Seguridad de los sistemas de control industrial

Por Enrique Larrieu-Let
elarrieulet@gmail.com

Para los que, como yo, hemos disfrutado de la seguridad de los Sistemas de Control industriales (ICS, del inglés, *Industrial Control System*) totalmente aislados, y luego poco a poco fuimos testigos de cómo inexorablemente esa calma se veía invadida; este artículo, basado en las recomendaciones del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, del inglés, *National Institute of Standards and Technology*), pretende promover la toma de conciencia para el establecimiento de sistemas de control industriales seguros. Estos ICS incluyen los sistemas de supervisión, control y adquisición de datos (SCADA, del inglés, *Supervisory Control and Data Acquisition*), los sistemas de control distribuido (DCS, del inglés, *Distributed Control System*) y los controladores lógicos programables (PLC, del inglés, *Programmable Logic Control*), entre otros sistemas de control que se encuentran a menudo en los sectores de control industrial.

La importancia de cuidar los ICS radica en que se utilizan normalmente en industrias tales como electricidad, agua, petróleo, gas natural, energía nuclear, transporte, química, farmacéutica, salud, alimentos, y en la fabricación discreta (por ejemplo, automotriz, aeroespacial y bienes duraderos), muchas de ellas pertenecientes a las infraestructuras críticas de un país.

Los sistemas SCADA, generalmente, se utilizan para controlar los activos dispersos utilizando la adquisición de datos y control de supervisión centralizada. Los DCS se utilizan, generalmente, para el control de los sistemas de producción dentro de un área local. Los PLC se utilizan, generalmente, para el control discreto en aplicaciones específicas y, también generalmente, proporcionan un control para regular alguna variable. Estos sistemas de control, que a menudo son sistemas altamente interconectados y mutuamente dependientes, suelen ser vitales para el funcionamiento de las infraestructuras críticas de una organización y hasta de un país.

Todo tiene sus pros y sus contras. Inicialmente, los ICS tenían poco parecido con los sistemas de tecnología de la información y comunicación (TIC) tradicionales dado que eran sistemas aislados que ejecutaban protocolos de control propietarios y utilizaban hardware y software especializado. Si bien uno vivía

Enrique Larrieu-Let
Ingeniero, CISM,
Profesional en Seguridad y Tecnologías de Sistemas de Información
Asociación de Auditoría y Control de Sistemas de Información - ADACSI, IAIA, Universidad del Salvador

tranquilo desde el punto de vista de la seguridad, resultaba poco práctico desde lo operativo. Es indudable que la tendencia nos dirige hacia la conectividad de 'todo con todo'. Permanentemente, surgen dispositivos que utilizan el conjunto de protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*, 'protocolo de control de transmisión/protocolo de Internet') que está reemplazando a las soluciones propietarias, lo que incrementa la posibilidad de vulnerabilidades de seguridad y facilita la aparición de ciberincidentes. Por lo expresado, es fundamental identificar las amenazas y vulnerabilidades de estos sistemas y proporcionar recomendaciones, buenas prácticas y contramedidas de seguridad para mitigar los riesgos asociados y reducir el impacto de los ciberincidentes de seguridad.

Los ICS están adoptando soluciones de TIC para brindar conectividad y capacidades de acceso remoto a los sistemas de negocio corporativos, y además están siendo diseñados e implementados usando computadoras estándar, sistemas operativos y protocolos de red; están empezando a parecerse a los sistemas de TIC tradicionales. Esta integración es compatible con las nuevas capacidades de TIC, pero disminuye significativamente el aislamiento de los ICS con el mundo exterior respecto de los sistemas predecesores, creando una mayor necesidad de proporcionar seguridad a estos sistemas. Si bien las soluciones de seguridad han sido diseñadas para hacer frente a los problemas de seguridad en los sistemas típicos de TIC, se deben adicionar precauciones especiales cuando se introducen estas mismas soluciones en los entornos del ICS. En algunos casos, hasta se requieren nuevas soluciones de seguridad específicas que se adapten a dichos entornos.

A pesar de que algunas características son similares, los ICS también tienen características que difieren de los sistemas de procesamiento de información y comunicación tradicionales. Muchas de estas diferencias se derivan del hecho de que la lógica de ejecución en los ICS tiene un efecto directo en el mundo físico. Algunas de estas características incluyen: riesgo significativo para la salud y la seguridad de las vidas humanas y daños graves al medioambiente, así como graves problemas financieros, tales como pérdidas de producción, impacto negativo para la economía de una nación y compromiso de las infraestructuras críticas.

En sus comienzos, las implementaciones de los ICS solo eran susceptibles a las amenazas locales, pues la mayoría de sus componentes se encontraban en zonas físicamente seguras y aisladas de las redes o sistemas informáticos. Sin embargo, esta tendencia hacia la integración de los ICS con las redes de TIC proporciona significativamente menos aislamiento para los ICS desde el mundo exterior que los sistemas predecesores, incrementa las amenazas y extiende el perímetro de seguridad. Con el acceso a los ICS desde redes remotas a través de redes inseguras como Internet, el perímetro de seguridad se extiende a todo el mundo y, si le agregamos además el acceso a través de dispositivos móviles y las redes inalámbricas, el universo de posibles atacantes se torna inmanejable e imposible de identificar.

Las amenazas a los sistemas de control pueden provenir de varias fuentes, incluyendo desde simples errores de configuración, negligencia en la gestión de operación o mantenimiento, empleados descontentos, intrusos maliciosos, fallas accidentales, gobiernos hostiles y grupos terroristas, hasta desastres naturales. Los objetivos de seguridad de los ICS tienen típicamente como prioridad 1) la disponibilidad; 2) la integridad, y 3) la confidencialidad, en ese orden.

Los posibles incidentes que un ICS puede enfrentar son los siguientes:

- Bloqueo o demora del flujo de información a través de las redes de los ICS, que podría interrumpir el funcionamiento del ICS y, como consecuencia, algún proceso crítico.
- Cambios no autorizados a las instrucciones, comandos o umbrales de alarma, lo que podría dañar, deshabilitar o apagar algún equipo, crear impactos ambientales y/o poner en peligro a la vida humana.

- Envío de información inexacta a los operadores del sistema, ya sea para disimular cambios no autorizados o para hacer que los operadores inicien acciones inapropiadas, lo que podría tener múltiples efectos negativos.
- Modificación del software de ICS o sus parámetros de configuración, infección del software de ICS con malware, lo que podría tener varios efectos negativos.
- Interferencia con el funcionamiento de los sistemas de seguridad, lo que podría poner en peligro a la vida humana.

Los principales objetivos de seguridad para una implementación de un ICS deben incluir lo siguiente: restricción del acceso lógico a la red del ICS y a la actividad de la red, restricción del acceso físico a la red y a los dispositivos de ICS, protección de los componentes individuales del ICS, mantenimiento de las operaciones en condiciones adversas y restauración del sistema después de un incidente.

- Restricción del acceso lógico a la red del ICS y a la actividad de la red: esto incluye el uso de una arquitectura de red de zona desmilitarizada (DMZ, del inglés, *Demilitarized Zone*) con los firewalls para evitar que el tráfico de red pase directamente sin filtro entre las redes corporativas y la del ICS, y que tenga mecanismos de autenticación y autorización con credenciales separadas para los usuarios de las redes corporativas y del ICS. El ICS también debe utilizar una topología de red que tenga múltiples capas, logrando que las comunicaciones más críticas ocurran en la capa más segura y fiable.
- Restricción del acceso físico a la red y a los dispositivos de ICS: el acceso físico no autorizado a los componentes podría causar graves trastornos de la funcionalidad del ICS. Se debe utilizar una combinación de controles de acceso físico, tales como cerraduras, lectores de tarjetas, y/o dispositivos biométricos de seguridad.
- Protección de los componentes individuales del ICS: esto incluye el despliegue de parches de seguridad de la manera más expedita posible, después de ponerlos a prueba en condiciones de campo; deshabilitar todos los puertos y servicios no utilizados; restringir privilegios de los usuarios de los ICS solo a aquellos que sean necesarios en función de la necesidad de saber y de hacer de cada persona; seguimiento y monitoreo de las pistas de auditoría, y el uso de los controles de seguridad, tales como software antivirus y software de comprobación de integridad de archivos cuando sea técnicamente posible para prevenir, desalentar, detectar y mitigar el malware.
- Mantenimiento de las operaciones en condiciones adversas: esto implica diseñar el ICS para que cada componente crítico tenga una contraparte redundante. Además, si falla un componente, debe fallar de una manera que no genere tráfico innecesario en el ICS u otras redes, o no cause otro problema en cascada en otros sitios.
- Restauración del sistema después de un incidente: los incidentes son inevitables, y un plan de respuesta a incidentes es esencial. Una característica importante de un buen programa de seguridad es la rapidez con que un sistema puede recuperarse después de haberse producido un incidente.

Para abordar adecuadamente la seguridad en un ICS, es esencial contar con un equipo multifuncional de ciberseguridad que comparta su variado dominio del conocimiento y experiencia para evaluar y mitigar los riesgos a los ICS. El equipo de ciberseguridad puede consistir en: un miembro del personal de TI de la organización, un ingeniero de control, un operador de los sistemas de control, un experto en seguridad de sistemas y de redes, un miembro del equipo de dirección y un miembro del departamento de seguridad física.

Para la continuidad e integridad, el equipo de ciberseguridad debería consultar con el proveedor del sistema de control y/o integrador de sistemas también. El equipo de ciberseguridad debe reportar

directamente a la máxima autoridad del sitio (por ejemplo, el CISO —*Chief Information Security Office*, 'director de seguridad de la información'— de la empresa), o a quien asuma la responsabilidad completa y la responsabilidad por la ciberseguridad del ICS. Un programa de seguridad de la información eficaz para un ICS debe aplicar una estrategia conocida como "defensa en profundidad", que consiste en capas de mecanismos de seguridad de tal manera que el impacto de una falla en cualquiera de los mecanismos de alguna capa se pueda ver compensado por los mecanismos de seguridad de otra capa.

En ICS típicos, una estrategia de defensa en profundidad debe:

- Desarrollar políticas de seguridad, procedimientos, capacitación y material educativo que se aplican específicamente al ICS;
- tener presente a la seguridad en todo el ciclo de vida del ICS, desde diseño de la arquitectura y la puesta en marcha de la instalación, hasta el mantenimiento y desmantelamiento;
- implementar una topología de red para el ICS que tenga múltiples capas, logrando que las comunicaciones críticas ocurran en la capa más segura y fiable;
- proporcionar la separación lógica entre las redes corporativas y las del ICS (instalando, por ejemplo, un servidor de seguridad de inspección de estado entre ellas);
- emplear una arquitectura de red DMZ (es decir, evitar que ocurra el tráfico directo entre las redes corporativas y las del ICS);
- asegurar que los componentes críticos sean redundantes y se encuentren en redes redundantes;
- diseñar los sistemas críticos para que su degradación sea progresiva (sistema tolerante a fallos) para prevenir los episodios catastróficos en cascada;
- desactivar los puertos y servicios no utilizados en los dispositivos ICS después del período de ensayo para asegurar que esto no tendrá un impacto en el funcionamiento del ICS;
- restringir el acceso físico a la red y a los dispositivos de los ICS;
- restringir los privilegios de acceso a los ICS solo a aquellos usuarios que los necesiten, es decir, establecer un control de acceso basado en roles y configurar cada rol según el principio del menor privilegio y de la necesidad de saber y hacer;
- imponer el uso de mecanismos de autentificación y credenciales diferentes para los usuarios tanto de la red del ICS como de la red corporativa;
- promover el uso de tecnologías modernas, tales como tarjetas inteligentes y dispositivos biométricos para la verificación de identidad personal;
- cuando sea técnicamente posible, efectuar controles de seguridad tales como instalar software de detección de intrusiones, software antivirus y software para comprobar la integridad de archivos, para prevenir, desalentar, detectar y mitigar la introducción, exposición y propagación de software malicioso;
- donde se considere apropiado, aplicar técnicas de seguridad como el cifrado y/o resúmenes (*hashes*) criptográficos al almacenamiento de datos del ICS y las comunicaciones;
- priorizar la implementación de parches de seguridad después de probar dichos parches en condiciones de campo en un sistema de prueba, si es posible, antes de la instalación en el ICS;
- controlar y monitorear las pistas de auditoría en las áreas críticas de los ICS.

En los siguientes artículos, se ampliarán los temas mencionados en este. Se tratarán las amenazas y potenciales vulnerabilidades de los sistemas ICS, se analizarán los factores de riesgo y se describirán algunos posibles escenarios de incidentes. También se establecerán las pautas y recomendaciones para desarrollar e implementar un programa de seguridad. Asimismo se sugerirán buenas prácticas en lo referido a seguridad en la red y se describirán los controles de seguridad de gestión, operativos y técnicos. ❖