Grupo CMC aboga por abordar esta transformación desde la denominada resiliencia tecnológica durante un encuentro del Centro de Ciberseguridad Industrial (CCI)

El 90% de las empresas industriales aborda su conversión a Industria 4.0 sin la debida atención a la seguridad

Redacción Interempresas 21/05/2018

El 90% de las empresas del sector industrial está abordando su transformación hacia el nuevo entorno Industria 4.0 sin tener en cuenta el factor seguridad, lo que supone, a juicio de la consultora española Grupo CMC, un grave peligro, dado que los ciberataques a este tipo de entornos no dejan de crecer y sofisticarse.

De hecho, y según los datos que maneja **Grupo CMC**, el 69% de los responsables de seguridad de empresas industriales considera que las amenazas a los sistemas de control industrial (ICS por sus siglas en inglés), son elevadas y críticas.

La consultora española del entorno de las TI, Grupo CMC, ha alertado de esta realidad en el XXIV encuentro de 'La Voz de la Industria', organizado por el Centro de Ciberseguridad Industrial (**CCI**), y abogó por abordar esta transformación desde dos principios de base: la resiliencia tecnológica y la continuidad del negocio.

Según Emeterio Cuadrado, director de la unidad de Seguridad de Grupo CMC, "ante cualquier cambio y a diferencia del concepto de resistencia, la resiliencia tecnológica implica mutar en aras de la adaptación y eso es justamente lo que exige a las organizaciones industriales la transformación que implica entrar a jugar y asegurar su capacidad competitiva en la liga de la Industria 4.0".

Pedro Gallego, del Grupo CMC.

La visión de la protección de los entornos industriales de Grupo CMC abarca siete capas de protección: capa corporativa, capa de datos, capa de aplicación, capa de host, perímetro, capa de comunicaciones y capa física. Esta es la principal diferenciación frente a la mayoría de los proveedores de soluciones y servicios de este mercado.

De acuerdo con Grupo CMC, el cumplimiento de los estándares, la normativa y los procedimientos de actuación son la clave para garantizar que la capa corporativa es indemne a los ataques, mientras que la seguridad e integridad de los datos descansa en el cifrado y en asegurar la navegación segura.

La protección de la capa de aplicaciones empieza por la programación segura y el uso de servicios como ADAM (Active Directory Application Mode), junto con la ejecución controlada de actualizaciones y app, y la evitación de uso de aplicaciones configuradas con parámetros por defecto.

La seguridad de la capa host exige, por su parte, el uso avanzado del directorio cctivo, el establecimiento de roles de acceso, la restricción de privilegios, el bastionado de sistemas y el control USB; sin olvidar la ejecución de copias de seguridad, la actualización y el parcheo permanente de los sistemas operativos, y la implantación de un Sistema de Prevención de Intrusiones basado en el Host (HIPS), evitando igualmente el uso de parámetros por defecto.

En el perímetro, CMC aboga por el control de los accesos remotos, el uso de Sistemas de Control Industrial (ICS) con reglas de filtrado y el despliegue y aplicación de perfiles de seguridad y autenticación de usuarios remotos; en tanto que la seguridad a nivel de la capa de comunicaciones pasa, entre otras medidas, por la segmentación, el uso de listas de control de acceso (ACLs), la securización de MAC (Media Access Control) y de protocolos como ARP (Address Resolution Protocol) y DHCP (Dynamic Host Configuration Protocol). El uso de tarjetas inteligentes y sistemas biométricos se incluyen entre el abanico de medidas para la protección de la capa física.

Susana Sánchez y Antonio Navarrete, del Grupo CMC.

La capa de red es especialmente crítica y, de hecho, el 44% de los responsables de seguridad en empresas del sector industria considera que la integración de nuevos dispositivos sin capacidad de protección es el principal vector de amenaza a sus Sistemas de Control Industrial (ICS).

Según Carlos Navares, director de la unidad de Negocio IoT de Grupo CMC, "el concepto Industria 4.0 implica mucho más que una evolución de las plantas de fabricación con la integración de todo tipo de sensores y elementos IoT, exige ampliar la visión que la organización tiene de la ciberseguridad, así como capacitarse para hacer frente a los ciberataques y para minimizar, específicamente, su posible impacto en un entorno TI y TO convergente".

En el encuentro, los expertos de Grupo CMC incidieron específicamente en las implicaciones en cuanto a responsabilidad de los responsables de seguridad o CISO (por sus siglas en inglés) de empresas industriales que hacen uso de servicios Industria 4.0 desplegados en la nube. En este sentido, Grupo CMC se distingue por su capacidad para, a través de la integración de soluciones hardware y software, ofrecer protección en las cinco posibles capas de servicios en la nube, desde la protección frente a ataques DDoS en servicios delegados hasta la protección de appliances virtuales, pasando por la protección redes IP públicas (black listing), el aislamiento de redes virtuales y la virtualización de funciones de la red.