Las empresas industriales abordan su transformación sin pensar en la ciberseguridad

Transformación digital 16 MAY 2018

El concepto Industria 4.0 implica mucho más que una evolución de las plantas de fabricación con 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 minimizar su posible impacto en un entorno TI y TO.

Poco a poco, la industria 4.0 va ganando terreno, pero el 90% de las empresas del sector industrial está abordando su transformación hacia el nuevo entorno sin tener en cuenta el factor seguridad, lo que supone 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) son elevadas y críticas.

Ante esta realidad, Grupo CMC aboga 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".

De acuerdo con Grupo CMC, el cumplimiento de los estándares, la normativa y los procedimientos de actuación es 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. La seguridad de la capa host exige, por su parte, el uso avanzado del Directorio Activo, 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).

En el perímetro, CMC aboga por el control de los accesos remotos, el uso de 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 (ACL), la securización de MAC y de protocolos como ARP y DHCP. El uso de tarjetas inteligentes y sistemas biométricos se incluyen entre el abanico de medidas para la protección de la capa física.

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.

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".