SIEMENS

Siemens México implementa un concepto holístico de ciberseguridad industrial contra un conjunto de amenazas potenciales

- Las aplicaciones que aumentan la productividad pueden integrarse en los entornos industriales rápidamente, con poco esfuerzo y un mínimo riesgo.
- Los ataques cibernéticos relacionados al *phishing* han aumentado un 85% en los últimos meses. México y Brasil son los países con mayor número de ciberataques en América Latina.
- En el marco del Día Internacional de la Seguridad de la Información, Siemens comparte el concepto de protección eficaz que protege a las instalaciones industriales.

Ciudad de México, 30 de noviembre de 2020.- El mundo se está digitalizando de una manera exponencial y se conecta cada vez más desde los dispositivos personales hasta sistemas complejos en las industrias. Hoy en día, el mundo cuenta con más de 17 billones de dispositivos conectados (7 bilones sin contar laptops, celulares o tablets). El trabajo a distancia ha hecho que tanto las empresas como las personas, se conecten desde redes remotas y con un alto flujo de información. Esto para completar todo tipo de actividades, desde tareas escolares hasta el control completo del funcionamiento y operación de las fábricas.

Millones de dispositivos y máquinas inteligentes generan e intercambian cantidades masivas de datos, y generan más de 2.5 quintillones de bytes al día. Para que dimensionemos lo anterior, es importante añadir que 90% del total de datos en el mundo se han producido sólo en los últimos dos años, y 80% del total han sido producto de la data generada en el sector industrial. De esos datos, sólo 5% es analizado y aprovechado en el sector industrial para la toma de decisiones. Por ello, es crucial usar esta enorme cantidad de información para tomar decisiones inteligentes y de valor.

La pandemia ha provocado una latente necesidad de comunicación e intercambio rápido de bienes y productos; como consecuencia, los usuarios deben compartir datos personales y laborales a través de redes inalámbricas buscando facilitar la vida diaria. Sin embargo, debido a esta alza en el uso de medios digitales, se ha incrementado la vulnerabilidad de todos, por lo que estar preparados ante posibles ataques cibernéticos es, hoy más que nunca, imprescindible.

La necesidad del Home Office desató que, tan solo entre marzo y abril, la ciberdelincuencia en México creciera 14% (estimaciones del Centro de Respuesta de Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional). A estas alturas, es probable que se hayan superado los pronósticos en materia de ciberseguridad, que Kaspersky preveía a inicios de año para México y la región en 2020.

Según los últimos reportes, entre enero y septiembre de 2020, se registraron más de 37 millones de ciberataques en países de Latinoamérica como México, Brasil, Chile, Perú, Argentina y Colombia. De éstos, los países más atacados, por número de empresas, son México y Brasil. Al respecto, Natalia Oropeza, Chief Cybersecurity Officer de Siemens a

nivel global, comenta que “la evidente vulnerabilidad ha ocasionado que los ciberataques hayan incrementado en 85%, principalmente el *phishing* que contienen malware, el cual puede venir desde un simple email; de allí la urgente necesidad de que las industrias apliquen normas armonizadas a lo largo de las cadenas de producción para que garanticen la calidad, la seguridad y la protección de los productos, procesos y servicios”.

En mayo pasado, Izumi Nakamitsu, jefa de Desarme de la ONU, indicó que ante la pandemia por COVID-19, se ha registrado un incremento de 600% en correos electrónicos maliciosos. Esto significa que hay un ciberataque cada 39 segundos en algún lugar del mundo.

Un mail sobre una factura que no se ha pagado o un cargo no reconocido a la tarjeta son tan sólo un ejemplo de los mensajes que hacen al usuario abrir un correo electrónico, generando pánico, distrayendo la mente y motivando a investigar qué sucedió. Esto hace que se olvide por completo la veracidad del mensaje y de la seguridad digital, de manera que se ha atrapado a una presa más.

Ante ese panorama y en el marco del Día Internacional de la Seguridad de la Información, Siemens, el grupo tecnológico alemán, recomienda a las empresas digitales que actualmente están generando e integrando más datos, desarrollen un concepto holístico en varios niveles que proteja a la producción de forma integral y a profundidad. Un sistema basado en la seguridad de las plantas, la seguridad de las redes y la integridad de los sistemas según las normas y estándares de seguridad en la automatización industrial.

La seguridad en la planta debe estar enfocada en las necesidades de la producción, es decir, en la personalización, en el análisis de riesgos, y la implementación y seguimiento de las medidas adecuadas como la actualización de software o controles de acceso a áreas sensibles. Por otro lado, la seguridad de la red es clave para una comunicación constante que permita proteger adecuadamente los sistemas de fácil acceso dentro de las plantas y/o corporativos, además de la protección de las redes de automatización contra el acceso no autorizado.

Hay mucho más en la ciberseguridad que la simple instalación de un nuevo antivirus. Incluso cuando las soluciones están en su lugar, el trabajo no termina ahí. Se debe tener un conocimiento completo de los clientes y de la industria, para saber qué ataques son específicos de la Tecnología Operativa (OT) y entender la forma en que los sistemas digitales impactan en los productos y servicios que se ofrecen. Para mantener la integridad del sistema, se requiere de la protección integral contra cambios de configuración no autorizados en el nivel de control, así como contra el acceso no autorizado a la red. Esto facilita la detección de cualquier intento de manipulación de archivos sensibles.

Dentro de su oferta de ciberseguridad industrial, “Defense in Depth”, Siemens utiliza Machine Learning monitoreando activamente una red de equipos de manufactura. Esto para aprender cuál es el comportamiento normal de cierta infraestructura y alertar al ser humano cuando se detecta un comportamiento anómalo que pudiera tratarse de un ciberataque.

Es imperativo adoptar medidas de protección adecuadas, especialmente para las instalaciones de infraestructura crítica. Es esencial un enfoque que abarque todos los niveles simultáneamente -desde el operacional hasta el de campo, y desde el control de

acceso hasta la protección contra copias- para proteger ampliamente las instalaciones industriales contra los ciberataques internos y externos.

El sistema holístico de ciberseguridad, como el que plantea Siemens, no sólo es una necesidad, sino que también representa un enorme valor añadido: La protección contra los ataques hace que los productos y servicios sean más fiables, asegura la confianza de los clientes y mejora la competitividad. Los gastos en ciberseguridad son, por lo tanto, inversiones con repercusiones económicas positivas, no sólo para grandes empresas, también para las pequeñas y medianas.

La seguridad dentro de las industrias es clave para mantener los datos de su operación frente al incremento en la digitalización que estamos viviendo. Al haber una supervisión remota, existe una mayor vulnerabilidad de los sistemas frente a un posible ataque cibernético, por lo que un plan de ciberseguridad puede prevenir fallas en la producción y vacíos que ponga en riesgo la seguridad de todos los procesos operativos.

--o0o--

Siemens AG (Berlín y Múnich) es una potencia tecnológica mundial que ha sido sinónimo de excelencia en ingeniería, innovación, calidad y confianza a nivel mundial por más de 170 años. La empresa, con presencia en todo el mundo, se centra en la infraestructura inteligente para edificios, sistemas de energía distribuida y en la automatización y digitalización en las industrias de procesos y manufactura. Siemens reúne al mundo digital y físico para beneficiar a los clientes y a la sociedad. A través de Mobility, un proveedor líder de soluciones de movilidad inteligente para el transporte ferroviario y de transporte, Siemens está ayudando a dar forma al mercado mundial de servicios de pasajeros y mercancías. A través de su participación mayoritaria en la empresa Siemens Healthineers, que cotiza en bolsa, Siemens es también un proveedor líder mundial de tecnología médica y servicios digitales para el sector salud. Además, Siemens tiene una participación minoritaria en Siemens Energy, líder mundial en la transmisión y generación de energía eléctrica que cotiza en la bolsa desde el 28 de septiembre de 2020.

En el año fiscal 2019, que terminó el 30 de septiembre de 2019, el Grupo Siemens generó ingresos por 58,500 millones de euros e ingresos netos de 5,600 millones de euros. Al 30 de septiembre de 2019, la compañía contaba aproximadamente con 295, 000 empleados en todo el mundo sobre la base de las operaciones continuas. Puede obtenerse más información en Internet en www.siemens.com. En México Siemens inició sus operaciones en 1894 y desde entonces ha contribuido constantemente al desarrollo sostenible del país, aportando soluciones innovadoras. Con más de 125 años en el país, Siemens es un aliado estratégico de México. Para más información consulte la página de internet: https://new.siemens.com/mx/es.html