Nº 81 febrero 2023

CLAVES DE LA SEGURIDAD ELECTRONICA

NUEVAS CLAVES EN LA SEGURIDAD ELECTRÓNICA

1. Combinación de Tendencias Tecnológicas en beneficio del negocio

La actual tendencia es el desafío de combinar ***"Tecnologías espaciales, tecnología limpia, Inteligencia Artificial y tecnologías de realidad inmersiva"*** para crear productos e iniciativas únicas que generen valor, no solo en el incremento de los niveles de seguridad sino en la utilización de la información generada para la toma de decisiones empresariales.

Esta evolución es bastante evidente en la **industria de la seguridad física** y su tendencia a la integración e implementación al unísono de la ciberseguridad y las tecnologías de privacidad de datos.

La **inteligencia artificial (IA) y la** combinación de aplicaciones basadas en la nube y configuradas en las instalaciones en campo están trabajando juntas para equilibrar la solución para el cliente y ofrecer un enfoque más escalable. Especialmente reseñable es el caso de la Videovigilancia, donde los avances en el procesamiento de imágenes, la integración del metadato y su gestión híbrida en servidores locales y servicios en la nube ha supuesto un importante avance en este sentido.

2. Punto de inflexión en la adopción de nuevas tecnologías

Muchos desarrollos tecnológicos revolucionarios, como el 5G, la IA y los servicios en la nube, permiten optimizar la aceleración y la automatización de las cargas de trabajo, y la administración de los recursos, mientras pueden llegar a ofrecer una excelente garantía de los servicios de seguridad.

Las nuevas tecnologías evolucionan rápidamente cada año y posteriormente permanecen estancadas debido a la mentalidad más tradicional del "si no está roto, no lo arregles" o del “si funciona, no lo toques”. Esta actitud especialmente latente en la industria de la seguridad física, ya precisó de muchos años para hacer la transición de una industria analógica a la digital. La transición hacia la seguridad cibernética y el puente entre las necesidades de ***OT (tecnología operativa) y los grupos de TI*** está suponiendo un gran esfuerzo de colaboración e interrelación entre el mundo físico y el lógico.

3. Creación del Entorno de Trabajo adecuado para los Ingenieros de Seguridad

Ante las actuales circunstancias VUCA (Volatilidad, Incertidumbre, Complejidad y Ambigüedad) y la falta de definición en la formación de los Ingenieros de Seguridad, la problemática fundamental radica, al igual que en el entorno de las tecnologías digitales, en la retención de talento en el sector y la promoción de iniciativas y actividades basadas en la excelencia en ingeniería y la competencia científica o tecnológica.

La industria de la seguridad física ahora se ve directamente afectada por tecnologías emergentes como la IA, la robótica y el análisis del dato, mucho más atractivas para la incorporación de un adecuado relevo generacional. Es imprescindible que las Empresas de Seguridad inviertan en el desarrollo individual de los ingenieros de seguridad e incorporen talento con capacidad multidisciplinar en las citadas tecnologías emergentes.

4. La innovación en la nube: proporcionar la inteligencia, seguridad y confiabilidad

El concepto de nube está comenzando a madurar en las grandes organizaciones y la escalabilidad se ha vuelto muy importante ya que la fuerza laboral de estas empresas ha crecido durante los últimos años. Pero la pandemia de COVID-19 también provocó que muchas empresas perdieran talento y encontraran formas de paliar la pérdida de su fuerza laboral a través de una estrategia en la nube.

La nube está cambiando la seguridad. La seguridad, en el contexto de esta tendencia, se refiere a la protección de los activos de información. Las preocupaciones de seguridad fueron la razón de la adopción lenta y el movimiento hacia la nube. Sin embargo, eso ha cambiado y ha dado paso a una nueva forma en que las organizaciones piensan sobre la seguridad de la información, una vez incluida en la gestión de riesgos corporativos.

ASPECTOS MÁS IMPORTANTES PARA PREVENIR LOS RIESGOS EN LA SEGURIDAD ELECTRONICA.

La industria de la seguridad electrónica tiene hoy en día como principal desafío la aplicación de los principios de ciberseguridad en sus sistemas de seguridad física, especialmente en sus dispositivos de perímetro como cámaras IP, sistemas de gestión de video, sistemas de control de acceso y en los de gestión del dato generado en los distintos subsistemas de detección de intrusión.

Muchos profesionales de la seguridad ignoraron los riesgos de ciberseguridad y afirmaron que sus sistemas no tenían conexión con el mundo exterior a través de Internet. Una vez que la responsabilidad y la rendición de cuentas en torno a las infracciones cibernéticas redefinieron la importancia de estos sistemas aislados separados, se abrió la puerta para que los servicios conectados, como la nube, desempeñen un papel más importante en la ampliación de las necesidades de seguridad y la gestión del sistema para los equipos de OT y TI.

La seguridad de la información y la protección de datos se han convertido en una prioridad para las empresas de seguridad electrónica en los últimos años.

Una mala gestión de contraseñas, el uso de herramientas de seguridad obsoletas o la falta de una estrategia robusta de protección de datos; son solo algunos de los elementos que pueden poner en grave riesgo un entorno de TI y sistemas seguridad electrónica.

Es correcto decir que un sistema electrónico de seguridad está expuesto a un riesgo cuando es vulnerable a ataques que pueden afectar a su:

- **Disponibilidad:** Cuando un sistema está expuesto a un ataque que puede interrumpir sus funciones normales, podemos afirmar que existe un verdadero riesgo dado que este debe considerarse como un subconjunto más de los sistemas de información y comunicación de una Empresa y su neutralización debería ser una preocupación importante para los equipos de TI.
- **Confidencialidad** Los sistemas de seguridad han facilitado exponencialmente el intercambio de datos entre individuos y sistemas. Esta capacidad tiene un lado muy práctico y positivo, pero para las empresas representa un factor de riesgo. Esto se debe principalmente al hecho de que muchos sistemas de seguridad gestionan grandes cantidades de datos confidenciales. Su divulgación a terceros puede tener consecuencias muy dañinas, por ejemplo, puede afectar la confiabilidad de la organización o incluso hacer que la empresa enfrente problemas legales.

- **Fiabilidad:** En los sistemas de seguridad electrónicos actuales la fiabilidad en su funcionamiento ya no es negociable, la generación de falsas alarmas o falsos positivos debe traducirse en tiempo real en un incremento del riesgo. Un sistema no solo debe ser eficaz sino fundamentalmente fiable y lo que detecte o genere, debe ser lo pretendido.
- **Integridad de la información proporcionada:** Los datos representan uno de los recursos más importantes que tienen las empresas, también los generados en los sistemas de seguridad electrónicos, y debe ser vital la importancia que merece los sistemas de respaldo de la información. Es necesario procedimentar de manera automatizada la creación de copias de seguridad que permitan restaurar información vital antes de que se vea comprometida.
- **Operatividad por el mal uso de los sistemas:** El mayor porcentaje de los incidentes de seguridad están relacionados con la actuación del usuario. Ya sea sin darse cuenta o intencionalmente, el riesgo es real. Esto significa que no es suficiente implementar una estrategia de control de privilegios en la operación, mantenimiento y administración de los sistemas tecnológicos de seguridad, también es necesario informar a los empleados sobre las mejores prácticas. De esta manera pueden estar más atentos para identificar y reportar cualquier irregularidad que puedan percibir.
- **Falta de actualizaciones periódicas:** La protección en tiempo real de todos los activos tecnológicos de seguridad requiere soluciones avanzadas con actualizaciones periódicas. Las Organizaciones que deciden utilizar herramientas gratuitas ponen en alto riesgo sus sistemas, ya que limitan la posibilidad de detectar de forma anticipada intrusiones de amenazas inesperadas. Las herramientas de pago ofrecen la última tecnología y agregan funcionalidades que van más allá de las soluciones tradicionales como la Monitorización del Comportamiento de los sistemas.

Julio Pérez Carreño es Secretario de la JD de AES, coordinador del área de trabajo de Seguridad Electrónica y Director de Operaciones de Eulen Seguridad.