Seguridad de la Información en Sistemas SCADA

Baquero Salamanca, Germán Darío
germanbaquero@gmail.com
Universidad Piloto de Colombia

Resumen—El presente artículo pretende mostrar la importancia de la seguridad de la información en los sistemas de control SCADA, empezando con una introducción donde se explica que son los sistemas de control industrial y los sistemas SCADA. Siguiendo con la importancia que tiene estos sistemas SCADA, continuando con las principales amenazas, riesgos y los controles de protección, finalizando con algunas guías de buenas prácticas que se pueden implementar en estos sistemas que permiten mejorar la seguridad de la información.

Abstract—This paper just pretend to show the importance of information security over SCADA Control Systems, starting with an introduction explaining what are industrial control system and SCADA control system. Following with the importance what have these SCADA systems, continuing with the main threats, risks and protective controls, concluding with some guidelines of good practice that may be implement in these systems that improve the secure of information.

Índice de Términos—*CONTROLES-RIESGOS-SCI-SCADA-SISTEMAS DE CONTROL-SEGURIDAD DE LA INFORMACIÓN-TECNOLOGÍAS.*

I. INTRODUCCIÓN

Los sistemas de control industrial (SCI) son sistemas de información especializados que interactúan físicamente con el ambiente y muchos forman parte de la infraestructura crítica de un país. SCI es un término general que incluye varios tipos de sistemas de control como SCD (Sistemas de Control Distribuido), SCP (Sistemas de Control de Procesos), PLC´s (Controladores Lógicos Programables) y SCADA (Supervisión, Control y Adquisición de Datos).

Los sistemas SCADA son sistemas altamente distribuidos que se utilizan para controlar los activos geográficamente dispersos, a menudo dispersos en miles de kilómetros cuadrados, donde la adquisición de datos y control centralizados son críticos para el funcionamiento del sistema. Se utilizan en los sistemas de distribución, como los sistemas de distribución de agua, alcantarillado, tuberías de petróleo y gas natural, también en las redes de energía eléctrica, los sistemas de transporte ferroviario y aéreo, en las instalaciones de centros de investigaciones, en los sistemas de seguridad, en sistemas de alarmas, en los controles de comunicación, en las plantas nucleares, en los parques de diversiones, en los sistemas de riego, en las entidades bancarias, en los servicios gubernamentales y en los servicios de emergencias.

Un centro de control SCADA realiza una supervisión centralizada y el control de los sitios de campo a través de redes de comunicaciones de larga distancia, incluyendo las alarmas de control y los datos de estado de procesamiento. Con base en la información recibida de las estaciones remotas, automatizados o los comandos de control del operador impulsado se puede empujar a los dispositivos de control de la estación remota, que se refieren a menudo como los dispositivos de campo. Los dispositivos de campo controlan las operaciones locales, tales como la apertura y cierre de las válvulas y los interruptores, la recogida de

datos de los sistemas de sensores y vigilancia del medio local para las condiciones de alarma.

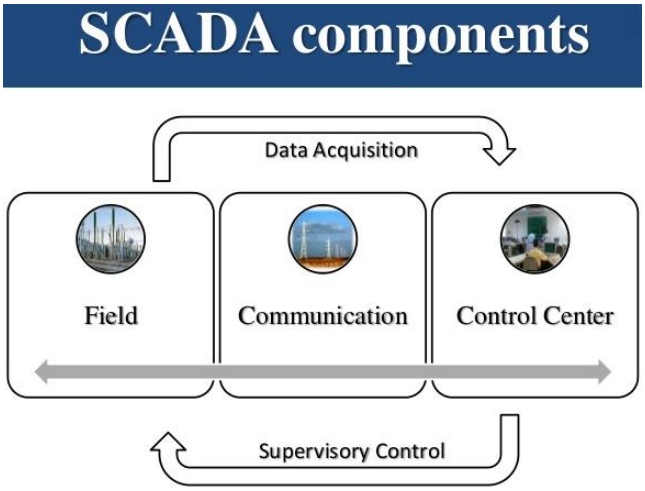
Actualmente, los sistemas SCADA raramente incorporan seguridad en sus protocolos de comunicación y estos protocolos contienen diferentes vulnerabilidades brindando información que permite obtener datos relevantes de la infraestructura. Además el incremento de las conexiones a internet de estos sistemas pone mucho más en riesgo la seguridad. Y finalmente recientemente noticias hablan sobre errores del software de los sistemas SCADA permite controlar 7600 plantas industriales lo cual es una situación grave de seguridad [1].

II. IMPORTANCIA DE LA SEGURIDAD EN LOS SISTEMAS SCADA

El objetivo principal de los sistemas SCADA, es facilitar en tiempo real la retroalimentación del sistema, controlando automáticamente el proceso con los datos de los diferentes sensores que lo conforman. Asimismo, suministra datos en tiempo real del estado del proceso, pudiendo tener información sobre el control de calidad, los niveles de producción, y otras variables que ayudan a la gestión del proceso.

La importancia de estos sistemas radica en como los daños que sufra la infraestructura crítica puede afectar el poder nacional. Éste tiene sus factores como lo es económico, político, social, militar y tecnológico. También dentro de estos factores se encuentra la industria. Y si una amenaza afecta la industria de un estado, este pierde sus capacidades de generar y producir y por lo tanto los efectos lo siente la población y su bienestar.

En la siguiente imagen ilustra el esquema de los sistemas SCADA con sus respectivos componentes que permite el funcionamiento adecuado de su infraestructura, contando con un control central que se conecta al centro de comunicaciones dando la supervisión y control, y adquirir los datos.



Esquema componentes SCADA. Tomado de http://www.slideshare.net/AnsumanMansingh/scada-systems

III. AMENAZAS, FACTORES DE RIESGOS Y VULNERABILIDADES

El principal riesgo de una falla en los sistemas SCADA son pérdidas humanas. Otros riesgos a considerar son el riesgo de daños en la infraestructura empresarial como operaciones detenidas, daños costosos, y tiempo de recuperación elevado. Además, el riesgo a la infraestructura metropolitana como en las refinerías de petróleo y estaciones de gas.

En muchos casos las vulnerabilidades están asociadas con la antigüedad de los equipos, sistemas operativos viejos (Windows NT, Windows 3.11, SCOUNIX) y además no tienen los parches de seguridad. Todo esto en objetivos para los atacantes. Como la reciente noticia de seguridad informática que habló que el sistema SCADA Yokogawa fue lanzado sobre Windows 98 en el año 1998 que permite supervisar y controlar maquinaria en grandes instalaciones industriales, que encontraron errores de seguridad según expertos e investigadores de seguridad encontrados y

explotados, podrían acceder remotamente a los sistemas de control de instalaciones.

Casos ocurridos años atrás como fue el sonado virus Stuxnet, virus cuyo objetivo eran las plantas nucleares en Irán. Impactaba sistemas SCADA de la empresa Siemens, aprovechándose de vulnerabilidades de Windows. También otro conocido virus fue Blaster que se cree fue el principal responsable de un apagón en Nueva York en el 2003. Se mencionan algunas predicciones que se manejan tres objetivos clave de ataques como lo son: las redes sociales, dispositivos móviles, y sistemas industriales (SCADA).

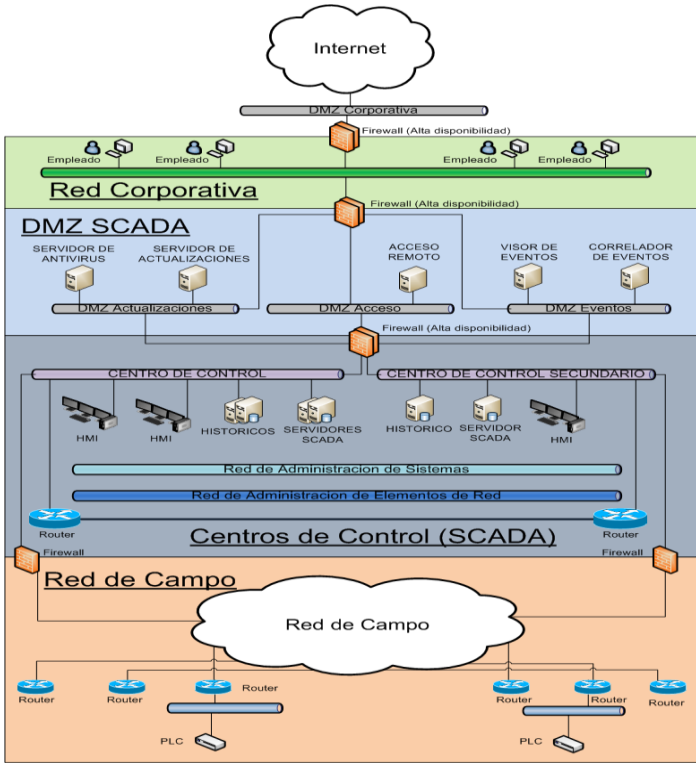
De acuerdo a los datos en el repositorio para Incidentes de Seguridad Industrial (RISI) base de datos de los sectores de la industria del agua y el transporte de aguas y residuos han experimentado tanto un gran aumento en el número de incidentes de seguridad cibernética denunciados en los últimos años, 160% y 60% respectivamente. Estos hallazgos y muchos más fueron publicados hoy en el Informe Anual 2013 sobre Incidentes de Seguridad Cibernética y tendencias que afectan a los sistemas de control industriales [2]. ICS y seguridad SCADA ha sido una preocupación seria por más de una década, pero ha ido creciendo a partir del descubrimiento del virus Stuxnet en 2010, el virus DuQu en 2011 y el virus Shamoon en 2012. Todos estos virus fueron encontrados para dirigirse específicamente a sistemas de control industrial. RISI indica que el 33% de todos los incidentes de seguridad ICS fueron perpetrados a través de acceso remoto. Esta técnica ha sido apoyada por el 48% de los encuestados informaron de que se permite el acceso remoto a los sistemas de control en sus instalaciones.

IV. CONTROLES DE SEGURIDAD

Como consecuencia de las amenazas, riesgos y vulnerabilidades existentes es importante realizar el análisis de riesgos buscando que puede afectar los sistemas SCADA, empezando por la probabilidad de ocurrencia, el impacto que hay en la población, y en el negocio. En cuanto en la seguridad física contar con un control de acceso físico, en las instalaciones en general, en los cuartos de control y en los cuartos de cómputo y comunicaciones. También tener un control de fuego y temperatura, como el uso de sistemas automáticos contra incendio, tener el personal capacitado para emergencias y contar con temperaturas adecuadas.
Respectivamente para la seguridad de la red, la realización de la revisión de la red realizando segregación de la red es decir separada por VLAN o el de uso de IDS, IPS. También la identificación de los host activos y revisión de los servicios disponibles, además un análisis de tráfico en segmentos de control, igualmente servicios intermedios con conexiones a redes de control y administrativas. Del mismo modo, los accesos remotos revisar si son estrictamente necesarios, tener una autenticación, la correcta administración y la disponibilidad de este servicio.

Los controles de acceso lógico es también importante en los servidores, las estaciones de trabajo, los equipos cliente con acceso a redes y sistemas de control deben contar con actualizaciones de seguridad tanto como en sistema operativo, la base de datos y el software instalado. Además, prohibir el uso de USB en estos equipos, mantener un esquema de respaldo robusto y adecuado, mantener activo y configurado el firewall para cada equipo y no permitir conexión directa a internet de estos equipos, y por ultimo crear perfiles de los sistemas de control.

La implementación de una arquitectura de red segura para los sistemas SCADA, permite mitigar estas amenazas, riesgos y vulnerabilidades existentes. En la siguiente imagen muestra un posible diseño de red segura.



Arquitectura de red segura sistemas SCADA. Tomado de http://www.inteco.es/file/5ik7qnpsCJD6GNls9ZYKrA

V. ALGUNAS GUÍAS Y ESTÁNDARES DE LA SEGURIDAD DE LA INFORMACIÓN

A continuación se mostrarán algunas guías y estándares de buenas prácticas de la seguridad de la información en sistemas industriales de control.

A. 21 PASOS PARA FORTALECER LA SEGURIDAD EN SCI

Está guía muestra 21 pasos que nos permite fortalecer la seguridad en los sistemas de control industrial, estos pasos se enfocan mucho en endurecer la red SCADA removiendo servicios innecesarios, implementando sistemas de detección de intrusos [3].

B. ESTÁNDAR DE SEGURIDAD ISA-99

El objetivo de este estándar es mejorar la confidencialidad, la integridad, y la disponibilidad de los sistemas o componentes utilizados para manufactura o control y proveer una serie de criterios para la compra e implementación de sistemas de control seguro [4].

C. NIST SP800-82

NIST creo el proyecto Industrial Control System Security Project y el objetivo fue desarrollar una guía para la implementación de los controles de seguridad que identifica las amenazas y vulnerabilidades más comunes y recomienda algunas prácticas para contrarrestar está información [5].

D. NIST SP800-53

Seguridad y controles de privacidad para los sistemas de información federales y organizaciones proporciona un catálogo de controles de seguridad para todos los sistemas de información y contiene 17 familias de control y 171 controles [6].

E. ESTÁNDAR DE SEGURIDAD NERC-CIP

El objetivo de esta guía es asegurar sistemas de control industrial en el sector de la electricidad. Tomando base las normas NERC CIP-002-4 a la CIP-009-4 las cuales algunas tratan controles de seguridad de la información [7].

F. GUÍAS CNPIC

El centro nacional para la protección de las infraestructuras críticas en colaboración que tiene con el Centro Criptológico Nacional (CCN), presenta una serie de guías de interés para la seguridad de los sistemas de control industrial [8].

VI. CONCLUSIONES

Los sistemas de control industrial (SCI) están experimentadas hoy en día un creciente número de vulnerabilidades.

Es importante reconocer que los sistemas SCADA son uno de los focos principales de los ciber-ataques, por ello debemos aplicar medidas permanentes de seguridad.

Para el desarrollo de la integración de los sistemas SCADA a protocolos como TCP/IP representa un alto riesgo a la seguridad, en caso de no contar con esquemas de red robustos.

Es importante la realización de las actualizaciones de seguridad en el software que soporta los sistemas SCADA ya que es uno de los pilares importantes de la seguridad.

VII. REFERENCIAS

[1] Cristian Borghello. (2014) SEGU-INFO Noticias de Seguridad. [En línea]. Disponible: http://blog.segu-info.com.ar/2014/04/bugs-en-software-scada-permitiria.html

[2] (2013). RISI Repositorio de incidentes de seguridad. [En línea]. Disponible: http://www.securityincidents.net/index.php/news/2013_report_on_control_system_cyber_security_incidents_released/

[3] (2014) 21 Steps to Improve Cyber Security of SCADA Networks. [En línea]. Disponible: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[4] (2014) ISA 99 Industrial Automation and Control System Security. [En línea]. Disponible: https://www.isa.org/isa99/

[5] (2013) NIST Special Publication 800-82. [En línea]. Disponible: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

[6] (2013) NIST Special Publication 800-53. [En línea]. Disponible: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[7] (2011) Standard CIP -002.4. [En línea]. Disponible: http://www.nerc.com/files/CIP-002-4.pdf

[8] (2010) Centro Nacional para la protección de las infraestructuras Críticas. [En línea]. Disponible: http://www.cnpic-es.es/Ciberseguridad/4_Guias_Scada/index.html

Autor

German Darío Baquero Salamanca
Ing. de Sistemas y Telecomunicaciones
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia