KASPERSKY lab

Kaspersky Security Bulletin 2018

PREDICCIONES SOBRE LAS AMENAZAS PARA LA SEGURIDAD INDUSTRIAL EN 2019

Los últimos años han sido muy intensos y activos en lo referente a incidentes que afectaron la seguridad informatica de los sistemas industriales. Entre ellos, nuevas vulnerabilidades, nuevos vectores de amenaza, infecciones accidentales de sistemas industriales y ataques selectivos detectados. En respuesta, el año pasado elaboramos algunas Predicciones sobre las amenazas para la seguridad industrial en 2018, con una descripción de las tendencias más probables para el año.

En general, el entorno de amenazas para la ciberseguridad industrial avanza a un ritmo más lento y más rígido que el entorno de amenazas para las tecnologías informáticas. Los ataques contra los Sistemas de control industrial (ICS) aún son difíciles de monetizar. Las organizaciones industriales siguen fuera del ámbito de la mayoría de los ciberdelincuentes. Son un blanco relativamente reciente para los adversarios que ya han comenzado a atacarlas. Siguen aplicando herramientas y tácticas existentes a sus ataques. Por este motivo, a pesar de que algunas de las predicciones sobre las amenazas industriales para el año pasado se cumplieron, la mayoría sigue en curso.

Los especialistas de Kaspersky Lab han dedicado varios años a la investigación del entorno de ciberamenazas para las organizaciones industriales e intentan llevar su experiencia y tecnología a los entornos de tecnología operativa (TO). Todavía nos queda un largo camino por delante, con varias dificultades y problemas que resolver. Gracias al contacto permanente con muchos investigadores en otras organizaciones de seguridad y con algunos pioneros en seguridad de ICS de las empresas industriales, hemos llegado a la conclusión de que algunas de las dificultades que enfrentamos son comunes a toda la industria. Resolverlas es fundamental para que el mundo sea un lugar más seguro.

Por ello, mientras aguardamos que la niebla de predicciones y amenazas para 2018 se disipe, hemos decidido enfocarnos en los principales problemas que podrían afectar el trabajo de los profesionales involucrados en los sistemas industriales para 2019.

LOS CUATRO PRINCIPALES DESAFÍOS DE CIBERSEGURIDAD QUE ENFRENTARÁN LAS EMPRESAS INDUSTRIALES EN 2019

1. El aumento constante de la superficie de ataque

El incremento de los sistemas de automatización, la variedad de herramientas de automatización, la cantidad de organizaciones y personas con acceso directo o remoto a los sistemas de automatización y el surgimiento de los canales de comunicación para el monitoreo y el control remoto entre objetos antes independientes, son factores que aumentan las oportunidades de planificación y ejecución de ataques de los ciberdelincuentes.

2. El creciente interés de los ciberdelincuentes y los servicios especiales

Una menor rentabilidad y mayores riesgos en los ciberataques dirigidos a víctimas tradicionales están obligando a los ciberdelincuentes a buscar nuevos blancos, entre los que se encuentran las organizaciones industriales.

Al mismo tiempo, los servicios especiales en muchos países, junto con otros grupos organizados (motivados por intereses políticos internos y externos) y grupos con motivación financiera, tienen un compromiso activo con la investigación y el desarrollo de técnicas para implementar espionaje y ataques terroristas dirigidos a empresas industriales.

Si se tiene en cuenta el contexto geopolítico, el desarrollo de sistemas de automatización de las empresas industriales, además de la transición a nuevos procesos de administración y modelos de producción y actividad económica, esta situación seguirá desarrollándose en los próximos años y afectará de forma negativa a las organizaciones industriales.

3. La subestimación de los niveles generales de amenazas

La falta de acceso público a la información sobre los problemas de seguridad de la información dentro de las empresas industriales, junto con la rareza relativa de los ataques dirigidos contra los sistemas de automatización, una confianza exagerada en los sistemas de protección de emergencia y la negación de la realidad objetiva tienen un efecto negativo en la evaluación de los niveles de amenaza que hacen los propietarios y los operadores de las empresas industriales y su personal.

4. El malentendido de los aspectos específicos de las amenazas y la elección poco afortunada de opciones de protección

En el universo de la ciberseguridad industrial, varios incidentes de alto perfil, llevados a cabo con la ayuda de ataques dirigidos contra una cantidad muy limitada de víctimas, generaron un panorama informático que conformó la idea de amenaza potencial, tanto entre los investigadores de seguridad informática y los desarrolladores de seguridad, como entre los posibles usuarios de estas herramientas.

No obstante, la mayoría de los posibles usuarios tenía dificultades para comprender los informes profesionales de estos incidentes, que, además, carecían de detalles importantes sobre TO. El campo de información que se forma bajo estas condiciones, que conlleva la ausencia de la necesidad diaria de desviar los ataques dirigidos a los sistemas de control automáticos, brindó a los desarrolladores una oportunidad para crear productos que quizás funcionen mejor en los escenarios artificiales imaginados por los investigadores que contra las amenazas diarias reales. Esto podría ocasionar que los sistemas de automatización de las empresas industriales queden expuestos a los ataques reales, incluidos los ataques aleatorios y las campañas de ataques dirigidos organizadas por los ciberdelincuentes.