Ciberseguridad: qué hacer, a quién llamar

Ing. José María Suárez
Phoenix Contact Argentina
www.phoenixcontact.com.ar

Hoy en día en la industria es cada vez más común hablar sobre digitalización, Industria 4.0, Internet industrial de las cosas (IIoT), inteligencia artificial, Big Data, entre otras cosas. Es necesario destacar la importancia de estas nuevas tecnologías aplicadas en la industria para mejorar los procesos productivos y manufactureros. Sin embargo, es fundamental tener en cuenta que la implementación de estas tecnologías sin una plataforma de comunicación robusta y cibersegura podría representar un potencial riesgo de ataques cibernéticos.

La implementación de estas nuevas tecnologías en la industria implica la necesidad de vincular las redes de OT (tecnologías operacionales) con las redes de IT (tecnologías de la información), o tener conexión a Internet directamente en las redes de automatización. Estas implementaciones deben considerar ciertas cuestiones de manera de mantener la red de automatización lo más segura posible.

Cada vez son mayores las amenazas de *ransomware* para los sistemas de control industrial. Recientemente, la Agencia CISA (Agencia de Seguridad de Infraestructura y Ciberseguridad) publicó un *paper* en el cual destacó la realidad de las amenazas de *ransomware* en 2021 en relación con los activos de tecnología operativa y los sistemas de control industrial [1].

A continuación, se describen algunas de las cuestiones más importantes a la hora de asegurar las redes de automatización.

Ciberseguridad: por dónde comenzar a implementarla

La prevención comienza desde la segmentación de redes IT y OT. Esto servirá como una barrera para detener intentos de ataques que se realicen a través de la red. La segmentación de red proporciona servicios de seguridad específicos para cada segmento de red, lo que brinda más control sobre el tráfico de red, optimiza el rendimiento de la red y mejora la seguridad.

Para realizar una segmentación segura, es recomendable la implementación de *firewalls*, mediante los cuales se podrá definir claramente cuáles son los flujos de comunicación entre ambas redes, permitiendo filtrar el tráfico no deseado o desconocido.

Es importante conocer qué equipos hay en la red de automatización y saber si presentan vulnerabilidades. Una vulnerabilidad es una debilidad en los procedimientos de seguridad de un equipo o sistema. Dentro de las vulnerabilidades están las llamadas "vulnerabilidades de día cero", que son aquellas que fueron descubiertas recientemente y aún no tienen un parche que las solucione.

Cada vez son mayores las amenazas de ransomware para los sistemas de control industrial.

Cómo atender las vulnerabilidades

Los atacantes tratarán de explotar las vulnerabilidades con el objetivo de causar un impacto que afecte la confidencialidad, integridad o disponibilidad de un sistema. Existe una gran cantidad de vulnerabilidades conocidas en los equipamientos industriales (PLC, SCADA, VFD, switches, routers, entre otros).

Es posible encontrar la información en el sitio web de CISA [2] o en la página web de los fa-

bricantes de dispositivos, por ejemplo, Phoenix Contact cuenta con un equipo autorizado a responder a posibles vulnerabilidades de seguridad, incidentes y otros problemas de seguridad de sus propios productos (equipo de respuesta a incidentes de seguridad de los productos) [3].

En estas páginas se puede buscar, por marca de fabricante o modelo de equipo, los reportes de vulnerabilidades junto con una evaluación de riesgo y detalles técnicos. El informe cuenta también con la mitigación para dicha vulnerabilidad que recomienda el fabricante. Esta mitigación puede ir desde una actualización de *firmware* donde se corrige dicha vulnerabilidad, hasta la implementación de hardware o software adicional de manera que se puedan prevenir ataques que exploten esas vulnerabilidades.

En muchos casos, desde que se conoce una vulnerabilidad de día cero hasta que los fabricantes de los dispositivos implementan la mitigación en el *firmware*, la red puede estar expuesta. En muchos otros casos también ocurre en la industria que por motivos de operación no es tan sencillo programar una actualización de *firmware* ya que eso puede implicar la parada de un proceso o la indisponibilidad durante un tiempo de los equipos involucrados.

El primer paso que realizan los equipos de ciberseguridad de los fabricantes de dispositivos es

generar informes de seguridad que expliquen los métodos que se pueden aplicar para proteger los dispositivos ante un posible intento de explotación de esa vulnerabilidad. En la gran mayoría de estos casos, la solución que suele ser más efectiva para mitigar vulnerabilidades no resueltas por *firmware* es la utilización de *firewalls*.

La prevención comienza desde la segmentación de redes IT y OT. Esto servirá como una barrera para detener intentos de ataques que se realicen a través de la red.

Acerca del firewall

Un *firewall* es un dispositivo de seguridad de red que supervisa el tráfico de entrada y salida de una red, de manera que puede decidir si permite o bloquea un tráfico específico basándose en un conjunto definido de reglas de seguridad.

Los *firewalls* han sido la primera línea de defensa en la seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas seguras y controladas en las que se puede confiar y las redes externas no confiables.

Un *firewall* puede ser un dispositivo de hardware, de software o de ambos.

Un factor importante a tener en cuenta sobre la utilización de *firewalls*, es que deben estar correctamente configurados para las tareas que deben realizar. Se presentan dos principios de configuración:

- Principio de permiso predeterminado: no se bloquea ningún tráfico, los paquetes no autorizados se tienen que definir explícitamente; tiene como desventaja que los riesgos se deben conocer de antemano.
- Principio de negación predeterminado: se bloquea todo el tráfico, los paquetes autorizados se deben definir explícitamente.

Desde el punto de vista de la seguridad, va a ser recomendable trabajar bajo el principio de negación predeterminado para las reglas de entrada. Esto se debe a que, si se utilizara el principio de permiso predeterminado, se deberían conocer todas las excepciones, lo cual es prácticamente imposible.

Phoenix Contact cuenta con una familia de routers/firewalls denominada mGuard, los cuales permiten otorgar mayor seguridad a la red de OT, proteger equipamiento específico, y vincularlo de la manera más segura a la red de IT.

Es importante tener en cuenta que para realizar una correcta configuración de los *firewalls* no solamente es necesario tener conocimiento de la red y los protocolos de comunicación involucrados, sino que también es parte fundamental saber configurar los equipos correctamente y aplicar todas sus funcionalidades. Es por ello que Phoenix Contact ofrece cursos de capacitación gratuitos, donde se podrán adquirir conocimientos de ciberseguridad, como configurar correctamente los *firewalls* y explotar al máximo sus funcionalidades de red como NAT, port *forwarding*, configuración y utilización de conexiones VPN, junto con herramientas para aplicar mantenimiento remoto a través de internet.

Ciberseguridad: no todo es equipamiento de red

La seguridad de las redes no solamente está vinculada a la utilización de equipamiento de red. Es necesario tener en cuenta temas como la utilización de contraseñas seguras y no utilizar contraseñas estándar o idénticas para todos los equipamientos. Es necesario que las empresas tengan una política de seguridad clara con capacitaciones hacia el personal, de manera de poder entender y detectar potenciales amenazas como el *phishing*, o utilizar correctamente un software antivirus, entre otras cosas.

Para tener mayor seguridad y disponibilidad de las redes también es importante tener en cuenta funcionalidades como la redundancia de redes, de manera de poder seguir teniendo conectividad con todos los equipamientos de planta por más que un conexionado sufra un desperfecto. Es por ello que se destaca la importancia de switches gestionables como los switches 2000, los cuales pueden manejar protocolos de redundancia como MRP o RSTP.

No solamente es conveniente contar con la redundancia de redes, sino también con la redundancia de alimentación, por lo cual una opción es la familia de fuentes Quint, que puede proveer alimentación redundante con la utilización de o'rings, e ininterrumpida con la utilización de UPS.

Palabras finales

La implementación de equipamiento de seguridad como *firewalls*, sumados a una infraestructura de red robusta y unas políticas de ciberseguridad claras van a facilitar la integración cibersegura de los equipamientos industriales a las redes potencialmente peligrosas. Phoenix Contact cuenta con personal idóneo y altamente capacitado para brindar el soporte necesario. ❖

Es importante conocer qué equipos hay en la red de automatización y saber si presentan vulnerabilidades.

Referencias

[1] https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf

[2] https://us-cert.cisa.gov/ics

[3] https://www.phoenixcontact.com/online/portal/pc/pxc/offcontext/insite_landing_page/!ut/p/z1/xZRRT4MwFIV_DY_kdtC19ZHgsoWFuDkn0BdSoGB1FObI0H8v00czwC-zEvjRNzjn33jb9gEMIXIuzKkSjKi0O3TniJGbW2l0t8cxnlm-hLVuSte04D3Q7h2fgwFPd1M0LRHWaSQO1MjF-QledppRv50RhI6ZNqZHwQOlO6iGtRyJOBBLVmVGJqi-hwTE6c0MQXFzLQTkuR3WNhIoHGqSwt1qjKlRqmDvpm8O-QHeP3K_f4PH-dGV5aAhf9T56VUBmUFwVrKFva7ey-4Jd3-8nhUaqmDfWKE_3kfTxk_b_QJPG0-mjaeTxu9v7d4b-hsdr9Tr8cidDko_-IHwv6gUXlYbIE2v4IKSb0EPK3aZjO8X8SZ-0Ny7UZcnsT6XMyDu37VNeugn7vQXm2yNzvgBXSF9v/?urile=wcm:path:/pcen/web/offcontext/insite_landing_pages/a7217e47-af46-4c7b-a748-3b6bf94a30a0/a7217e47-af46-4c7b-a748-3b6bf94a30a0