus protocolos (Modbus, Profibus, IEC 104, KNX, Ethercat, RTUs, IEDs o PLCs), de forma que se pueda garantizar la disponibilidad y continuidad del negocio. Para lograrlo, Nextel ofrece diferentes servicios, que cubren todos los ámbitos: desde los proyectos de consultoría a la monitorización de plantas industriales completas, pasando por la integración de la tecnología.

Integración de Sistemas de Prevención y Detección de Intrusiones (IDS/IPS) y cortafuegos industriales.

Comprende la planificación, diseño, configuración y despliegue de soluciones de seguridad, basadas en dispositivos de prevención y detección de intrusiones, y cortafuegos industriales que posibiliten la segmentación de la red industrial (OT) y de la red de administración (IT) y el análisis de tráfico de ambas redes. Esta segmentación previene de los incidentes de seguridad, como puede ser código malicioso que intente entrar por las oficinas y de ahí saltar a las máquinas de producción industrial.

Bastionado de equipos y redes industriales.

Configuración de los sistemas industriales, de forma que se minimicen sus vulnerabilidades, implementando para los servicios necesarios las políticas de seguridad acordes a su criticidad y deshabilitando los servicios no utilizados.

Análisis de riesgos de seguridad industrial.

Evaluación cuantitativa y análisis de riesgos, así como adecuación a las buenas prácticas. Es un servicio orientado a identificar, evaluar y clasificar cuantitativamente y de forma periódica los principales riesgos físicos y lógicos, tanto en las redes de administración como la red industrial, que afectan a los procesos industriales y a los activos que los soportan dentro de una organización. Este análisis está basando en la metodología de análisis de riesgos Magerit v3, en conjunción con los principales estándares de seguridad IACS, como ISA-99/IEC 62443, NIST 800 o NERC-CIP.

Auditorías técnicas de seguridad.

Comprenden:

- Análisis de vulnerabilidades.
- Test de intrusión interno/externo.
- Análisis de código fuente de software SCADA y equipamiento industrial.
- Análisis de comportamiento de la red industrial.

Análisis GAP de cumplimiento frente a las principales guías de buenas prácticas y estándares de seguridad.

Incluye la integración del Sistema de Gestión de Ciber-seguridad Industrial (SGC).

LAS ESPECIALES NECESIDADES DE SEGURIDAD DE LOS SISTEMAS SCADA

A la complejidad cada vez mayor que nos encontramos a la hora de aplicar seguridad en toda la infraestructura, lo que pide nuevos enfoques en la forma como se entrega la información y la estructura de todo el stack tecnológico, debemos añadir nuevos retos y complejidades cuando de lo que se trata es de proteger sistemas SCADA.

SCADA es el acrónimo de "Supervisory Control And Data Acquisition" (Supervisión, Control y Adquisición de Datos). Se emplea para definir los programas para ordenadores que permiten controlar y supervisar procesos industriales a distancia. Esto facilita la retroalimentación en tiempo real con dispositivos que están monitorizando los procesos, como los sensores, y controla estos procesos automática-mente. Un sistema SCADA recoge toda la información que genera el proceso productivo, desde la supervisión hasta el control de producción, de calidad o almacenamiento de datos, y permite su gestión.

En los sistemas SCADA la seguridad es muy importante, más aún cuando muchos gestionan y monitorizan infraestructuras críticas.
Un fallo o una interrupción del funcionamiento de uno de los componentes del sistema puede suponer un impacto negativo sobre el funcionamiento de estas infraestructuras.
Por esta razón es esencial establecer un proceso de auditoría de seguridad, para garantizar que estas redes e infraestructuras sean siempre fiables y estén disponibles.

La evolución de los sistemas SCACA a sistemas más distribuidos presenta nuevos retos de seguridad que presentamos a continuación:

- Actualmente, estos sistemas usan componentes Off-The-Shelf (COTS) o componentes “sacados de la caja”, que podríamos definir como elementos no-desarrollativos de suministro, no personalizados, que se venden en grandes cantidades en el mercado comercial. Aunque fueron adquiridos en favor de reducir costes y tiempos de implementación, ahora juegan en contra de la seguridad: existen bases de datos públicas con listas de vulnerabilidades de componentes COTS, lo que aumenta y mucho los riesgos.

- La apertura de las redes corporativas y de control pone al descubierto protocolos de automatización industrial sobre TCP/IP que, la mayoría de ellos, presentan vulnerabilidades al no disponer de los mecanismos específicos de seguridad.

- La aparición de servicios web para la monitorización y gestión del panel SCADA conlleva un punto adicional de inseguridad, donde se podría ver comprometida la base de datos relacional.

- La validación tradicional de usuarios, de usuario-contraseña, puede ser insuficiente cuando el sistema ya no está cerrado. Se necesitan nuevos métodos de autenticación.

- La nueva arquitectura de los entornos SCADA, donde interviene Internet, obliga a revisar todos los mecanismos de seguridad, como cortafuegos (NGFW), Sistemas de Detección de Intrusiones (IDS), de Prevención de Intrusiones (IPS), antivirus, antimalware, conexiones seguras mediante túneles VPN, servidores RADIUS, etc.

RECOMENDACIONES PARA SECURIZAR UN SISTEMA SCADA

Este nuevo modelo de control industrial precisa de diversas acciones que recomendamos sean puestas en práctica lo antes posible:

Una política de usuarios fuerte.

En entornos SCADA es necesaria la máxima seguridad, que en cuanto a política de usuarios recomendaríamos se basase en autenticación biométrica, incluyendo elementos electrónicos para la validación, como chips RFID (acrónimo de "Radio Frequency Identification" o identificación por radiofrecuencia), vídeo, etc. En el marco de un servicio web es recomendable definir y establecer un conjunto sólido de roles y limitar al máximo los permisos de cada usuario.

Auditar el código de nuestra plataforma.

Las interfaces web contienen a menudo errores de programación que pueden ser explotados mediante ataques de XSS (Cross Site Scripting), SQL Inject o fuerza bruta. Con herramientas de auditoría de código podemos detectar posibles vulnerabilidades que permitan estos ataques. El segundo paso sería realizar un informe con propuestas de mejora, para optimizar la calidad de nuestro software.

Por otra parte y para mantener unas mejores prácticas, debemos revisar periódicamente si hay nuevas versiones del software o firmware, para parchear cualquier vulnerabilidad detectada.

Implementar una política de recuperación

Un sistema SCADA en una infraestructura crítica no puede fallar. Es por ello muy recomendable establecer desde el principio un plan de recuperación ante desastres, donde los usuarios asignados conozcan la existencia de este protocolo de recuperación así como del funcionamiento de la infraestructura. Adicionalmente y como en cualquier plan de contingencia, deben disponer de los datos de contacto y pautas para responder con agilidad a cualquier incidente.

Actualizar las políticas de seguridad

La nueva perspectiva que se presenta a la hora de manejar sistemas SCADA obliga a revisar las configuraciones de hardware y software, auditorías, seguridad física y seguridad en las comunicaciones. Es esencial mantener este aspecto en mejora continua, al ser uno de los más importantes dentro de la protección de un entorno SCADA. Respecto a estas políticas de seguridad, habría que tener en cuenta diversos aspectos:

- En el caso de comunicaciones inalámbricas recomendamos un plan de mejores prácticas que incluya desactivar los puertos inactivos y el "broadcast" del SSID, emplear cifrado TLS y WPA con un servidor RADIUS y revisar los sensores inalámbricos de los procesos de control.

- El cortafuegos es la primera línea defensiva. Cisco tiene un porfolio extenso en seguridad perimetral con protección específica para entornos industriales con Cisco ISA.
  Es importante ampliar este nivel de protección mediante soluciones de nueva generación que no solo llegan a la capa de red, sino que son capaces de inspeccionar el tráfico y operar en la capa de aplicación directamente. Recomendamos adicionalmente revisar las políticas del IDS e IPS y emplear DMZ.

- Al deslocalizar las operaciones de control de un sistema SCADA, los procesos de cifrado deben ser revisados al alza, del mismo modo que los métodos de autenticación. En el caso de que la red de control tenga una conexión directa a Internet, es obligado implementar una VPN ("Virtual Private Network" o red privada virtual) con cifrado SSL dentro de un túnel IPSec o similar.

- Cuando la comunicación se realiza a un dispositivo de campo, se usan protocolos como Modbus o DNP3, que por defecto carecen de medidas de seguridad. El sistema debe gestionar el cifrado de forma transparente a través de un dispositivo mediador. Si se está usando protocolo TCP/IP será necesario establecer procedimientos de seguridad estándar que cifren la comunicación de extremo a extremo.

- El almacenamiento debe tenerse también en cuenta, al ser un factor de riesgo para un posible ataque de elevación de privilegios. Es recomendable establecer un sistema de cifrado de datos para la información crítica, dado que el acceso a la misma podría aumentar la gravedad de un posible ataque. En este punto, incluimos también las bases de datos, aunque su trato debería ser algo diferente al tener que auditar su rendimiento.

- Por último, la monitorización puede ser una excelente herramienta de protección. Un consumo excesivo de CPU, un proceso activo de escritura masiva de ficheros, o un acceso descontrolado a muchas direcciones simultáneas pueden ser síntomas de una intrusión o compromiso y dar margen suficiente a un operador para tomar las medidas necesarias para evitar una propagación mayor o daños.

Estas son algunas de las recomendaciones que te proponemos, aunque no son todas ni mucho menos, para establecer una seguridad óptima en un entorno industrial.

NUESTRA ELECCIÓN: CISCO 3000 SERIES INDUSTRIAL SECURITY APPLIANCES

Dentro de las soluciones para el control y protección de redes industriales, destaca por su probada efectividad Cisco 3000 Series Industrial Security Appliances (ISA), especialmente a la hora de simplificar el funcionamiento así como proteger los dispositivos que forman parte de la Internet de las Cosas.

Como ya hemos comentado, las redes industriales y sistemas SCADA tienen necesidades muy específicas y avanzadas de protección contra amenazas, requiriendo una solución robusta que ayude a garantizar unos servicios seguros y confiables. Dentro del porfolio de soluciones ofrecidas por Cisco, destacan las Cisco 3000 Series Industrial Security Appliances (ISA) con FirePOWER Services.

Cisco 3000 Series Industrial Security Appliances es una robusta solución que incluye la más amplia gama de controles de acceso, detección de amenazas y visibilidad de aplicaciones para los entornos más duros y exigentes de la industria. El Industrial Security Appliance 3000 extiende la red, como un sensor y como un ejecutor, a los entornos de Internet de las Cosas.

Estas son sus principales características:

- Visibilidad y control de protocolos incluyendo los principales como son DNP3, CIP, Modbus, IEC 61850 y aplicaciones de Omron, Rockwell, GE, Schneider, Siemens.
- Capacidad de trabajar en ambientes hostiles, con un rango de temperatura de -40° a 60°C
- Protección ante vibraciones, golpes, sobretensiones e inmunidad al ruido eléctrico.
- Cuatro puertos de enlace ascendente de 1 Gigabit Ethernet, que proporcionan múltiples opciones de diseño resilientes.
- Cumplimiento de las especificaciones multisectoriales para la automatización industrial, los ITS y los entornos de subestaciones eléctricas.
- Un diseño de unidad de carril DIN compacto, con características LED industriales para facilitar el monitoreo.
- Convección sin ventilador y sin partes móviles para mayor durabilidad.
- Gestión múltiple a través de cientos de dispositivos
- Acceso y control específicos del usuario.
- Detección de amenazas probada con más de 25.000 reglas para la más amplia gama de protección operacional de la tecnología.
- Visibilidad y control de la infraestructura DMZ, aplicaciones IoT y protocolos

Con un peso de solo 1,9 kg, pocos dispositivos pueden ofrecer tanto, con la garantía de ser Cisco y la ventaja de proteger no sólo la red industrial sino además prestar especial atención al que sin duda será un importante caballo de batalla en los próximos años, como es la Internet de las Cosas.

Nextel S.A.
Ingeniería y Consultoría