Señalan que casi el 50 % de ataques de ransomware afectan a la industria

- *Además, también podría verse afectada la infraestructura crítica de las ciudades*

Por staff Infosecurity Mexico.

Hablar de ciberseguridad debe llevarnos a reflexionar sobre las vulnerabilidades que nos afectan en los diferentes ambientes en los que nos movilizamos e interactuamos, ya sea en el doméstico, el del transporte, oficina, fábrica, o en cualquier otro, porque prácticamente todo el día estamos conectados a un dispositivo enlazado a Internet, tanto en redes caseras, privadas o públicas.

Y desde luego, los entornos industriales no son la excepción. Como usuarios finales, quizá no escuchamos frecuentemente sobre las amenazas y los ataques que sufren las fábricas y las plantas de producción de distintos artículos, pero lo cierto es que los cibercriminales están aprovechando las nuevas vulnerabilidades de la industria un 43% más rápido que en el primer semestre de 2023, de acuerdo con un informe especializado[1].

De hecho, el mismo reporte señala que el 44% de todas las muestras de ransomware y wiper se dirigieron a los sectores industriales, aunque se denota cierta desaceleración en los ataques de secuestros de datos en el último año, probablemente porque los ciberdelincuentes dejaron la estrategia tradicional de “distribución y oración” para diseñar estrategias dirigidas a las industrias de energía, atención médica, manufactura, transporte, logística, y automotriz.

Vale la pena considerar que con el transcurso del tiempo, los negocios y el entorno industrial han dependido de recursos como la Tecnología Operativa (OT - hardware y software para controlar y monitorizar dispositivos, procesos físicos e infraestructuras); o como los Sistemas de Control Industriales (ICS - hardware y software que automatizan los procesos de producción, monitorizan y soportan la infraestructura industrial), o los Sistemas de Control de Supervisión y Adquisición de Datos (SCADA – para el control de los equipos, y para recopilar y registrar datos operativos).

Y es que el uso de tales elementos, en conjunto, incluso rebasan el propio entorno industrial para utilizarse como elementos de apoyo y contribuir al abasto de agua, electricidad y gas a las viviendas, transportar la gasolina necesaria para los vehículos, apoyar el funcionamiento del transporte público, y desde luego, fabricar productos de consumo como alimentos, medicamentos y bebidas[2].

Cabe destacar que la tecnología operativa (OT), no se diseñó originalmente para el mundo digital, del que hemos visto su desarrollo acelerado en etapas recientes, y por ello, gran parte de la infraestructura crítica, que incluye a las instalaciones, sistemas físicos o servicios esenciales y de utilidad pública vitales para el funcionamiento de la sociedad y la economía, se ejecuta en sistemas heredados (obsoletos, pero que siguen en uso) que son más susceptibles a los ciberataques.

Por ello, muchos de estos sistemas no tienen las características y capacidades de protección que incluyen los equipos modernos (como software antivirus, parches de seguridad, contraseñas, y otros elementos), pero la necesidad de generar y recibir información en tiempo real para tomar decisiones y optimizar el rendimiento ha requerido que estén conectados a las redes comerciales e Internet.

[1] https://n9.cl/fqzcz
[2] https://n9.cl/cx2d5

Ante tal panorama, los ciberataques a estos sistemas pueden afectar la seguridad de los trabajadores y del público, así que la infraestructura crítica no solo debe proteger estos sistemas contra ataques, sino que también debe incorporar resiliencia operativa para que las operaciones sigan funcionando en caso de que un ciberataque tenga éxito.

Son varios los daños que pueden causar los ciberataques a los sistemas OT/ICS/SCADA, como afectaciones al abasto de agua, energía, combustible y gas; pérdida de servicios de comunicaciones, en celulares y en líneas fijas; interrupciones en servicio de transporte público o privado, de cualquier modalidad; escasez de productos de consumo de limpieza, medicinas y otros; y como consecuencia, movimientos sociales de protesta ante la falta de estos servicios.

Pero ante ese posible escenario, existen alternativas tecnológicas para prevenir ciberataques y para corregir los daños, y es parte de la razón de ser de Infosecurity Mexico, evento en el que los profesionales de la ciberseguridad conocerán soluciones comprobadas y nuevas, para tales fines, además de que se enterarán de las mejores prácticas en esa materia los próximos 22 y 23 de octubre, en el Centro Citibanamex de la CDMX. Aquí la información:
https://www.infosecuritymexico.com/es/visitantes/pases.html

Facebook: https://www.facebook.com/infosecmexico
LinkedIn: https://www.linkedin.com/company/infosecurity-mexico/
Instagram: https://www.instagram.com/infosecuritymexico?igsh=MWxkeDhzM2Q0N2J3Yw==
Mail de contacto: info@infosecuritymexico.com

###

Artículos para prensa: Prensa (infosecuritymexico.com)

Acerca de RX: RX es líder global en eventos y exposiciones, aprovechando la experiencia de la industria, los datos y la tecnología para construir negocios para individuos, comunidades y organizaciones. Con presencia en 25 países en 42 sectores industriales, RX organiza aproximadamente 350 eventos anualmente. RX se compromete a crear un ambiente laboral inclusivo para todas nuestras personas. RX capacita a las empresas para prosperar aprovechando ideas impulsadas por datos y soluciones digitales. RX es parte de RELX, un proveedor global de herramientas de análisis y toma de decisiones basadas en información para clientes profesionales y comerciales. Para obtener más información, visite www.rxglobal.com.

Acerca de RELX: RELX es un proveedor global de herramientas de análisis y toma de decisiones basadas en información para clientes profesionales y comerciales. RELX atiende a clientes en más de 180 países y tiene oficinas en aproximadamente 40 países. Emplea a más de 36,000 personas, más del 40% de las cuales están en América del Norte. Las acciones de RELX PLC, la empresa matriz, se negocian en las bolsas de Londres, Ámsterdam y Nueva York utilizando los siguientes símbolos bursátiles: Londres: REL; Ámsterdam: REN; Nueva York: RELX.

*Nota: La capitalización de mercado actual se puede encontrar en http://www.relx.com/investors

Para mayor información: Jorge Morales García / Agencia Communika
T: +52 55 1795 2790 E: jorgem@communika.com.mx