Pablo López López. Ingeniero de Telecomunicación.

Ciberresiliencia industrial e infraestructuras críticas

Los Ingenieros de Telecomunicación tenemos un papel clave en las organizaciones para garantizar la seguridad de las infraestructuras críticas, la continuidad del negocio de las industrias y la prestación de servicios a los ciudadanos, porque aportamos nuestros conocimientos técnicos y nuestra visión de negocio de alto nivel, **asegurando la ciberresiliencia frente a los ciberataques** y los nuevos modelos de ataque de guerra híbrida.

Desde múltiples puntos de vista, los Ingenieros de Telecomunicación tenemos una participación decisiva para garantizar la seguridad de las infraestructuras críticas, la continuidad del negocio en las organizaciones privadas y la prestación de servicios a los ciudadanos en las administraciones públicas.

Según el último Mapa socio-profesional del titulado en Ingeniería de Telecomunicación realizado en 2017 por el COIT, en colaboración con la consultora IDC, vemos que la gran mayoría de los Ingenieros de Telecomunicación realizan tareas técnicas. Pero también se descubre que un 55,4% realiza tareas

Cada vez más existen dispositivos IoT conectados a las redes corporativas mediante el protocolo TCP/IP que no incluyen la seguridad desde el diseño

de gestión, administración o dirección dentro de las organizaciones. La conexión entre el mundo de los negocios y el mundo de las telecomunicaciones es clara, puesto que éste es una herramienta clave para conseguir la transformación digital en la que se han embarcado estas organizaciones.

Los Ingenieros de Telecomunicación que ocupan puestos directivos tienen muy claro el impacto que tiene sobre la continuidad del negocio o de la prestación del servicio el que la organización industrial o la infraestructura crítica se vean comprometidos. Por eso promueven activamente políticas de concienciación sobre ciberseguridad dentro de las organizaciones y se aseguran de que se establezcan medidas técnicas que minimicen los riesgos de sufrir ciberataques que tengan un grave impacto sobre el negocio. Entienden la importancia de la resiliencia, o la capacidad que tiene la organización de resistir ante una situación adversa, y de recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometida. Y son imprescindibles para participar en la elaboración de planes de contingencia y continuidad de negocio, ya que aportan una visión técnica y de negocio de alto nivel que ayuda a proteger los activos críticos de la organización, sin los que no se puede prestar el servicio.

Ataques a organizaciones industriales

En marzo de 2019, Norsk Hydro, uno de los principales productores de aluminio del mundo, sufrió un ciberataque que paralizó durante semanas varias plantas industriales. El impacto económico de este ataque se ha valorado en más de 75 millones de dólares.

Las organizaciones industriales están evolucionando hacia la *Smart Factory*, dentro del concepto de Industria 4.0. Es la industria conectada, en la que se están desplegando miles de dispositivos IoT para disponer de la máxima información posible para tomar decisiones de negocio. También, gracias a la tecnología móvil 5G, es posible desplegar

Planta de agua Israel

redes privadas móviles en las plantas industriales. Pero todo esto ha aumentado la superficie de ataque en las organizaciones, y las vulnerabilidades a las que deben enfrentarse, al difuminarse el perímetro de defensa.

En las organizaciones industriales se utilizan protocolos específicos, sistemas SCADA y múltiples PLC en las líneas industriales. Pero cada vez más existen dispositivos IoT conectados a las redes corporativas mediante el protocolo TCP/IP que no incluyen la seguridad desde el diseño. Se despliega infraestructura WiFi en las plantas industriales, con redes para invitados mal configuradas y con acceso a la red OT (tecnología de operaciones), y se establecen conexiones remotas con los fabricantes de maquinaria para que realicen tareas de mantenimiento sin el control del departamento de IT (tecnología de información) corporativo.

Además, debido a la situación actual provocada por la pandemia de la COVID-19, se ha promocionado fuertemente el teletrabajo de los empleados. Muchas organizaciones han implementado el protocolo RDP (Remote Desktop Protocol) para permitir que sus empleados puedan acceder al escritorio del equipo de trabajo desde los lugares donde permanecían confinados, utilizando sus routers WiFi caseros y sus equipos personales, sin una política BYOD (Bring Your Own Device) clara.

Las empresas muchas veces dejan sus puertos RDP abiertos sin tomar las medidas de seguridad adecuadas, lo que

Los Ingenieros de Telecomunicación somos decisivos para garantizar la seguridad de las infraestructuras críticas en las organizaciones

Robots industriales SEAT

ha generado un aumento exponencial en los ataques de fuerza bruta contra las conexiones RDP, permitiendo a los ciberdelincuentes obtener acceso y controlar por completo el dispositivo de los empleados, ganando el acceso a la información corporativa.

Ataques a infraestructuras críticas

También las infraestructuras críticas sufren este tipo de ataques, y los Ingenieros de Telecomunicación somos imprescindibles para hacerles frente. Son aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permiten soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales, y pueden afectar a las vidas de los ciudadanos.

El pasado mes de abril de 2020, un ataque a los sistemas de distribución de agua en Israel atribuido a Irán intentó que fallaran las bombas de agua, para dejar sin suministro de agua a miles de personas, y aumentar significativamente los niveles de cloro en el agua potable, pudiendo hacer enfermar a cientos de personas. Unas semanas después, el puerto iraní de Shahid Rajaee en el Estrecho de Ormuz se vio afectado por un ciberataque atribuido a Israel que paralizó durante días el tráfico de mercancías en el puerto.

Como podemos comprobar con estos ejemplos, la seguridad de los organismos definidos como infraestructuras críticas es clave para garantizar la continuidad de la prestación de los servicios a los ciudadanos. El ciberespacio es el quinto dominio de guerra. Pero el nuevo modelo de guerra híbrida, que aúna ataques físicos junto con ciberataques a objetivos específicos, limita la capacidad de respuesta ante este nuevo tipo de ataques. Los atacantes han modificado sus tácticas, técnicas y procedimientos (TTP), lo que obliga a los responsables de la seguridad de las infraestructuras críticas a desarrollar metodologías de análisis y respuesta como MITRE Att&ck Framework o CAT (Intelligence-Led Cyber Attack Methodology) para adaptarse y hacer frente a este nuevo tipo de amenazas. ■

El nuevo modelo de guerra híbrida, que aúna ataques físicos junto con ciberataques a objetivos específicos, limita la capacidad de respuesta

El valor de los Ingenieros de Telecomunicación

- Para minimizar los riesgos asociados a todas estas situaciones, tanto en los departamentos de IT corporativos como en los puestos directivos de estas organizaciones industriales y de infraestructuras críticas debe haber Ingenieros de Telecomunicación que entiendan el impacto sobre el negocio de estos ataques.
- Deben ser capaces de garantizar una buena segmentación entre las redes IT y OT mediante la aplicación del conjunto de estándares IEC 62443/ISA-99 y de buenas prácticas NIST SP 800-82, para evitar que un posible incidente que se produzca en la red IT se propague a la red OT y paralice la producción industrial.
- También deben ser capaces de analizar la topología de las redes, para evitar el grave riesgo de la aparición del *Shadow* IT, el uso de *hardware* o *software* relacionado con TI por parte de un departamento o individuo sin el conocimiento del departamento de IT corporativo, para garantizar la seguridad de las comunicaciones y evitar el ciberespionaje industrial y la exfiltración de información crítica para las organizaciones.
- Y deben asegurarse de la concienciación en ciberseguridad de todos los empleados para evitar ser víctimas de este tipo de ciberataques.