ALERTA: Ataques de RANSOMWARE a empresas de Agua Potable y de Desperdicios (Basura) (06/DICIEMBRE/2021)

Cooperación Inter Agencias de los Estados Unidos de Norte América, reportaron en octubre de 2021, amenazas para comprometer redes, sistemas y dispositivos de TI y OT en industrias de distribución de agua potable y desperdicios.

Introducción

Una investigación en conjunto con CISA, EPA, FBI y NSA de los EEUU, detectaron actividad cibernética maliciosa por parte de varios actores, dirigidos a las redes, sistemas y dispositivos de tecnología de la información (TI) y tecnología operativa (OT) de las instalaciones del Sector de Sistemas de Agua y Aguas Residuales (WWS) de EE.UU.

Se generaron intentos de comprometer la integridad de sistemas, a través de un acceso no autorizado mediante vectores de ataque comúnmente conocidos. Se solicita a las Instituciones implementar múltiples barreras descritas en la sección recomendaciones de esta alerta.

En 2021, se registraron principalmente tres ciberataques dirigidos a EEUU, el primero fue de tipo ransomware Ghost a una planta en California; el segundo, de tipo ransomware ZuCaNo, el cual logró ingresar a través de un acceso remoto en una computadora SCADA de una planta en Maine; y el tercero, de tipo ransomware Darkside, dirigido a la compañía de oleoducto Colonial Pipeline en Estados Unidos, que causó la interrupción del servicio y amenazó la distribución de combustible en gran parte del territorio norteamericano.

Vector de ataque: Phishing, movimiento lateral, explotación de sistemas sin actualización a nivel de OS/Firmware.

En organizaciones con infraestructura TI con sistemas OT, los atacantes pueden obtener acceso a los activos OT, después de que la red de TI se haya visto comprometida a través de spear phishing y otras técnicas derivadas del mismo, y que son de las más comunes actualmente. Adicionalmente, pueden realizar explotación de servicios y aplicaciones conectados a Internet que permiten el acceso remoto a redes, como por ejemplo, escritorios remotos expuestos al mundo.

Es probable que los actores de amenazas busquen aprovechar las distintas debilidades de organizaciones que no tienen, o eligen no priorizar recursos, en lugar de la modernización de la infraestructura de TI / OT. Las instituciones tienden a asignar recursos a la infraestructura física que necesita ser reemplazada o reparada (por ejemplo tuberías) en lugar de la infraestructura de TI / OT a nivel de software/hardware

Impacto:

La pérdida de control, pérdida de la información, secuestro de información, o generación de sistemas fuera de línea de infraestructuras críticas, o de agua potable y residuos como en el caso de lo ocurrido en EEUU, pueden generar una crisis local (ciudades principales), o Nacional de ser el caso. Dejando a la población local de cientos de miles o de millones de habitantes en las distintas ciudades de Ecuador, sin acceso al sistema de agua potable, y con una recolección de residuos colapsada en ciudades, barrios, calles y aceras; así como también, plantas de tratamiento fuera de línea, que se convertirían en bombas de tiempo que podrían causar afectaciones ambientales críticas e irreparables de ser el caso. Sumado a las pérdidas millonarias, recursos que en muchos de los casos, son imposibles de cuantificar y recuperar.

Recomendaciones:

El Centro de Respuesta a Incidentes Informáticos, EcuCERT, de la ARCOTEL, ante lo expuesto, recomienda:

- Tener una arquitectura de IT, totalmente aislada de la arquitectura de OT.
- Utilizar sistemas de autentificación de doble factor, sumado al uso de contraseñas robustas.
- Utilizar listas de bloqueo y acceso previamente configuradas de forma óptima a través de la seguridad perimetral.
- Cierre de puertos de red no necesarios para el trabajo diario de sistemas IT/OT.

- Implementar un plan de respuesta a emergencias de la organización, considerar la gama completa de impactos potenciales que los ciberataques plantean a las operaciones, incluida la pérdida o manipulación de la vista, la pérdida o manipulación del control y las amenazas a la seguridad.
- No abrir, manipular, o interactuar con correos electrónicos altamente sospechosos recibidos en las respectivas bandejas de correo ya sea personales o Institucionales.
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Identificar y suspender el acceso de usuarios que exhiban una actividad inusual.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

Referencias

Ciberseguridad LATAM. (n.d.). Retrieved from
(2021)
Grupos de ransomware apuntan a plantas de tratamiento de agua
https://www.ciberseguridadlatam.com/2021/12/04/grupos-de-ransomware-apuntaron-a-plantas-de-tratamiento-de-agua/

The United States Computer Emergency Readiness Team (US-CERT) an organization within the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Retrieved from
(2021)
Ongoing Cyber Threats to U.S. Water and Wastewater Systems
https://us-cert.cisa.gov/ncas/alerts/aa21-287a