Implementación de Políticas de Seguridad en los Sistemas SCADA

Fajardo Rosas, Franklin
franklin.fajardo@live.com
Universidad Piloto de Colombia

Resumen—Este artículo pretende dar un enfoque general de la importancia de la implementación de las políticas adecuadas de seguridad en los sistemas SCADA, teniendo en cuenta las vulnerabilidades que estos sistemas puedan presentar así como también el impacto producido si el sistema es vulnerado.

Abstract—This article search to make a general focus about the importance to provisioning policies according with the security in SCADA systems, it is necessary keep in mind the systems vulnerabilities and also the impact inside the violated system.

Índice de Términos *— SCADA — AMENAZA — CODIGO MALICIOSO — TI — PLC — SCD*

Index Term *— SCADA — THREAT — MALWARE — IT — PLC — SCD*

I. INTRODUCCIÓN

En la actualidad la mayoría por no decir la totalidad de las compañías que prestan servicios críticos como lo son sistemas de transporte, servicios públicos, hidroeléctricas, acueductos usan sistemas SCADA para su trabajo diario, y de ahí la importancia de resguardar estos sistemas de las amenazas existentes.

SCADA es el acrónimo para Supervisory Control And Data Acquisition, SCADA es un sistema que es

usado para tomar medidas de sensores y datos de equipos remotos. Luego de esto las medidas son procesadas para determinar si los valores están dentro de rangos permisibles, si no es así el sistema realizara las correcciones correspondientes para que se mantenga el correcto funcionamiento

Teniendo en cuenta que este es un proceso de control es necesario tener a la seguridad en un primer plano, ya que una falla en uno de estos procesos podría generar invaluables pérdidas económicas, daños ambientales severos, hasta la muerte de personal que labore en la empresa.

Los sistemas SCADA presentan una estructura basada en un servidor o granja de servidores centralizados, PLC que controlan los distintos dispositivos, pantallas en donde se realiza monitoreo y control, y un servidor de base de datos de los históricos.

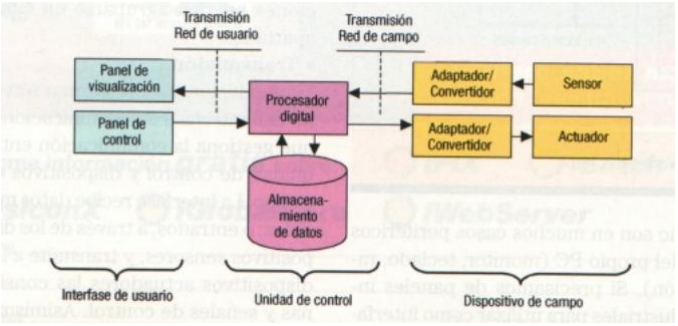

Figura 1: Esquema Básico Sistemas SCADA [5]

II. HISTORIA SCADA

Los sistemas SCADA nacieron en vista de la necesidad de hacer un mejoramiento en el proceso de control y monitoreo de los distintos dispositivos que hacen parte de las empresas, esto haciendo uso de una herramienta de software que sirve de interfaz entre los PLC y la gestión.

En un inicio los sistemas SCADA eran sistemas que funcionaban en forma independiente, elementos aislados creados a la medida de las necesidades tanto a nivel de software como de hardware. La capacidad de procesamiento de estos elementos eran limitados y no podía desarrollar mas tareas de las inicialmente propuestas, adicionalmente los protocolos propietarios de comunicaciones eran desarrollados para permitir el paso la información en tiempos determinísticos, esto significa que se conoce el tiempo que durara un proceso es siempre conocido; esta característica abre una brecha de seguridad en el sistema.

III. VULNERABILIDAD SISTEMA SCADA

Los sistemas SCADA fueron diseñados antes del surgimiento de Internet. Fueron pensados para ser sistemas aislados y no conectados en red. Tradicionalmente carecen de dispositivos de seguridad como cortafuegos, mecanismos de cifrado o software antivirus. [2]

De otra mano y teniendo en cuenta que la tendencia actual en todos los sistemas es que haya una interrelación entre ellos dentro de las mismas compañías, esto en vista de lograr una mayor productividad; adicional también se busca que se presenten acuerdos entre diferentes compañías para que se brinde cooperación mutua entre ellas siendo los sistemas parte fundamental de este tipo de ayuda. No yendo en contravía a esta tendencia los sistemas SCADA en la actualidad son sistemas que trabajan no en forma aislada controlando unas pocas funciones sino que forman un conjunto en donde todas las variables controladas (Dispositivos) hacen un gran sistema, lo mismo sucede al hacer la conjunción de los sistemas SCADA de diferentes empresas.

Adicional a esto, las áreas gerenciales comenzaron a solicitar ampliación en la capacidad del trabajo haciendo que las empresas se incorporaran a plataformas estándar de hardware y software como lo son sistemas operativos como Unix o Windows, uso de protocolos de comunicaciones TCP/IP, y uso de aplicaciones WEB, al realizar esta inclusión también se introdujo las vulnerabilidades propias que poseen cada una de las redes de las compañías.

Teniendo estos aspectos presentes y siendo conscientes que muchos de los dispositivos que hacen parte de SCADA no se han actualizado de la misma forma como si lo ha hecho el resto de la tecnología, podemos identificar que se presenta una brecha en la seguridad ya que se tiene un combinación de hardware y software antiguo hecho a la medida el cual no esta preparado a los ataques actuales a los que se ven sometidos los sistemas operativos Linux y Windows, esto puede llegar a considerarse una vulnerabilidad del sistema.

En esta misma línea, como se ha mencionado anteriormente el software y el hardware se realizaban a la medida de las expectativas y

requerimientos propios de la función que se quería hacer, cada empresa se encargaba era propietaria del hardware y del software que el sistema SCADA usaba. En la actualidad estos dos componentes son estándares utilizados por la mayoría de las empresas, esto representa más vulnerabilidades a las compañías.

Siendo el hardware y software sistemas desarrollados no pensando en la necesidad especial de cada compañía, estos no se adaptan a los requerimientos de seguridad ni a la complejidad propia de cada uno de los sistemas SCADA. De otro lado al tratarse de unos desarrollados conocidos en la industria también sus vulnerabilidades son conocidas lo que hace que se amplié el número de posibles atacantes a los sistemas SCADA.

De otro lado el personal de IT no posee el conocimiento o la sensibilización necesaria de que necesita proteger en una red SCADA, es decir en los sistemas SCADA existen vulnerabilidades que normalmente no pueden considerarse de alto impacto en las redes corporativas pero en el marco de este tipo de sistema si lo son produciendo grandes pérdidas, o también puede presentarse el caso que las medidas de control usadas normalmente por TI no han sido adaptadas a los sistemas SCADA, por lo que la implementación de las medidas no pueden ser lo suficientemente buenas para mantener el entorno protegido.

IV. PROTECCION SISTEMA SCADA

En general cualquier medida técnica usada en IT puede ser implementada en SCADA siempre y cuando esta técnica cumpla con los requerimientos de SCADA en donde se garantice que exista coherencia en lo que se va a implementar.

Siendo SCADA un punto neurálgico para la producción de las empresas, es necesario protegerlo de los ataques tanto externos como internos que se puedan producir contra él, en este proceso es necesario involucrar a toda la organización para realizar una evaluación total de los aspectos de mas alto impacto para el desarrollo normal de las tareas de la compañía. Aunque la promoción de la gestión de seguridad y la importancia de los sistemas SCADA deben venir provenientes de los cargos mas importantes dentro de la organización.

Para efectuar una correcta protección de este tipo de sistemas es necesario desarrollar un análisis de riesgo del sistema SCADA de la compañía, es decir conocer los activos, las amenazas, las vulnerabilidades, el impacto sobre la organización y los controles establecidos o por establecer.

Entre las amenazas tenemos denegación de servicio, incidentes accidentales, accesos controles no autorizados y código malicioso o no autorizado instalado, estas amenazas vienen de hackers, atacantes internos, personal descontento, ingeniería social, contratistas

En este mismo sentido se deben determinar los activos de la organización tomando en cuenta los siguientes elementos: Infraestructura, sistemas operativos, software usado, acceso remoto, procesos y procedimientos realizados, gestión de terceros entre otros.

Para evitar o mitigar estos riesgos, se debe crear un plan integral de seguridad dentro de la organización para lograr el objetivo de llegar a tener un nivel de impacto asumible por la organización, para lograr esto se deben de seguir los siguientes pasos de acuerdo a la norma 27001-2005.

- Creación de una política de seguridad: Dentro de la organización se debe establecer las necesidades de seguridad

correspondientes al sistema SCADA implementado dentro de ella, esto se debe documentar así como también compartir con las partes interesadas dentro de la organización. Esta documentación debe ser contantemente revisada para garantizar la eficacia y efectividad de la misma.

- Organización de la seguridad de la información: Dentro de la organización se debe establecer y comunicar los roles de seguridad, las responsabilidades y los niveles de acceso para la gestión de IT, de los colaboradores y los accionistas de la compañía.

- Gestion de activos: Se debe mantener la protección adecuada sobre los activos pertenecientes a SCADA, es decir se debe documentar todas las conexiones, en donde se hace el almacenamiento de los datos, cuales son las aplicaciones, componentes e infraestructura de red críticos para sistema SCADA, así como también quienes son los designados para salvaguardar estos activos dentro de la organización.

- Seguridad de los recursos humanos: Dentro de la organización todos los colaboradores deben ser sensibles y responsables de acuerdo a la información por ellos manejada en su rol respectivo, esto cobra vital importancia al hablar de sistemas SCADA ya que estos sistemas son de criticidad alta para el continuo funcionamiento de la empresa.

  Dentro de esta sensibilización es importante que exista una interrelación alta entre el personal responsable de SCADA y el personal de IT, para que los objetivos de cada uno se cumplan en su mayoría, logrando seguridad y operacionalidad en los sistemas.

- Seguridad física y ambiental: Se deben implementar sistemas de control de acceso a los lugares en donde se hace la monitorización del sistema SCADA, así como también al lugar donde están presentes los servidores del sistema y de la base de datos.

- Gestión de las comunicaciones y operaciones: En este punto se debe garantizar el correcto funcionamiento de la red, garantizando que no exista malware dentro de ella para alcanzar esto se necesita la implementación de varias políticas. Se debe desconecta cualquier red innecesaria o desautorizada de su sistema SCADA, incluyendo puertos USB, conexiones inalámbricas o links a extranets terceras inseguras. En concordancia y adicional a esta política se deba aislar el sistema SCADA del resto de la red, una forma de lograr esto es hacer la implementación de firewalls para establecer zona desmilitarizadas.

  “Implemente soluciones de seguridad de defensa en profundidad como firewalls de próxima generación o UTMs, que protegen contra brechas un único punto de fallo (single-point-of-failure). Las soluciones efectivas se caracterizan por unas defensas multi-prong, incluyendo prevención de intrusiones, antimalware, filtrado de contenidos y firewall de aplicación inteligente. Garantice que sus servicios de seguridad están continuamente actualizados con las últimas firmas y parches”. [4]

En lo posible no dejar configuraciones por defecto o configuraciones mínimas de los equipos del sistema SCADA, ya que esto puede ampliar las vulnerabilidades a ataques de intrusión o accesos no autorizados al sistema. En lo posible haga un diseño en conjunto con el proveedor del dispositivo para obtener una mejor relación entre seguridad y desempeño del elemento que hace parte del sistema SCADA.

Por último es indispensable realizar un proceso de monitoreo de actividades anómalas que existan dentro de la red. En vista de esto se debe hacer creación de archivos de logs de todos los equipos que hacen parte de la red, estos equipos deben estar sincronizados para poder hacer una correcta intercorrelación de los eventos que se produzcan dentro de la red.

- Control de acceso: Los administradores del sistema deben diseñar e implementar normas fuertes de control de acceso a los dispositivos y a la información presente en los sistemas SCADA. Adicional establecer usuarios que tengan acceso al sistema haciendo diferenciación de los privilegios que debe tener cada uno de estos, limitando estos privilegios al mínimo con lo que pueden desarrollar sus funciones.

  En esta misma vía se deben realizar auditorías constantes de los logs de accesos de los usuarios buscando actividad sospechosa. Se deben hacer un barrido de los usuarios en busca de cuentas inactivas o cuentas que han cambiado de rol para realizar la eliminación o los cambios de permisos necesarios según sea el caso.

  En el caso de acceso remoto, se debe definir, implementar y monitorizar todas las conexiones de acceso remoto externas tanto de entrada como de salida que necesiten los usuarios, para este ítem es necesario: "Asegure todos los accesos remotos sobre las redes privadas virtuales utilizando tecnologías punto a punto IPSec o SSL sin necesidad de cliente"[4].

- Adquisición, desarrollo, y mantenimiento de los sistemas de información, toda nueva modificación que se haga sobre el sistema respondiendo a necesidades comerciales deben conservar el componente de seguridad del sistema
  Adicional a lo anterior es necesario hacer una correcta política de control de cambios de configuración sobre la red, y sobre los equipos que hacen parte de la misma, proveyendo y realizando la documentación necesaria de cada uno de los cambios que se hacen, y guardando los backups recientes para evitar grandes traumatismos en caso de algún reinicio accidental.

- Gestión de incidentes en la seguridad de la información, es necesario generar una política en donde basado en las alertas que se presenten y en el monitoreo de todo el sistema SCADA, se puedan obtener conclusiones acerca de las debilidades que este puede presentar, y así poder tomar las decisiones adecuadas en forma oportuna para prevenir ataques y evitar indisponibilidades del servicio.

  Con el desarrollo de varios sistemas comerciales de monitoreo estándar del tráfico de red se puede tener una respuesta más rápida a los incidentes que se puedan presentar dentro de la red, estos sistemas funcionas tanto en las redes de datos como

en los aplicaciones SCADA.

- Gestión de continuidad comercial, los sistemas SCADA son frecuentemente usados en organizaciones dedicadas a operaciones de carácter crítico, por lo que se debe tener un plan de recuperación que funcione de una forma rápida y eficiente para no generar grandes traumatismos en los sistemas SCADA. Para lograr esto se necesita tener esquemas de backup que funcionen en forma automática, tener backups actualizados de las configuraciones de los equipos y que estas se puedan acceder desde equipos alternos para poder realizar la recuperación.
- Cumplimiento, con el objetivo de maximizar la efectividad y minimizar la interferencia del proceso de auditoría sobre el sistema SCADA, se debe realizar una verificación completa del sistema en forma rutinaria, hacer revisión de los incidentes presentados para hacer una retroalimentación dentro del sistema en forma continua, y por último es necesario tener una documentación actualizada de la red SCADA y sus componentes. Estos puntos cumplidos se requieren para hacer correcciones y tomar medidas pertinentes para adelantarse a los incidentes antes de que estos se materialicen.

V. CONCLUSIONES

Los sistemas SCADA como cualquier otro sistema presentan vulnerabilidades que pueden ser explotadas por distintos actores, pero al ser estos unos sistemas críticos para la operación de muchas organizaciones se deben tener unos mayores controles y mejores planes de recuperación, ya que la falla en estos servicios pueda significar grandes pérdidas desde económicas hasta vidas humanas.

En la creación de políticas para los sistemas SCADA toda la organización debe estar involucrada para compartir diferentes puntos de vista, pero la gerencia debe ser la que dicte los preceptos a seguir en la formulación de las políticas.

En la generación de las políticas se deben tener en cuenta tanto la usabilidad del servicio como la seguridad, haciendo que haya un equilibrio entre estas dos, de nada nos vale tener un sistema SCADA totalmente seguro si el monitoreo no se hace en tiempo real, de nada nos vale tener un sistema rápido pero expuesto a muchos riesgos.

VI. REFERENCIAS

[1] NORMA ISO 27001-2005.
[2] “The SCADA Security Challenge: The Race Is On” Steven Smith – Nov. 2006
[3] CENTRO CRIPTOLOGICO NACIONAL “Guía de Seguridad de las TIC (CCN-STIC-480) Seguridad en Sistema Scada – Marzo 2010.
[4] InfoPLC, “¿Cómo garantizar la seguridad de los sistemas SCADA?”. Available: http://www.infoplc.net/documentacion/209-ciberseguridad-industrial/1107-icomo-garantizar-la-seguridad-de-los-sistemas-scada
[5] Introducción a SCADA. Available: http://www.uco.es/grupos/eatco/automatica/ihm/descargar/scada.pdf

Autor

Franklin Alexis Fajardo Rosas
Ing. Electrónico
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia