Riegos

Un estudio realizado por el Instituto SANS de cientos de profesionales de sistemas de control industrial (ICS) y las partes interesadas de seguridad cibernética en diversas industrias verticales, incluyendo la energía, la industria manufacturera, y el petróleo y el gas ha revelado que 4 de cada 10 profesionales del ICS carecen de visibilidad en sus redes ICS.

Esto significa que el 40% de los los defensores están trabajando con los ojos vendados. Siendo incapaces de detectar un ataque cibernético, averiguar de dónde viene y remediarlo en una cantidad de tiempo razonable. Una estadística aún más aterrador si se tomamos en cuenta todo lo que ya hemos comentado en posts anteriores: las amenazas a los sistemas de ICS son altos, o severa y crítica.

Al investigar sobre las amenazas que se detectan en la industria, las cuatro más apremiantes son:

- Añadir dispositivos que no pueden protegerse a sí mismos a la red.
- Incidentes internos estimulados por acciones accidentales.
- Amenazas externas de hacktivistas y ataques financiados.
- Extorsión – incluyendo ransomware.

Las amenazas de seguridad cibernética que afectan a los sistemas de control industrial están creciendo y la identificación de ataques sigue siendo un reto importante según la encuesta anual sobre los sistemas de control

industrial llevada a cabo por el SANS Institute, en la que participaron algunos líderes de la industria como Nozomi redes. Esta encuesta llegó a la conclusión de lo que ya venimos comentando tiempo atrás: a pesar de que se hayan realizado avances en la protección de activos críticos e infraestructura, han surgido nuevas amenazas.

Como sugiere la frase inicial, cuatro de cada 10 profesionales de la seguridad ICS carecen de visibilidad en sus redes ICS, que es uno de los principales impedimentos para asegurar estos sistemas. Por estos motivos, el ransomware fue recientemente identificada como una amenaza parte superior, junto con la creciente adición de dispositivos a la red.

A pesar de la cobertura de noticias casi a diario de los recientes ataques a los sistemas sin parches, SANS encontró que sólo el 46% de los encuestados se aplica regularmente los parches del fabricante; y 12% no aplica ni los parches de seguridad ni de capa de protección alrededor de los activos críticos del sistema de control.

Además de los riesgos ya comentados, existen muchas otras amenazas que acechan a los sistemas de control industrial. Entre ellos están:

- El alto número de cuentas privilegiadas o de administración que permiten al usuario o a las aplicaciones acceder al ICS
- El uso de cuentas compartidas que permite el acceso a sistemas críticos sin ningún tipo de supervisión.
- El uso de aplicaciones industriales con credenciales *hard-coded* embebidas.
- Es uso de estaciones de trabajo con privilegios

administrativos completos.

Tal es el riesgo, que es necesario afrontar estas amenazas de una forma proactiva, de tal forma que prever el riesgo se vuelve una prioridad. Es tal, que están apareciendo en el mercado un sin fin de soluciones que permiten a las empresas gestionar sus riesgos y su seguridad de una forma más cómoda.

Como ya hemos comentado anteriormente, el gran problema, y de donde vienen la mayoría de los riesgos, es de conectar al Internet unos sistemas que no estaban pensados para ser conectados. Los sistemas SCADA son otro de los grandes riesgos que tiene la industria. Estos sistemas estaban pensados con una robustez innegable, y son impenetrables cuando son atacados desde los flancos para los que tienen sus defensas preparadas. Sin embargo, la conexión a Internet no es un flanco para el que estuvieran preparados. Además, a todo esto se suma la poca tolerancia a cambios que tienen los SCADA. Están pensados para ser instalados y durar décadas, no para que se les apliquen los frecuentes parches de firmware a los que tan acostumbrados estamos ya. Por ello, las compañías están dejando de utilizar estos sistemas, que han dejados de responder a una industria en constante cambio.

En conclusión, la mayoría de los riesgos surgen de la entrada de Internet en la industria, algo con muchas ventajas, de las que las empresas quisieron aprovecharse lo antes posible, pero descuidaron uno de los aspectos más importantes: la seguridad.

Referencias:

Industrial Control Systems Security, consultado el 7 de noviembre. https://www.cyberark.com/solutions/security-risk-management/industrial-control-systems-security-compliance/

Applied Risk: An established leader in Industrial Control Systems security, consultado el 7 de noviembre. https://applied-risk.com/

https://www.technologyreview.com/s/511671/cybersecurity-risk-high-in-industrial-control-systems/