MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokio 100-8310 (Japón)

PARA SU PUBLICACIÓN INMEDIATA **N.º 3106**

Este texto es una traducción de la versión oficial en inglés de este comunicado de prensa y se le proporciona a modo de referencia, para su comodidad. Consulte el texto original en inglés para obtener detalles específicos. En caso de que ambas versiones difieran, prevalecerá el contenido de la versión en inglés.

Consultas de los clientes

Information Technology R&D Center
Mitsubishi Electric Corporation
www.MitsubishiElectric.com/ssl/contact/company/rd/form.html
www.MitsubishiElectric.com/company/rd/

Consultas de los medios

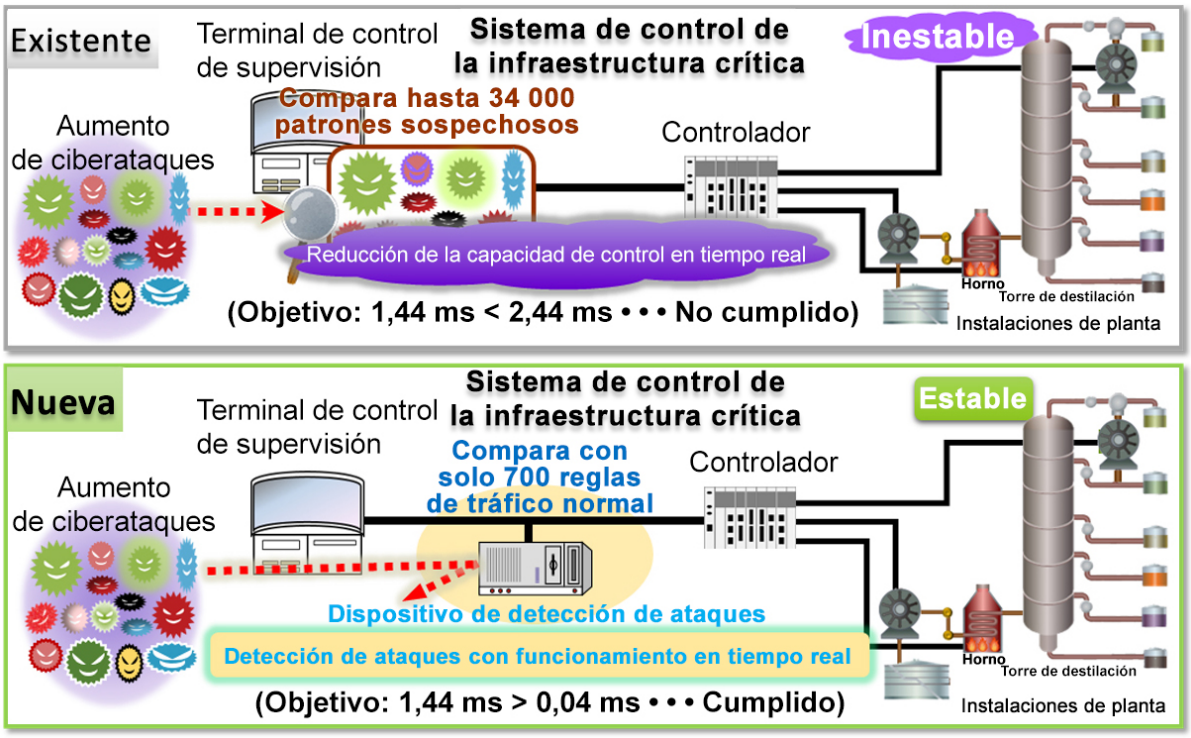
Public Relations Division
Mitsubishi Electric Corporation
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric desarrolla una tecnología de detección de ataques cibernéticos para sistemas de infraestructuras críticas

La detección en tiempo real de ciberataques a sistemas de control contribuirá a la estabilidad de las infraestructuras

TOKIO, 17 de mayo de 2017 – Mitsubishi Electric Corporation (TOKIO: 6503) ha anunciado hoy el desarrollo de una tecnología de detección de ataques cibernéticos capaz de identificar rápidamente todo el tráfico de red que difiere de los comandos normales en los sistemas de control de la infraestructura crítica. Esta tecnología detecta sofisticados ataques cibernéticos, disfrazados de comandos normales, que van destinados a infraestructuras críticas de diversos sectores: energía eléctrica, gas natural, agua, productos químicos y petróleo. Además, no influye en la capacidad de control en tiempo real de la infraestructura, ayudando así a garantizar su estabilidad.

La comercialización de las infraestructuras de energía eléctrica está prevista para el año fiscal 2018. Se desarrollarán otras aplicaciones para la seguridad cibernética de la infraestructura crítica en colaboración con la iniciativa Strategic Innovation Promotion Program (SIP, Programa de Promoción de la Innovación Estratégica).



Los resultados obtenidos de "Ciberseguridad para la infraestructura crítica", que ha llevado a cabo el Centro de Seguridad de Sistemas de Control (CSSC), han respaldado inicialmente la implementación de la nueva tecnología. "Ciberseguridad para la infraestructura crítica" forma parte del Programa de Promoción de la Innovación Estratégica (SIP), que ha impulsado el Consejo de Ciencia, Tecnología e Innovación y que ha llevado a cabo la Organización para el Desarrollo de Tecnología Industrial y Nuevas Energías (NEDO).

Características clave

- A fecha del 17 de mayo de 2017, esta tecnología fue la primera en definir las reglas de detección basadas en los comandos normales para cada estado de funcionamiento del sistema de control y en interpretar las desviaciones de los comandos normales como ataques.
- Según nuestra consideración, se garantiza el funcionamiento en tiempo real del sistema de control durante la detección de ataques, ya que la tecnología no implica un laborioso proceso de cotejo de patrones sospechosos.
- La tecnología contribuye a la estabilidad de las infraestructuras, reduciendo el tiempo de detección y garantizando un mínimo impacto en los procesos de los sistemas de control, que deben finalizarse dentro de unos determinados límites de tiempo.

Comparación con tecnologías existentes

	Método	Funcionamiento en tiempo real de los sistemas de control	Viabilidad
Nueva	Detecta la desviación de las reglas de comandos normales que determina el estado de funcionamiento	Bajo impacto debido a reglas concisas de los comandos normales	Eficacia probada en simulaciones de sistemas de plantas
Existente	Compara patrones sospechosos con un elevado número de reglas	Riesgo de alto impacto debido al aumento de ciberataques	Se utiliza actualmente en sistemas empresariales

Ha habido casos en los que ciberataques complejos han penetrado los sistemas de control para emitir comandos que parecían normales y que apenas se podían distinguir de los comandos reales. Los métodos de detección existentes, que comparan el tráfico entrante con patrones sospechosos comunes, no pueden detectar estos ataques. La comparación con el enorme volumen de patrones sospechosos comunes puede durar mucho tiempo y causar fallos en el funcionamiento del sistema de control.

Mitsubishi Electric comprobó que, dependiendo de si el sistema está o no en funcionamiento o en mantenimiento, el tráfico normal de un sistema de control de infraestructura crítica es diferente. Por tanto, la nueva tecnología emplea diferentes reglas de detección para cada estado de funcionamiento. Debido al aumento continuo de ciberataques, se necesita una enorme cantidad de tiempo para generar patrones sospechosos y buscar coincidencias. Sin embargo, el número de comandos normales de los sistemas de control es limitado. Por tanto, las reglas también se pueden limitar, lo que permite a la nueva tecnología de Mitsubishi Electric buscar coincidencias con rapidez, detectar ataques y mantener el funcionamiento en tiempo real de los sistemas de control. Según nuestra consideración, la empresa evaluó el tiempo de procesamiento de la detección de ataques al sistema de control. La evaluación puso de manifiesto que la nueva tecnología solo necesita 0,04 ms para la detección, frente a los 2,44 ms de una tecnología existente; y el requisito en tiempo real se sitúa en 1,44 ms.

Antecedentes

En una época en la que las infraestructuras recurren cada vez más al Internet de las cosas (IoT), cada vez es más importante garantizar la ciberseguridad de las infraestructuras críticas que constituyen los pilares de la sociedad. Hasta ahora, la seguridad de las infraestructuras dedicadas a la energía eléctrica, gas natural, agua, productos químicos y petróleo se basaba en el aislamiento físico, los cortafuegos para controlar el tráfico y una estricta gestión operativa. Sin embargo, en los últimos años se ha producido un aumento, especialmente en el extranjero, de ciberataques avanzados que penetran en los sistemas de control de infraestructuras para enviar comandos maliciosos en forma de comandos normales con el propósito de causar daños, como apagones y destrucción de equipos.

Patentes

Patentes pendientes de la tecnología anunciada en este comunicado de prensa: siete en Japón y otras siete en el extranjero.

###

Acerca de Mitsubishi Electric Corporation

Con más de 90 años de experiencia en el suministro de productos fiables y de alta calidad, Mitsubishi Electric Corporation (TOKIO: 6503) es un líder mundial reconocido en la fabricación, comercialización y venta de equipos eléctricos y electrónicos utilizados en el procesamiento de la información y las comunicaciones, en el desarrollo espacial y las comunicaciones por satélite, en los aparatos electrónicos de consumo, en la tecnología industrial, en la energía, en el transporte y en los equipos de construcción. Aprovechando el espíritu de su declaración corporativa "Changes for the Better" y su declaración medioambiental "Eco Changes", Mitsubishi Electric se esfuerza por ser una empresa internacional comprometida con el medio ambiente líder y por enriquecer la sociedad con la tecnología. La empresa registró ventas de grupo consolidadas de 4 238,6 mil millones de yenes (unos 37,8 mil millones de dólares estadounidenses*) en el ejercicio fiscal que terminó el 31 de marzo de 2017. Para obtener más información, visite:

www.MitsubishiElectric.com

*Tipo de cambio de 112 yenes por dólar estadounidense, tipo concedido por el Mercado de divisas de Tokio el 31 de marzo de 2017