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

ZUR SOFORTIGEN VERÖFFENTLICHUNG **Nr. 3106**

Bei diesem Text handelt es sich um eine Übersetzung der offiziellen englischen Version dieser Pressemitteilung, die nur als Hilfestellung und Referenz bereitgestellt wird. Ausführliche und/oder spezifische Informationen entnehmen Sie bitte der englischen Originalversion. Im Falle von Abweichungen hat der Inhalt der englischen Originalversion Vorrang.

Kundenanfragen

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

Presseanfragen

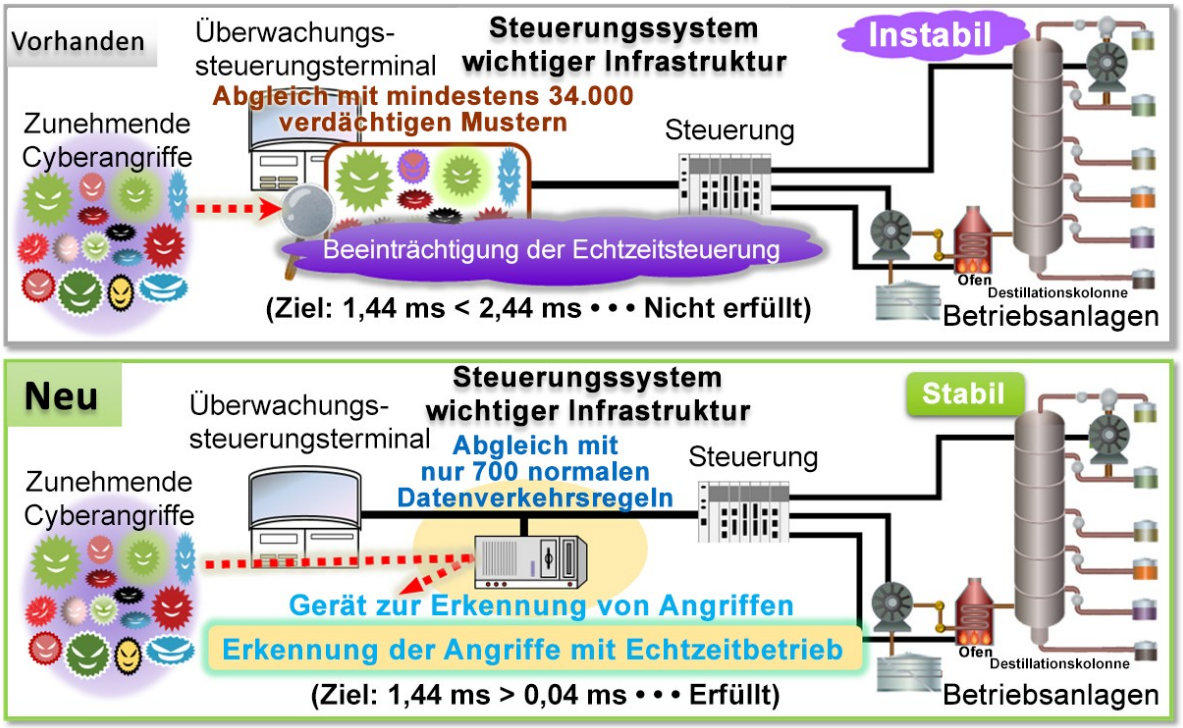
Public Relations Division Mitsubishi
Mitsubishi Electric Corporation
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric entwickelt Technologie zur Erkennung von Cyberangriffen für wichtige Infrastruktursysteme

Die Echtzeiterkennung von Cyberangriffen auf Steuerungssysteme wird zur Stabilität der Infrastruktur beitragen

TOKIO, 17. Mai 2017 – Mitsubishi Electric Corporation (TOKIO: 6503) gab heute die Entwicklung einer Technologie zur Erkennung von Cyberangriffen bekannt, die Netzwerkverkehr schnell identifiziert, der von den vorgegebenen, normalen Befehlen in den Steuerungssystemen wichtiger Infrastruktur abweicht. Die Technologie erkennt ausgeklügelte, auf wichtige Infrastrukturen für Strom, Erdgas, Wasser, Chemikalien und Erdöl gerichtete Cyberangriffe, die als normale Befehle getarnt sind, ohne dabei die Echtzeitsteuerung zu beeinträchtigen. So soll die Stabilität der Infrastruktur sichergestellt werden.

Der gewerbliche Einsatz in der Strominfrastruktur ist ab dem Geschäftsjahr 2018 geplant. Andere Anwendungen für die Cybersicherheit wichtiger Infrastruktur werden in Zusammenarbeit mit dem Strategic Innovation Promotion Program (SIP, strategisches Programm zur Innovationsförderung) entwickelt.



Die Umsetzung der neuen Technologie basiert teilweise auf den Ergebnissen des Projekts „Cybersicherheit für kritische Infrastrukturen", welches vom „Control System Security Center" (CSSC) durchgeführt wurde. Das Projekt ist Teil eines ministerienübergreifenden strategischen Programms zur Innovationsförderung, das vom „Council for Science, Technology and Innovation" gefördert wird und von der „New Energy and Industrial Technology Development Organisation" (NEDO) in Auftrag gegeben wurde.

Hauptmerkmale

- Seit 17. Mai 2017 ist diese Technologie weltweit die erste, die auf der Basis von normalen Befehlen Erkennungsregeln für jeden Betriebszustand des Steuerungssystems definieren und Abweichungen von den normalen Befehlen als Angriffe bewerten kann.
- Bei der Erkennung von Angriffen wird der Echtzeitbetrieb des unter unserer Beobachtung stehenden Steuerungssystems sichergestellt, da die Technologie keinen zeitaufwendigen Abgleich von verdächtigen Mustern erfordert.
- Die Technologie trägt zur Stabilität der Infrastruktur bei, indem die Erkennungszeit verkürzt und ein minimaler Einfluss auf die Prozesse des Steuerungssystems sichergestellt wird, die innerhalb von bestimmten Zeitfristen abgeschlossen sein müssen.

Vergleich mit vorhandenen Technologien

	Verfahren	Echtzeitbetrieb von Steuerungssystemen	Durchführbarkeit
Neu	Erkennung von Abweichungen von normalen Befehlsregeln, die vom Betriebsstatus bestimmt werden	Geringe Auswirkung dank präziser Regeln für normale Befehle	Hat sich in Simulationen für Anlagensysteme bewährt
Vorhanden	Abgleich von verdächtigen Mustern mit einer riesigen Anzahl von Regeln	Risiko einer großen Auswirkung aufgrund zunehmender Cyber-angriffe	Wird derzeit in Unternehmenssystemen verwendet

Es gab Fälle, in denen moderne Cyberangriffe in Steuerungssysteme eingedrungen sind und Befehle erteilten, die man als normal einstufen würde und von den echten Befehlen kaum unterscheiden kann. Vorhandene Erkennungsverfahren, die den eingehenden Datenverkehr mit bekannten, verdächtigen Mustern vergleichen, können derartige Angriffe möglicherweise nicht erkennen. Der Vergleich mit einer riesigen Menge von bekannten, verdächtigen Mustern kann lange dauern und zu Störungen im Steuerungssystem führen.

Mitsubishi Electric hat festgestellt, dass sich der normale Datenverkehr von Steuerungssystemen in wichtiger Infrastruktur unterscheidet, je nachdem, ob das System in oder außer Betrieb ist oder gewartet wird. Daher nutzt die neue Technologie unterschiedliche Erkennungsregeln für jeden Betriebszustand. Angesichts der zunehmenden Anzahl an Cyberangriffen dauert es extrem lange, um verdächtige Muster zu erstellen und nach Übereinstimmungen zu suchen. Doch die Anzahl der normalen Befehle in Steuerungssystemen ist begrenzt. Somit können auch die Regeln begrenzt werden, und die neue Technologie von Mitsubishi Electric kann dadurch schnell nach Übereinstimmungen suchen, Angriffe erkennen und dabei den Echtzeitbetrieb von Steuerungssystemen aufrechterhalten. Das Unternehmen hat für das unter unserer Beobachtung stehende Steuerungssystem die Verarbeitungszeit für die Erkennung der Angriffe ausgewertet. Die Auswertung ergab, dass die neue Technologie nur 0,04 ms und die vorhandene Technologie 2,44 ms für die Erkennung benötigt, während die Echtzeitanforderung bei 1,44 ms liegt.

Hintergrund

Da das Internet der Dinge aus dem Bereich der Infrastruktur kaum noch wegzudenken ist, nimmt die Cybersicherheit für die wichtige Infrastruktur, die unserer Gesellschaft zugrunde liegt, einen immer größeren Stellenwert ein. Bislang wurde die Sicherheit der Infrastruktur für Strom, Erdgas, Wasser, Chemikalien und Erdöl durch physische Isolierung, Firewalls für die Datenverkehrskontrolle und striktes Betriebsmanagement sichergestellt. In den vergangenen Jahren ist jedoch die Zahl von modernen Cyberangriffen, insbesondere im

Ausland, gestiegen, die in die Infrastruktur von Steuerungssystemen eindringen, um böswillige, als normal getarnte Befehle zu senden. Das Ziel dieser Angriffe ist es, Schaden, wie etwa Stromausfälle und Zerstörung von Anlagen, anzurichten.

Patente

Angemeldete Patente für die in dieser Pressemitteilung bekannt gegebene Technologie: 7 in Japan und 7 im Ausland.

###

Über die Mitsubishi Electric Corporation

Mit über 90 Jahren Erfahrung in der Bereitstellung zuverlässiger, hochwertiger Produkte ist die Mitsubishi Electric Corporation (TOKIO: 6503) ein anerkanntes, weltweit führendes Unternehmen in der Herstellung, in der Vermarktung und im Vertrieb von Elektro- und Elektronikgeräten für die Informationsverarbeitung, Kommunikation, Raumfahrtentwicklung und Satellitenkommunikation, Unterhaltungselektronik, Industrietechnik, den Energie- und Transportsektor sowie Gebäudeanlagen. Im Sinne seiner Unternehmensphilosophie „Changes for the Better“ und Umwelterklärung „Eco Changes“ setzt sich Mitsubishi Electric als globales, im Umweltschutz führendes Unternehmen dafür ein, die Gesellschaft mit neuen Technologien zu bereichern. Das Unternehmen verzeichnete konzernweit einen konsolidierten Umsatz von 4.238,6 Mrd. Yen (37,8 Mrd. US-Dollar*) im Geschäftsjahr zum 31. März 2017. Weitere Informationen erhalten Sie unter:
www.MitsubishiElectric.com

* Zum Wechselkurs von 112 Yen für einen US-Dollar, der am 31. März 2017 von der Tokioter Devisenbörse angegeben wurde.