Prueba de Evaluación Continua

Sergio Roselló Morell

En no más de 4 páginas y utilizando la infraestructura de red de la figura adjunta:

1. Determinar qué zonas y conduits habría que definir desde el punto de vista de la seguridad
2. Discutir cuáles serían los riesgos de seguridad más importantes asociados, bastaría con citar (y argumentar) los tres principales
3. Explicar qué medidas de seguridad serían las más importantes y urgentes a implementar y por qué
4. Hacer un "mini plan" de puesta en marcha de la política de seguridad asociada a todo lo anterior

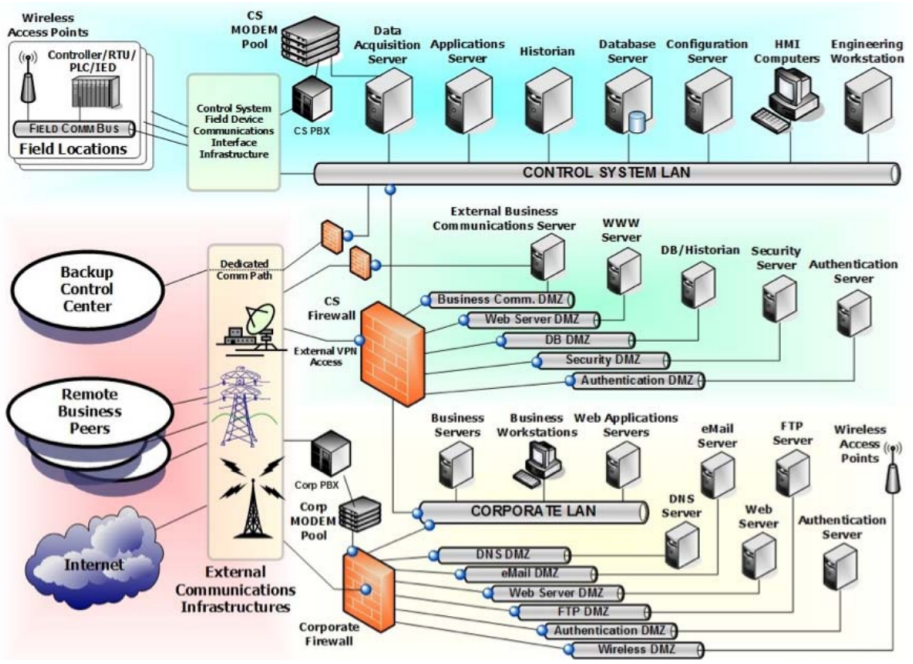

Figure 1: Figura adjunta

1. Zonas y Conduits a definir desde el punto de vista de la seguridad

Existen una serie de mejores practicas para las infraestructuras criticas. Dependiendo de la seguridad y criticidad de los elementos en uso, se deben establecer unas zonas u otras.

La regla general para mantener una buena seguridad, es separar el ICS en al

menos tantos niveles como indique la pirámide ISA-95. En nuestro caso, tenemos elementos del nivel 0, nivel 1 (PLC, IED), nivel 2 (HMI), nivel 3 (historians) y nivel 4 (red corporativa). Por lo tanto, como mínimo, tenemos que dividir nuestra red en 4 niveles. Cuanto mas granular y subdividida sea nuestra red, mas segura sera, si tenemos un buen control de trafico en los conduits.

Las zonas físicas:

- **ID:0.0..n** Agrupación de elementos de control de nivel 0 y 1 en la misma cadena de montaje (Parte superior izquierda azul)
- **ID:1** Agrupación de servidores, historiadores, equipos informáticos y HMI en la zona del sistema de control (Azul)
- **ID:2** Agrupación de servidores y equipos informáticos en el área corporativa (Amarillo)
- **ID:3.0..n** Cada uno de los DMZ con servidores (Amarillo)
- **ID:4.0..n** Zona de acceso remoto/WiFi (Amarillo)
- **ID:5.0..n** Cada uno de los DMZ intermedio entre las zonas corporativa y de control (Verde)
- **ID:6** Centro de copias de seguridad (Superior izquierda (rojo))
- **ID:7.0..n** Cada uno de los centros de empresas asociadas (Medio izquierda (rojo))
- **ID:8** Internet (Inferior izquierda (rojo))

Las zonas lógicas:

En la zona de control: (Azul)

- **ID:9.0..n** Cada una de las zonas físicas de nivel 0-1 con su HMI pertinente
- **ID:10.0..n** Cada una de las zonas físicas de nivel 0-1 con el historiador
- **ID:11** El historiador, servidor de adquisición de datos y base de datos de la zona de control
- **ID:12** La base de datos con el centro de copias de seguridad (subzona de **ID:1**)

En la DMZ intermedia (verde)

- **ID:13.0..n** Cada una de las empresas vinculadas, el servidor de comunicaciones de las empresas vinculadas y el servidor de autenticación y el servidor web (De donde obtendrán los datos del proceso o de sus dispositivos (Obtenido del DB/Historiador))

En la zona corporativa (Amarillo)

- **ID:14.0..n** Servidor de autenticación con servidor DNS y cada uno de los otros servidores o punto de acceso WiFi
- **ID:15.0..n** Red corporativa con servidor DNS con cada uno de los otros servidores o punto de acceso WiFi
- **ID:16** Internet con servidor de autenticación con la red corporativa

- **ID:17** Internet con servidor de autenticación con la red corporativa con cada uno de los servidores restantes en la red corporativa (Amarillo)
- **ID:18.0..n** Cada una de las empresas remotas con el servidor de autenticación y el LAN corporativa

Entre zonas

- **ID:19** Zona corporativa (Amarillo) con servidor de autenticación (Verde), con "Engineering workstation (Azul)

Conduits

Los conduits, siendo estos zonas únicamente compuestas de dispositivos de comunicación de red que unen varias zonas (Físicas o lógicas) vienen bastante definidos en el diagrama presentado.

- Existe un conduit entre la LAN corporativa y el Firewall intermedio (Verde)
- Entre el Firewall intermedio y la LAN de control
- Entre Internet y la LAN corporativa
- Entre el LAN corporativo y el de control
- Entre el LAN de control y el servidor de copias de seguridad

Estos Conduits conectan varias zonas entre ellas.

2. Riesgos de seguridad mas importantes

El desgrama de red de la DMZ proporcionada, es una zona segura de por si. Cumple con la mayoría de estándares en la industria, ya que:

- Usa una DMZ para comunicarse entre la zona de control y la zona de negocios
- No permite la conexión a Internet desde la zona de control
- Usa defensa en profundidad de una forma bastante agresiva, ya que usa IDS, segregación por zonas y Firewalls.

1. Sistema en DMZ comprometido, puede enviar trafico a la red de control

El problema generado por el control de trafico por un firewall entre DMZ y la red de control reside en que en el momento en el que un actor malicioso toma el control de un sistema dentro de la DMZ, puede enviar trafico a nivel de aplicación entre la DMZ y la red de control. En este escenario, dependemos de la configuración del firewall, para mantener nuestra zona critica segura.

Otro caso de uso con similar solución es el caso en el que se introduzca software malicioso a un dispositivo dentro de la red de control. Por ejemplo, al HMI. Pongamos que este dispositivo usa el protocolo HTTP para comunicarse. Este dispositivo tiene ahora la capacidad de enviar al servidor C2 contraseñas

capturadas en la zona de control desde un dispositivo en la DMZ con acceso a Internet, porque el Firewall acepta trafico HTTPS de este dispositivo.

2. Si el trafico llega a la zona de control, puede acceder sin filtro a dispositivos críticos.

Si un actor malicioso consigue acceder a la red de control, nada le impide acceder a los dispositivos críticos

3. Los negocios asociados se conectan al mismo Firewall que nosotros

Esto quiere decir que el sistema, aunque se puede configurar para que se tengan en cuenta distintas reglas para las empresas externas que para nosotros, es mas complejo de administrar. Ademas, si llega trafico malicioso desde las empresas asociadas (Cuya seguridad no podemos administrar) puede llegar a infectar nuestro Firewall y esto seria critico para nuestra empresa, dada la arquitectura presente.

3. Medidas de seguridad a implementar

Haciendo referencia al riesgo de seguridad primero, algunas formas de mitigar el diseño de red son:

- haciendo hardening de la maquina en la DMZ
  - Mantener la maquina constantemente actualizada
  - Revisar los registros del sistema
- aplicar el principio del menor privilegio
  - Asegurando que el Firewall únicamente permite el trafico especifico de las diversas aplicaciones que se usaran para comunicarse con la red control.
  - Cualquier otra forma de comunicación entre el sistema en la DMZ y la red de control queda bloqueado. Incluyendo trafico que venga de la misma aplicación de control del sistema en la DMZ, pero que no este explícitamente permitido por el planteamiento de la red.
- Limitar la comunicación entre la red de control y la DMZ a trafico que haya sido iniciado desde la red de control, permitiendo únicamente la comunicación en dirección a la red de control desde la DMZ, si anteriormente ha sido enviada una petición desde la red de control.
  - De esta forma, nos aseguramos que no se puede iniciar un ataque desde la DMZ, ya que no lo pide la red de control.

Una de las posibles soluciones es añadir un segundo firewall entre las comunicaciones, de forma que entre la red de control y la red corporativa existan dos Firewalls y exista una DMZ entre esos dos Firewalls.

El primer firewall protege tanto las zonas de DMZ como la red de control de trafico malicioso proveniente de la zona corporativa. El segundo firewall previene que trafico malicioso desde los servidores de las DMZ llegue a la zona de control

y previene que el trafico malicioso de la zona de control impacte la zona de servidores compartidos (DMZ)

Otra de las posibles soluciones es no permitir que el mismo protocolo sea la entrada de una zona y salida de otra. Por ejemplo: Si sale HTTP de la zona de control, no dejar que entre HTTP en la zona corporativa. De esta forma, el virus, deberá usar dos exploits en dos protocolos distintos para pasar de la zona de control a la zona corporativa o viceversa.

Esta vez, pensando en el segundo riesgo de seguridad, veo que no hay mas que firewall controlando el acceso de trafico desde las zonas externas a la capa de control a los dispositivos críticos, como Controladores, RTU's, PLC's o IED's. Esto es critico, porque quiere decir que todos los dispositivos críticos están al alcance de un actor malicioso que consiga entrar a la zona critica.

Para remediar este error, hace falta que se controle el trafico que se envía a los dispositivos críticos, mediante el uso de un Firewall. La política de seguridad, como he redactado previamente, debe seguir el principio de menor privilegio. Esto quiere decir que se tienen que bloquear los protocolos y paquetes en los protocolos que no se vayan a usar por cada dispositivo. En este momento, viene bien un inventario con los requisitos de cada dispositivo y las opciones que van a emplear.

Para solucionar el problema anotado en el tercer punto del apartado anterior, veo que es necesario que las empresas asociadas se conecten a un Firewall dedicado para ellas, de esta forma, si consiguen infectar el firewall, no vulneran el punto mas critico de la red interna entera.

Ademas, extendiendo lo mencionado previamente, si el Firewall principal falla, no hay ninguna medida de control. La red entera quedaría desmontada y el área corporativa no podría seguir los procesos del área de control. Para mitigar esto, es necesario que se establezca un segundo Firewall de recuperación. De esta forma, cuando el primer Firewall sea vulnerado o falle, tenemos uno secundario, preferiblemente de una marca distinta, para que no se pueda aplicar el mismo exploit al segundo Firewall.

4. Plan de puesta en marcha

1. Recabar información del ICS

Listar todos los dispositivos, y características (Tipo de SO y su versión, SW que tienen instalado, Revisiones de seguridad y su versión, protocolos que usan los equipos, entre otras características) dentro de nuestro ICS.

2. Análisis de riesgos

Revisar los riesgos a los que esta sometida el ICS. Estos no tienen por que ser ni malintencionados por naturaleza, ni técnicos. Puede ser un riesgo, que el ICS este situado en una zona con altas probabilidades de terremotos, al igual que

puede ser un riesgo que los empleados se descarguen aplicaciones piratas en sus teléfonos móviles y que los conecten al sistema industrial.

3. Identificación de las vulnerabilidades

Por cada dispositivo, revisar si existen vulnerabilidades en bases de datos de vulnerabilidades, como cve.mitre o incibe-cert. Incluyendo los dispositivos de las empresas asociadas, ya que están situados dentro de nuestra red interna.

Mitigar los riesgos mas probables de causar un incidente, no los mas interesantes, ni sencillos.

4. Determinar la probabilidad de que ocurra una vulnerabilidad

Contrastar las vulnerabilidades existentes, con la frecuencia con la que se dan. Otra forma de pensar en ello es

5. Determinar el impacto de dichas vulnerabilidades

6. Determinar el riesgo de dichas vulnerabilidades

7. Alternativas/formas de mitigar o controlar dichas vulnerabilidades

8. Redactar informe de los hallazgos