11 de marzo de 2018

Informe

Diagnóstico de Ciberseguridad de Planta TRASTER

Pepe García

Contenido

1 INTRODUCCIÓN

El Diagnóstico de Ciberseguridad cuyos resultados se detallan en este documento tiene como objetivo conocer cuál es el estado de la ciberseguridad de las redes y sistemas de la instalación de producción de TRASTER.

En los entornos industriales, el término seguridad es utilizado habitualmente para referirse a la seguridad física de los distintos componentes de la instalación y de las personas que en ella trabajan. Las organizaciones, son conscientes, desde hace muchos años, de la necesidad de garantizar la seguridad física y no han dudado en dedicar los recursos necesarios para ello. Sin embargo, en los últimos años, las instalaciones industriales están sujetas a un tipo de amenazas que las aproximaciones tradicionales de seguridad no son capaces de abarcar. Estas amenazas son las denominadas amenazas cibernéticas: Eventos que, mediante acciones realizadas sobre los sistemas lógicos que controlan las instalaciones industriales, pueden afectar al correcto funcionamiento de dichos sistemas. Mediante prácticas de Ciberseguridad tratamos de conocer y entender cuáles son esas amenazas con el fin de combatirlas de la forma más eficiente posible.

En el mundo actual, la frontera que separa el mundo físico del mundo virtual generado por los sistemas de información es cada vez más tenue y difusa. Muchas instalaciones industriales forman un nexo entre ambos mundos, generando la posibilidad de que las acciones realizadas en el mundo lógico de los sistemas de control tengan un efecto físico sobre el mundo real. Si dichas acciones no son adecuadamente controladas y protegidas, los efectos físicos pueden ser no deseados, abarcando efectos que van desde paradas de producción con el consiguiente perjuicio económico hasta el funcionamiento incorrecto de un proceso industrial que podría causar daños personales o al medioambiente.

Por tanto, el conocer cuál es el estado de la ciberseguridad de una instalación industrial se convierte en algo fundamental para garantizar su correcto funcionamiento a lo largo del tiempo.

Mediante la realización de un Diagnóstico de Ciberseguridad, una organización puede conocer de forma general cuál es el estado de la ciberseguridad de una instalación industrial, y de forma particular, **cuáles son sus puntos más débiles y que podrían provocar problemas de funcionamiento en la instalación**.

2 MÉTODO

Los trabajos realizados han consistido en una recopilación de información acerca de los componentes y arquitectura de las redes y sistemas de la instalación y en diversas pruebas de campo realizadas sobre las redes y sistemas de la planta de producción de planta TRASTER, tanto de forma remota como local.

Los sistemas de control industrial, históricamente, han sido diseñados para proporcionar fiabilidad en sus operaciones, sin embargo, esta fiabilidad se ha logrado a costa de sacrificar aspectos relacionados con la ciberseguridad de los dispositivos y asumiendo que funcionarían en sistemas aislados y controlados. Sin embargo, hoy en día, dichas asunciones no son válidas, ya que **cada vez es más común que las redes de los sistemas de control estén interconectadas con otras redes y sean accesibles de forma remota, lo cual puede poner en peligro su correcto funcionamiento**. De hecho, esto influye en **las labores de auditoría sobre sistemas de control industrial,**

ya que muchas de las tareas realizadas en auditorías clásicas de seguridad de la información podrían tener efectos no deseados sobre el funcionamiento de los sistemas de control. Por tanto, **se requieren métodos de trabajo diferentes a los habituales.**

En este tipo de trabajos se minimiza la interacción con los sistemas de control y se le da mayor relevancia a la revisión de información en la que se estudian versiones y configuraciones de software con el fin de realizar búsquedas *pasivas* de vulnerabilidades. Se realizan entrevistas con personal clave con el fin de identificar maneras de trabajo o características de funcionamiento no documentadas. Finalmente, y con un cuidado extremo, se realizan pruebas activas sobre ciertos sistemas, principalmente los que tendrán mayor exposición desde zonas ajenas a la instalación, con el fin de detectar posibles vulnerabilidades que puedan permitir, a un atacante remoto, lograr el compromiso de los sistemas de la instalación.

3 CONCLUSIONES Y RECOMENDACIONES: RESUMEN EJECUTIVO

En este apartado se describen las conclusiones más relevantes del trabajo realizado, así como las acciones a realizar para solucionar los problemas encontrados.

Fortalezas:

- La seguridad física de la planta de producción es excelente, contando con medidas implantadas tanto técnicas como organizativas.
- El personal encargado de la gestión de la planta es consciente de la necesidad de ciberseguridad.
- Existen numerosos procedimientos operativos muy detallados.

Debilidades:

- Existe una falsa percepción de seguridad:
  - Hay firewalls, pero están mal configurados.
  - Los sistemas requieren credenciales de acceso, pero éstas son débiles.
  - La separación entre las redes ofimática e industrial está formada por máquinas *dual homed*.
- Escasa segmentación en las redes industriales.
- Futura interconexión entre red multiservicio y redes industriales.
- Existencia de plantas paquete: Desde el punto de vista funcional son cajas negras con accesos remotos no controlados.

Acciones Recomendadas:

- Revisar la seguridad de los dispositivos existentes:
  - Establecer contraseñas seguras en los sistemas existentes.
  - Configurar correctamente los dispositivos con acceso externo (routers y firewalls).
- Configurar el firewall de la red ofimática para restringir el acceso entre las redes multiservicio e industriales.
- Estudiar el planteamiento de arquitectura y segmentación de red propuestos en este documento.
  - Incorporar dispositivos de filtrado en el acceso a los controladores

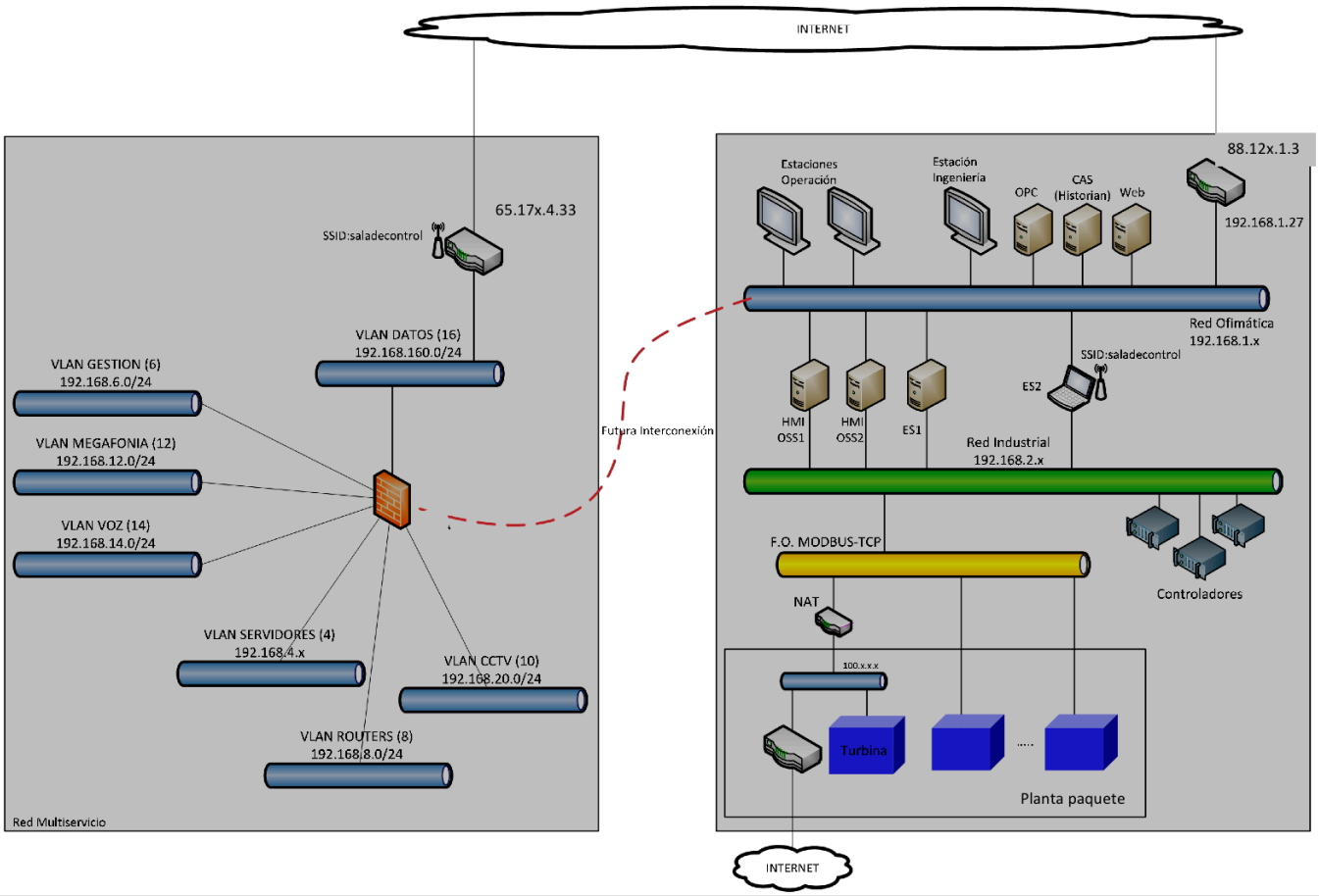
- Revisar la documentación operativa existente para incluir requisitos de ciberseguridad.
- Incorporar aspectos de ciberseguridad en los procedimientos operativos existentes.
- Desarrollar e implantar un procedimiento de incorporación segura de sistemas a la organización.
- Revisar las necesidades reales de accesos remotos por parte de proveedores con el fin de tratar de incorporarlos a los accesos corporativos.
- Realizar periódicamente sesiones de difusión y concienciación sobre la necesidad de mantener la ciberseguridad de las instalaciones.

4 ESTADO ACTUAL

4.1 Arquitectura de redes

La organización dispone de documentación muy detallada acerca de la estructura física de la red, sin embargo, no existe un diagrama lógico completo. El diagrama lógico de redes es fundamental para poder estudiar cuáles son las relaciones entre los distintos componentes y, de esa manera, poder determinar las necesidades de ciberseguridad.

A continuación, se reproduce un diagrama representativo de la estructura lógica de las redes de la organización.



Las redes de comunicaciones de la organización se dividen en dos grandes bloques funcionales:

Red Multiservicio: En esta red se albergan, en distintas VLANs, los dispositivos que no están relacionados con el proceso de producción. Equipamiento de oficina, teléfonos, megafonía, circuito de televisión. Es una red de TI típica construida sobre electrónica de red del fabricante **ZZZ**.

Redes de Producción: En estas redes se ubican los dispositivos relacionados con el proceso de producción. En la red industrial están conectados los equipos controladores y actuadores del proceso, mientras que en la red ofimática se encuentran las estaciones de ingeniería y operación. Esta red está construida sobre dispositivos de red industriales, principalmente del fabricante **YYYYYY**.

Aunque ambas redes están físicamente aisladas, está previsto que se realice una interconexión entre ambas con la intención de proporcionar a ciertos equipos de la red multiservicio acceso a los datos de funcionamiento de la zona de producción.

4.1.1 Red multiservicio

En los distintos segmentos que componen esta red se ubican los dispositivos que no tienen relación con el proceso de producción. La red multiservicio está compuesta por una serie de VLANs destinadas a albergar, cada una de ellas, equipos de las mismas características. Está previsto que la comunicación entre las distintas VLANs esté gestionada por un equipo firewall **XXX**. A fecha de la realización de este diagnóstico (31 de enero de 2016), dicho equipo aún no está instalado. Una de las VLANs (VLAN Datos) proporciona salida a Internet mediante un router del operador **MMMM**.

El router de salida a Internet proporciona una red WiFi (SSID: saladecontrol) asegurada con el protocolo WPA Personal y clave compartida.

4.1.2 Redes de producción

En las redes de producción se conectan todos los equipos relacionados con el proceso industrial. Existen dos redes de producción:

- Red Industrial: Alberga los controladores del proceso industrial.
- Red Ofimática: Contiene las estaciones de operación e ingeniería, así como los servidores que éstas requieren para su funcionamiento.

La interconexión entre ambas redes se realiza mediante máquinas puente (Dual-homed) que disponen de interfaces en ambas redes.

Una de estas máquinas puente es la estación de ingeniería (ES2), que además tiene las siguientes características: es un equipo portátil y tiene una interface de red inalámbrico. Es importante resaltar esto, ya que debido a dichas características es un equipo especialmente sensible desde el punto de vista de la seguridad. Este equipo se utiliza ocasionalmente para permitir accesos remotos a la red industrial. Para ello, se activa el interface inalámbrica, con lo que el equipo tiene acceso a Internet, y mediante un software de control remoto (**JJJJ**) permite que un operador acceda desde cualquier ubicación de Internet a los equipos en la red de producción. Con el fin de minimizar los riesgos, este procedimiento se realiza manualmente y bajo demanda, pero debe ser vigilado estrechamente debido a los potenciales efectos que tendría un mal funcionamiento o el compromiso de esta estación de trabajo.

La red ofimática está conectada a Internet mediante un router del operador **MMMM**. Este acceso a Internet es utilizado para el **acceso remoto a datos de funcionamiento por parte de miembros de la UTE**.

En la red industrial se ubican los equipos más importantes de toda la instalación en cuanto a que son los encargados de ejecutar y controlar el proceso de producción, por tanto, es fundamental el garantizar la seguridad en este segmento de red. La red industrial presenta la peculiaridad de que a ella se conectan dispositivos que no están gestionados por el personal de la propia planta. Esto son las denominadas ***plantas paquete***: componentes encargados de realizar una función determinada dentro del proceso productivo, pero que suponen una auténtica caja negra en cuanto a su arquitectura y funcionamiento, ya que han sido instaladas y mantenidas por proveedores externos.

Una de estas *plantas paquete* corresponde a una turbina de **RRRRR** instalada y mantenida por el proveedor **YYYYY**. Este proveedor, ha impuesto una serie de condiciones de configuración y arquitectura que deben ser cumplidas para que aquel realice el mantenimiento de la turbina. Estas condiciones pueden crear impacto sobre la ciberseguridad de toda la instalación, por lo que deben ser examinadas cuidadosamente. Las dos imposiciones más relevantes que ha hecho **YYYYY** son:

1. Utilizar un direccionamiento impuesto por el propio fabricante en los sistemas que componen la arquitectura de la turbina. Para permitir la comunicación entre los sistemas de la planta TRASTER, este direccionamiento debe ser integrado en las redes de la instalación. Para ello se ha introducido entre la red industrial de la planta y la red de la turbina un router que realiza una traducción de direcciones (NAT) que enmascara los detalles de implementación de la red de la turbina presentando todo el tráfico procedente de dicha red con una dirección IP de la propia red industrial.

2. Exigir una línea de acceso a Internet para que el fabricante realice accesos remotos al equipamiento de la turbina. Como se ha mencionado anteriormente, cada acceso a Internet que exista en la red supone un punto de entrada potencial para atacantes remotos. En este caso, la configuración y gestión de dicho acceso queda totalmente en manos del fabricante, suponiendo un punto débil desde el punto de vista de la seguridad. Durante los trabajos de campo, se ha verificado que no existen servicios accesibles a través del direccionamiento correspondiente a la línea de acceso para **YYYYY**

4.2 Sistemas

Los sistemas más relevantes desde el punto de vista de la ciberseguridad son los contenidos en las redes de operación. Aquí podemos diferenciar entre dos tipos fundamentales de equipamiento:

1- Equipamiento industrial: Dispositivos encargados de realizar el control de proceso industrial y de componer la red de comunicaciones industrial.

2- Equipamiento de propósito general: principalmente representado por las estaciones de operación e ingeniería y los servidores requeridos para el funcionamiento de las distintas aplicaciones de control.

Los equipos industriales deben ser el objetivo final de todas las medidas de seguridad que se implanten, ya que de ellos depende el correcto funcionamiento de los procesos de producción, sin embargo, desde el punto de vista de la ciberseguridad, los equipos de propósito general son mucho más delicados, ya que mientras que el equipamiento industrial es relativamente estático y homogéneo en cuanto a sus configuraciones y funcionamiento, los equipos de

propósito general, dotados de sistemas operativos de propósito general, son mucho más susceptibles a sufrir cambios que puedan influir en el estado de su seguridad.

Conscientes de esta problemática, los responsables de la instalación han implantado mecanismos para evitar la infección mediante discos USB. Para ello han restringido el acceso físico a los puertos USB mediante el emplazamiento de las cajas de los equipos dentro de armarios cerrados con llave. Además, se han instalado carteles informativos recordando que no está permitido utilizar dispositivos de almacenamiento USB en los sistemas de las redes industriales. Esto supone una buena medida de control para evitar las infecciones malware a través de puertos USB, sin embargo plantea ciertos problemas operativos como la dificultad que supone el extraer información de los sistemas de esta red.

4.2.1 Routers y Firewalls

En la instalación, hay un firewall **XXX** planificado para la red multiservicio. El objetivo principal de este firewall es controlar el tráfico originado en las VLANs internas y dirigido a Internet.

La instalación también cuenta con un firewall del fabricante industrial **RRRRR** para proteger el acceso remoto para los miembros de la UTE.

En la planta existen tres líneas de datos del operador **MMMM**.

4.2.2 Navegación red multiservcio

Rango	65.17x.4.33 - 65.17x.4.34
65.17x.4.33	Gateway del operador
65.17x.4.34	IP pública del router en VLAN de datos

La dirección pública del router (65.17x.4.34) está a la escucha en el puerto 5351/udp, habitualmente asociado con el servicio NAT-PMP. Este servicio permite automatizar el reenvío de puertos de manera que las aplicaciones que lo necesiten puedan realizar configuraciones del router. Este protocolo no debería estar publicado en Internet, y en caso de estarlo, sus posibles consecuencias deberían estar controladas por un firewall instalado tras el router.

El router en la VLAN de datos tiene la IP 192.168.160.1. Este router proporciona conectividad hacia Internet y una red inalámbrica desde la que los usuarios podrían acceder a Internet.

Se ha comprobado que la interface de administración del router es accesible, desde la VLAN de datos o la red inalámbrica con nombre de usuario admin y contraseña admin. Esto supone un problema de seguridad que debería ser resuelto mediante el establecimiento de credenciales de usuario seguras

4.2.3 Acceso remoto UTE

Rango	89.12x.1.3 - 89.12x.1.7
89. 12x.1.6	Firewall. Control de acceso remoto

Esta línea de datos da acceso directo a la red ofimática de la parte industrial, por lo que su seguridad ha de ser garantizada en todo momento. Se han realizado sobre un análisis de seguridad detallado desde Internet con el fin de determinar si la línea o los dispositivos en ella configurados suponen una amenaza para la seguridad de la organización.

Se ha comprobado que el acceso con un navegador web al puerto 80/tcp de la IP 89. 12x.1.6 y las siguientes credenciales:

- Login: admin
- Pass: administrador

El puerto 443/tcp de la misma dirección IP también está a la escucha. En este puerto se encuentra un servidor web que pide credenciales de acceso.

Proporcionando las siguientes credenciales:

- Login: TRASER
- Pass: TRASER

Se logra una validación correcta ante el servidor. Esto es muy preocupante, ya que las credenciales son realmente débiles al incumplir dos de las características más importantes de las contraseñas seguras:

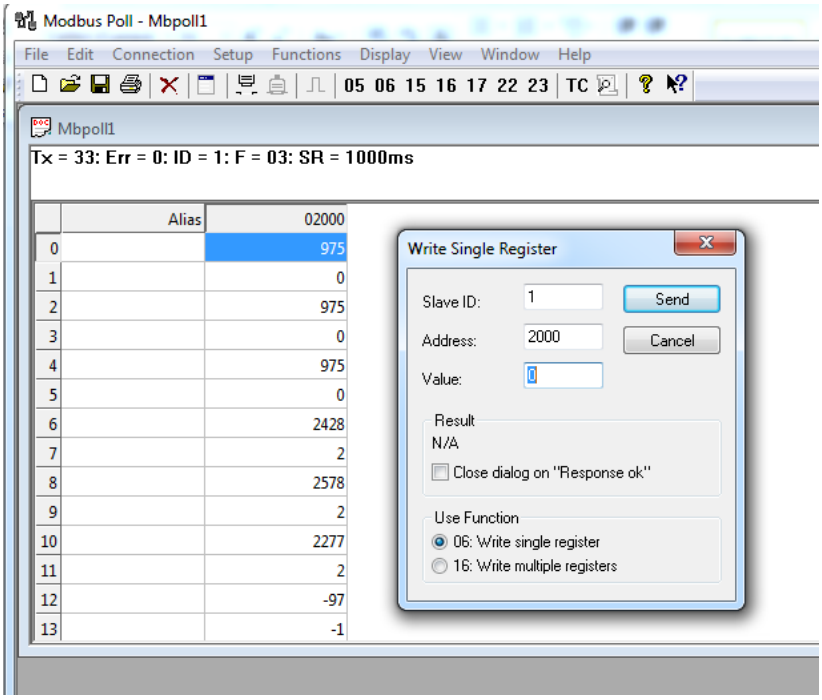
1- El login es igual a la contraseña

2- La longitud de la contraseña es muy corta, lo cual facilitaría el éxito de ataques de fuerza bruta.

4.2.3.1 Acceso remoto a Modbus

Se ha detectado otro puerto a la escucha en la dirección 89. 12x.1.6. En esta ocasión se trata del 502/tcp, asociado al protocolo Modbus sobre TCP. Durante la recopilación de información con el personal relevante de la instalación, se determinó que sólo desde ciertas direcciones IP pertenecientes a la UTE se podía acceder a la información proporcionada a través de esta línea, sin embargo, se ha comprobado que los servicios de la misma están accesibles desde cualquier dirección de Internet.

Durante las pruebas técnicas realizadas, se ha comprobado como con un software de emulación de Modbus, es posible realizar una conexión contra la IP 89. 12x.1.6 y leer y modificar los valores de los registros del dispositivo Modbus.



Esto es un grave problema, ya que Modbus no incorpora ningún mecanismo de seguridad (validación de credenciales, cifrado, filtros de conexión, etc…), por lo que en ningún caso debería permitirse que dispositivos Modbus estén a la escucha en direcciones públicas de Internet.

4.2.4 Acceso de mantenimiento a la turbina

Rango	89.14.28.104 - 89.14.28.107

Se han realizado escaneos de puertos, tanto TCP como UDP sobre este rango de direcciones sin encontrar ningún servicio a la escucha. Esto es bueno, ya que cualquier servicio a la escucha en este direccionamiento podría suponer un problema de seguridad potencial para la planta de la turbina.

4.2.5 Versiones de software y vulnerabilidades

Una de las problemáticas más habituales relacionadas con la ciberseguridad, dentro de las instalaciones industriales, se refiere al mantenimiento de las versiones de software utilizadas. Es inevitable que en el software utilizado aparezcan vulnerabilidades que pueden comprometer la integridad y el correcto funcionamiento de los sistemas. En los entornos típicos de Tecnologías de la Información, esto se resuelve mediante la aplicación de parches de seguridad y la actualización de los distintos componentes software. Sin embargo, en los entornos industriales, este proceso de actualización no siempre es de sencilla aplicación, ya que es frecuente que los componentes físicos de la

instalación industrial requieran un conjunto de versiones software determinado para su correcto funcionamiento. En otras ocasiones, es habitual que el fabricante o mantenedor de un determinado componente exija que un versionado de software determinado para mantener en vigencia la garantía del sistema y la realización de las fundamentales tareas de mantenimiento.

Debido a esto, es importante conocer cuáles son las versiones del software utilizadas en los distintos componentes de la instalación. A partir de este dato, es posible conocer cuáles son las vulnerabilidades que afectan a estos componentes, y por tanto, entender cuáles son los posibles efectos que podría tener su explotación.

A continuación, se detallan las versiones de software utilizadas en algunos de los componentes principales (desde el punto de vista de la operación y gestión) de la planta, así como las vulnerabilidades conocidas más importantes.

Microsoft

Software	Vulnerabilidad	Criticidad	Descripción
.NET Framework 2	Ejecución de código arbitrario	Alta	http://goo.gl/eceMd
	Ejecución de código arbitrario	Alta	http://goo.gl/qCGIv
	Ejecución de código arbitrario	Alta	http://goo.gl/3b2yw
	Ejecución de código arbitrario	Alta	http://goo.gl/emyTO
	Ejecución de código arbitrario	Alta	http://goo.gl/TSL8K
.NET Framework 3	---	---	----
MSXML 4.0 SP2	---	---	----
MSXML 6 SP2	---	---	----
MSXML 6.0 Parser	Ejecución de código arbitrario con denegación de servicio	Alta	http://goo.gl/y6bPz
Office 2003	Ejecución de código arbitrario con denegación de servicio	Alta	http://goo.gl/5MrQx http://www.cvedetails.com/cve/CVE-2008-1898/ (EXPLOITS)
	Ejecución de código arbitrario	Alta	http://goo.gl/qHF83
	Ejecución de código arbitrario	Alta	http://goo.gl/kCpwZ
	Denegación de servicio	Media	http://goo.gl/14VHX
Office Basic 2007	---	---	---
SQL Server 2005	Error de Buffer	Alta	http://goo.gl/xsgMU

			http://www.cvedetails.com/cve/CVE-2008-5416/ (EXPLOITS)
Windows Server 2003 SP1 Admon tools pack	Error de Buffer	**Alta**	http://goo.gl/uB7ET
	Error de Buffer	**Alta**	http://goo.gl/ZBYiF
	Error de Buffer	**Alta**	http://goo.gl/sd8Xa
XP Professional version 2002 SP3	Ejecución de código arbitrario	**Alta**	http://goo.gl/6cm14

Honeywell

Software	Vulnerabilidad	Criticidad	Descripción
MatrikonOPC Server for simulation	---	---	---

ModbusTools

Software	Vulnerabilidad	Criticidad	Descripción
Modbus Poll 5.5.0	---	---	---

OPC Foundation

Software	Vulnerabilidad	Criticidad	Descripción
OPC .NET API 1.0	Buffer Overflow (Ejecución de código arbitrario)	**Alta**	http://goo.gl/4qSQr
	Denegación de servicio	**Media**	http://goo.gl/PvfvM
OPC .NET API 2.00 Redistributable	Buffer Overflow (Ejecución de código arbitrario)	**Alta**	http://goo.gl/4qSQr
OPC Core components redistributable	Buffer Overflow (Ejecución de código arbitrario)	**Alta**	http://goo.gl/4qSQr
OPC NET API 2	Buffer Overflow (Ejecución de código arbitrario)	**Alta**	http://goo.gl/4qSQr

Oracle

Software	Vulnerabilidad	Criticidad	Descripción
VirtualBox 4.1.16	---	---	---

Realvnc

Software	Vulnerabilidad	Criticidad	Descripción
VNC Free Edition 4.1.3			

RRRRR (Fabricante industrial)

Software	Vulnerabilidad	Criticidad
RRRRR automation license manager vX	Consumo de memoria (Denegación de servicio)	Baja
	Sobrescribir archivos	Media
	Denegación de servicio (puntero a NULL)	Media
	Múltiples desbordamientos del buffer	Media
RZZZ BATCH SS client options	Escalada de privilegios	Media
RZZZ SS V9	Acceso a la base de datos	Media
RZZZ SS modbus tcp	Acceso a la base de datos	Media
	Base de datos vulnerable	Alta

La revisión de la lista anterior muestra que existe un gran número de vulnerabilidades asociadas al software utilizado en las redes industriales de la planta. Los efectos de dichas vulnerabilidades son variados, abarcando desde las denegaciones de servicio hasta la ejecución de código arbitrario en los sistemas vulnerables. Cualquiera de estos efectos tiene la capacidad de poner en peligro los procesos de producción de la planta, por lo que debe extremarse la precaución en el manejo y administración de estos sistemas.

5 RECOMENDACIONES

5.1 Arquitectura de redes

La arquitectura de redes actual tiene ciertas características que podrían comprometer la seguridad de los sistemas conectados a ella, a continuación, se detallarán dichas características y se propondrán opciones para tratar de mejorar la seguridad global de la red.

5.1.1 Redes de producción

La **salida a Internet existente en la red Ofimática supone un riesgo de seguridad**, ya que el firewall al que está conectado no está correctamente configurado (como se ha indicado en el apartado 4.2.1). Por otra parte, el tener varios accesos a Internet multiplica las probabilidades de compromiso al aumentar la superficie de exposición de la instalación en Internet. Sería **recomendable centralizar la salida a Internet** en un único punto controlado por un firewall correctamente configurado.

En la arquitectura actual, la comunicación entre la red ofimática y la red industrial se realiza mediante máquinas 'puente' provistas de dos interfaces de red (dual-homed). Si bien esto genera cierta segmentación entre ambas redes, dista mucho de ser una solución ideal, debido a que un problema de seguridad en alguna de esas máquinas se propagará inmediatamente a la red industrial. De hecho, **este tipo de máquinas son blancos habituales**[1] en los ataques a instalaciones industriales. Sería recomendable que **la comunicación entre las estaciones de operación e ingeniería, y los HMI** estuviese **controlada por firewalls**.

Otro de los puntos débiles de seguridad de las redes industriales son los accesos a Internet gestionados por los proveedores de las plantas paquete. Algunos de estos accesos son conocidos (por ejemplo, el acceso a la red de la turbina), pero podrían existir accesos por telefonía móvil más difíciles de detectar. Como primer paso se debería **revisar con cada uno de los proveedores de las plantas paquete la existencia de este tipo de accesos**, con el fin de determinar **si es posible trasladar dichos accesos a la infraestructura corporativa y de esa manera, lograr un mayor control sobre su configuración y utilización**. De manera adicional, y en caso de que haya que mantener accesos no corporativos, será **recomendable el realizar tests de intrusión periódicos** sobre ellos con el fin de garantizar que no suponen un riesgo de seguridad para la organización.

[1] http://www.tofinosecurity.com/blog/dual-homed-machines-are-juiciest-targets

5.1.2 Arquitectura propuesta

La arquitectura propuesta se basa en las especificaciones detalladas en el standard IEC 62443 que establece la creación de zonas de seguridad destinadas a evitar que posibles problemas o incidentes de seguridad en una de las zonas puedan transferirse al resto de la instalación.

Los niveles de seguridad recomendados por la norma IEC 62443 están basados en el modelo de jerarquía funcional ANSI/ISA-95 y describen las funciones y actividades desde el nivel de proceso (nivel 0) hasta el nivel corporativo (nivel 4)

Nivel 4 - Sistemas corporativos

Incluye las funciones y actividades necesarias para la gestión de la organización, incluyendo sistemas financieros, administrativos y de oficina en general.

Nivel 3 - Gestión de operaciones

Incluye las funciones relacionadas con la gestión de los flujos de trabajo necesarios para el proceso productivo: planificación, calidad, optimización, generación de informes, recolección de datos, etc.

Nivel 2 - Control de supervisión

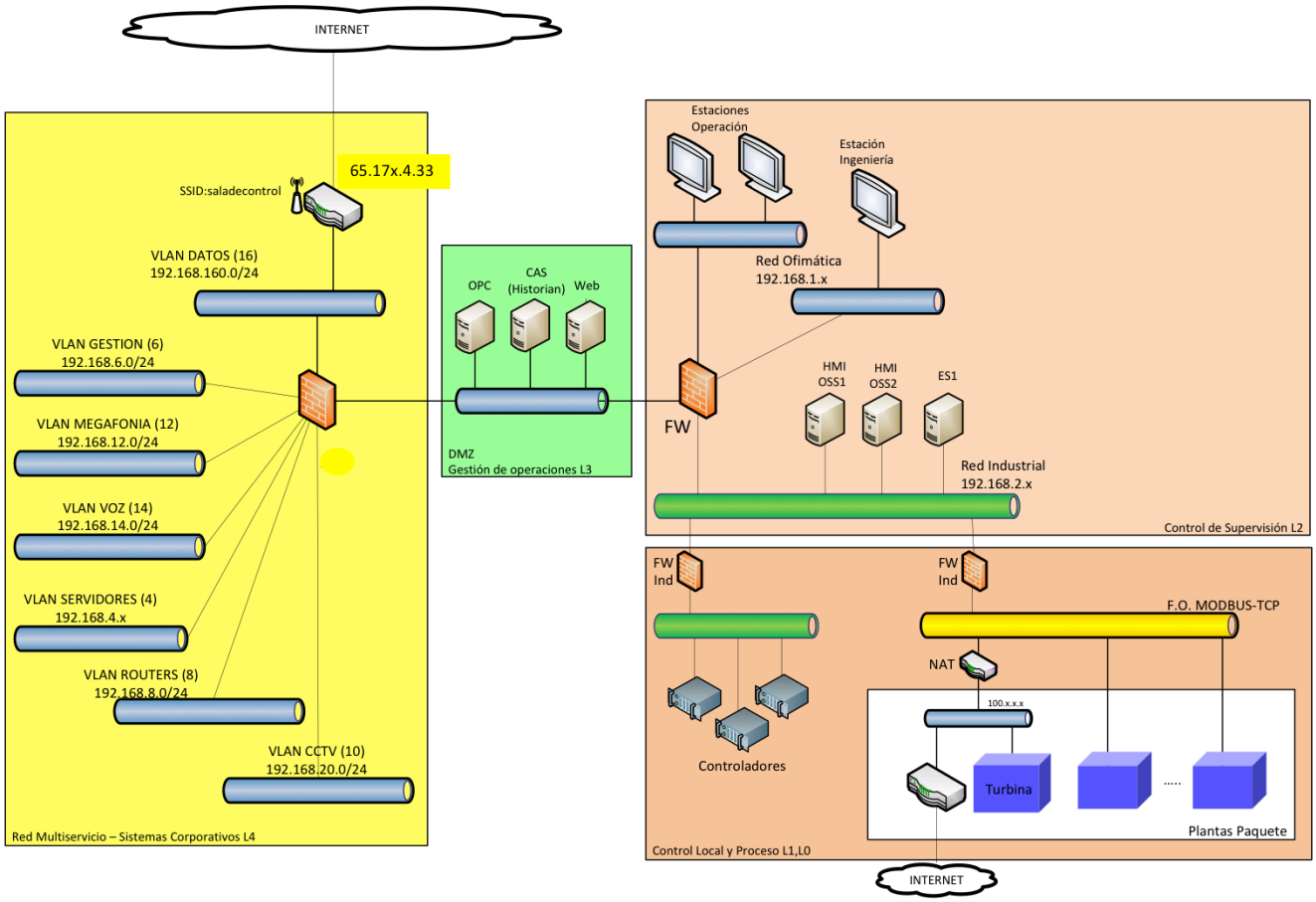
Este nivel incluye funciones relacionadas con la monitorización y el control del proceso físico. En este nivel, típicamente se albergan las estaciones de operación y las funciones de supervisión y control.

Nivel 1 - Control local

Incluye funciones relacionadas con la manipulación y detección del proceso físico. Lectura de sensores, ejecución de algoritmos, envío de datos a elementos terminadores, etc. Los controladores del nivel 1 están conectados directamente a los sensores y actuadores del proceso.

Nivel 0 - Proceso

En este nivel es donde realmente tiene lugar el proceso físico, y donde directamente se incorporan los sensores y actuadores.



En el diseño de red propuesto, se centraliza el acceso a Internet y se delega en el sistema de firewalls de la red multiservicio el acceso hacia y desde redes externas. Las políticas de seguridad configuradas en dicho firewall serán muy estrictas respecto al tráfico que puede tener como origen o destino Internet. Típicamente, no permitirá ningún tipo de tráfico originado en Internet con destino las redes de producción, y sólo permitirá en casos excepcionales y debidamente justificados el acceso a Internet de equipos desde la red de producción.

La interconexión entre ambas redes (Multiservicio y Producción) debería estar estrictamente controlada, para ello se propone la creación de una zona desmilitarizada (DMZ) entre dos sistemas firewall encargados de controlar el acceso entre ambas redes. En la DMZ creada de esta forma, se ubicarían los servidores que requieren acceso desde la zona multiservicio. De esta manera se evita que haya acceso remoto desde la red multiservicio a la red ofimática de las estaciones y servidores de operación e ingeniería y a la red industrial donde se encuentran los sistemas de producción.

Otra de las modificaciones propuestas consiste en evitar que existan máquinas con interfaces en las redes de ofimática e industrial, ya que un incidente de seguridad en dichas máquinas comprometería la seguridad de todas las redes. La propuesta está basada en la segmentación de ambas zonas y el establecimiento de filtrados de tráfico mediante firewalls industriales, de manera que la comunicación entre distintos tipos de dispositivos (estaciones, servidores, controladores) siempre esté controlada por dispositivos de filtrado. Esto permite incrementar en gran medida la seguridad de la solución mediante la creación de distintas zonas de seguridad capaces de contener los

daños en caso de que exista un problema de seguridad en una de ellas. De esta manera en caso de que hubiera un incidente de seguridad en alguno de los equipos de la red ofimática, este quedaría contenido en esta zona sin afectar al funcionamiento de los dispositivos de la red industrial.

Con el fin de lograr un mayor control del tráfico entre los distintos componentes funcionales de la solución, se plantea la introducción de firewalls industriales encargados de gestionar el acceso a los controladores y a las plantas paquete, de esta manera, se asegura que sólo los equipos que realmente lo necesitan puedan acceder a los dispositivos protegidos de esta manera, evitando así, la existencia de tráficos potencialmente dañinos dirigidos hacia los controladores de la red industrial.

Una segmentación como la propuesta en este apartado permite la evolución sencilla de la red y su adaptación a nuevas características o requisitos. Uno de estos requisitos podría ser la necesidad de habilitar accesos remotos. Por ejemplo, con esta arquitectura, resultaría relativamente sencillo configurar accesos VPN IPSec seguros que sólo tengan acceso a los sistemas y servicios estrictamente necesarios para su trabajo.

Evidentemente, un cambio de arquitectura de este tipo puede afectar al funcionamiento de los sistemas, por lo que deberá ser debidamente estudiado y planificado. Con el fin de facilitar esta planificación, a continuación, se enumeran las acciones más relevantes, relacionadas con la segmentación, desde el punto de vista de la seguridad.

Prioridad	Tarea	Descripción
1	Segmentar los niveles 0 y 1	Incorporar dispositivos de filtrado para entornos industriales con el fin de aislar a los elementos de control del resto de sistemas de la organización.
1	Filtrar y restringir el acceso desde la red multiservicio a las redes industriales	Es fundamental que cuando se realice la interconexión entre la red multiservicio y las redes industriales se realice un control estricto de los tráficos permitidos entre ambas partes. El firewall existente (de la red multiservicio) deberá establecer políticas de filtrado para restringir a los mínimos necesarios los accesos desde la red multiservicio a los sistemas de las redes industriales. De manera similar, deberá restringir por completo los accesos en el otro sentido (asumiendo que ninguna conexión originada en las redes industriales debería llegar a la red multiservicio)
2	Segmentar la red industrial (nivel 2)	La segmentación de esta zona permitirá separar en distintas zonas de seguridad a las estaciones de operación, las de ingeniería y a los distintos servidores. De esta manera, se logra compartimentalizar los posibles problemas que puedan ocurrir en alguna de las zonas de seguridad, y permite un filtrado muy granular de los accesos requeridos entre distintas zonas.
3	Creación de una DMZ de intercomunicación	La segmentación realizada en la tarea anterior permite la creación de una DMZ de intercomunicación entre ambos *mundos* de la planta: las zonas multiservicio y la zona industrial. En esta DMZ se podrán albergar los dispositivos a los que sea necesario acceder desde las zonas multiservicio. De esta manera se evita que existan conexiones originadas en la red multiservicio que tengan como destino alguna de las redes industriales.

5.1.3 Red inalámbrica

La red inalámbrica existente en la organización tiene unas características de seguridad mínimas, que hasta ahora se consideran suficientes para su función (proporcionar acceso a Internet a personal de la planta). No obstante, con el fin de garantizar que personas ajenas a la organización utilicen dicha red, sería recomendable configurar un mecanismo de autenticación que no esté basado en claves compartidas (típicamente WPA2-Enterprise). De esta manera, se evitará que usuarios que en un momento determinado hayan tenido acceso a la red inalámbrica, puedan seguir utilizándola tiempo después cuando ya no tengan requisitos de acceso a Internet.

5.2 Sistemas

El principal problema de seguridad de los sistemas de la planta viene dado por la existencia de multitud vulnerabilidades en el software, que podrían comprometer la seguridad de dichos sistemas. La acción recomendada sería realizar actualizaciones del software vulnerable. Sin embargo, es posible que existan condicionantes que impidan la realización de estas actualizaciones, por lo que deberán adoptarse medidas de seguridad complementarias como la segmentación de la arquitectura propuesta en este documento.

Otro de los problemas detectados se refiere a la configuración incorrecta o no segura de distintos dispositivos. En este apartado, se contarían problemas como las contraseñas débiles o por defecto, o los errores de configuración en las políticas de seguridad de los firewalls. Por tanto, sería recomendable realizar una revisión de la seguridad de los dispositivos instalados, prestando especial atención a las contraseñas y credenciales de acceso, así como a configuraciones incorrectas, especialmente, en los dispositivos de filtrado (firewalls)

Durante la realización de los trabajos del diagnóstico de ciberseguridad, se planteó una problemática que dificulta ciertas tareas de la gestión diaria de la planta. Dicha problemática consiste en la dificultad de extraer datos de los sistemas de las redes industriales, para su proceso fuera de la red de la planta. Una de las principales causas de este problema es la restricción en la utilización de los puertos USB de los equipos. Esta medida se adoptó para evitar incidentes relacionados con la introducción de malware en los sistemas de la organización. Sin embargo, sería deseable disponer de una alternativa que permitiera, de forma sencilla la extracción segura de archivos de los sistemas de la red industrial.

Una posible solución sería la utilización de un dispositivo NAS (Network-Attached Storage), que, conectado a la red industrial, permita:

- La realización de copias, automatizadas o manuales, de las carpetas deseadas de cada equipo de la red al dispositivo
- Programar la realización de dichas copias.
- Disponer de uno o varios directorios en red desde donde los usuarios puedan copiar los archivos que deseen en cada momento.

Una vez que los datos hayan sido copiados al dispositivo, éste podría desconectarse de la red con el fin de llevarlo a otra ubicación en la que se realizaría su extracción.

La premisa fundamental para estas operaciones es que se minimicen los riesgos de seguridad que introduciría esta solución, para ello, deberán cumplirse las siguientes condiciones:

- El dispositivo NAS deberá estar basado en un sistema operativo que reduzca la probabilidad de infección malware (i.e. UNIX). Es importante, hacer notar que no existe ningún sistema operativo que sea invulnerable, sino que lo que se trata es de minimizar las probabilidades de un compromiso de seguridad.
- Restricción por IP de origen, de manera que sólo los equipos autorizados puedan conectarse al dispositivo NAS.
- Acceso mediante certificados con el fin de garantizar la autenticidad de las conexiones
- Protocolos seguros mediante cifrado criptográfico (HTTP, SFTP) que puedan proteger los datos en tránsito
- Cifrado de las unidades de almacenamiento, para aportar una mayor seguridad al almacenamiento de los archivos en caso de pérdida, accesos no autorizados y robo.
- Antivirus. Sería deseable que el NAS disponga de un antivirus actualizable y que esta actualización se pudiese realizar de forma manual desde archivo, para evitar que el equipo tenga contacto con otras redes externas con acceso a Internet.
- Aplicación de políticas de uso. Para asegurar la información contenida en el dispositivo, sería recomendable la elaboración de una política de uso, incluyendo aspectos como:
    - Selección de una ubicación, tanto física como lógica, adecuada para el dispositivo. Para obtener una ubicación lógica adecuada, resultará de mucha ayuda la realización de la segmentación de la red propuesta en este documento.
- Designación de privilegios a empleados: Elaborar una lista limitada de usuarios con privilegios para acceder al dispositivo y restringir las operaciones que éstos pueden realizar sobre él.

Registro de entradas y salidas: Si el dispositivo va a abandonar las instalaciones para permitir la extracción de los datos, será conveniente desarrollar un procedimiento para la realización de dichos movimientos y mantener un registro de sus entradas y salidas.

5.2.1 Firewalls

Se propone la incorporación de los siguientes sistemas firewall:

Red multiservicio

Es fundamental la incorporación de un firewall encargado de realizar el filtrado de tráfico entre las distintas VLANs que componen la red multiservicio. Este firewall tendrá la responsabilidad de establecer cuáles son los tráficos

permitidos entre las VLANs de la red multiservicio y cuáles son las redes y dispositivos que podrán tener acceso a Internet. Una de las principales funciones del firewall será garantizar que no se permite tráfico desde la red de datos en la que se encuentra el router de Internet y los clientes inalámbricos, al resto de redes de la organización. Este firewall, además, supondrá la primera línea de contención entre la red multiservicio y las redes industriales, realizando un filtrado estricto del tráfico dirigido a éstas. Dado que este dispositivo controlará todo el tráfico entre las VLANs de la red multiservicio será necesario garantizar su disponibilidad, para ello se recomienda incorporar un segundo firewall en configuración de alta disponibilidad.

Redes industriales

La arquitectura propuesta para las redes industriales en el apartado 5.1.2 se basa en una compartimentalización creada por varios firewalls. Los firewalls propuestos para estas redes son de tipo industrial, que poseen ciertas características que los diferencian de los firewalls tradicionales.

- Su introducción en una red causa una muy baja latencia, del orden de microsegundos, equivalente a la que causa un switch
- Son capaces de entender protocolos de uso industrial. Algunos de estos protocolos (como OPC) no fueron diseñados para ser utilizados en una arquitectura segmentada, por lo que suelen causar problemas a la hora de configurar políticas de filtrado para ellos (Por ejemplo, OPC utiliza puertos dinámicos que no pueden ser conocidos a priori, debido a lo cual la configuración del firewall debe permitir una gran cantidad de flujos de tráfico que podrían comprometer los sistemas que deben ser protegidos. Los firewalls industriales son capaces de entender los requisitos de estos protocolos y adaptarse de forma dinámica a sus necesidades.

La función de estos firewalls será garantizar que sólo los tráficos necesarios para el proceso de producción lleguen a los controladores, minimizando de esta manera la posibilidad de que los sistemas sufran incidentes de seguridad.

Se recomienda implantar firewalls que controlen los accesos desde los equipos de operación e ingeniería hacia los controladores. También es recomendable instalar firewalls que controlen el tráfico procedente de las plantas paquete, de manera que un incidente de seguridad en la red de una de estas plantas no afecte al funcionamiento del resto de sistemas de la instalación.

5.3 Organización

Aunque la organización dispone de multitud de procedimientos operativos, éstos no contemplan aspectos de ciberserguridad.

Sería recomendable realizar una revisión de los procedimientos existentes con el fin de incluir aspectos relacionados con la ciberseguridad, especialmente en los procedimientos que se refieren a dispositivos de control, los relacionados con las operaciones de la planta o los que involucren a terceras partes que realicen trabajos en las instalaciones con

el fin de determinar las necesidades y tipos de los accesos que éstos requerirán y poder, por lo tanto, asegurarlos debidamente.

También sería recomendable desarrollar procedimientos para la gestión y generación de contraseñas, de forma que las contraseñas utilizadas en la planta tengan la complejidad adecuada para hacerlas resistentes a ataques de diccionario o fuerza bruta.

Otro de los procedimientos que sería recomendable desarrollar es el de incorporación de nuevos sistemas a las instalaciones. El objetivo de este procedimiento es garantizar que los nuevos sistemas que se conecten a las redes de la organización no introduzcan problemas de seguridad. Este procedimiento deberá incluir comprobaciones sobre las vulnerabilidades conocidas de los sistemas, necesidades de comunicación con el fin de determinar la zona de red más apropiada, revisiones de la configuración y el establecimiento de contraseñas de acceso seguras.

Habitualmente, en las organizaciones, los principales problemas de seguridad están provocados por malas prácticas efectuadas por el personal interno, por lo que es importante mantener en todo momento un nivel adecuado de concienciación sobre ciberseguridad. Para ello se recomienda realizar sesiones periódicas de concienciación. Estas sesiones pueden tomar la forma de charlas divulgativas, cursos, o carteles informativos en lugares visibles.

Desde el punto de vista del funcionamiento organizativo, uno de los aspectos más relevantes para la ciberseguridad es la existencia de dos únicos perfiles de usuario (operador y administrador) para acceso a los sistemas de la organización. Es recomendable que en el futuro, estos perfiles se conviertan en roles, y que cada usuario de la organización tenga una identidad única asociada a uno de estos roles. Esto facilitará la gestión de las identidades lógicas de los usuarios permitiendo una asignación granular de los permisos necesarios a la vez que se mejoran los registros de auditoría, que permitirán trazar una acción determinada con una identidad específica.

Actualmente, las copias de seguridad se están realizando de forma manual a dispositivos USB portátiles. Esto plantea problemas tanto operativos como de seguridad. La arquitectura propuesta en este documento podrá facilitar la implantación de un sistema automatizado de copias de seguridad.