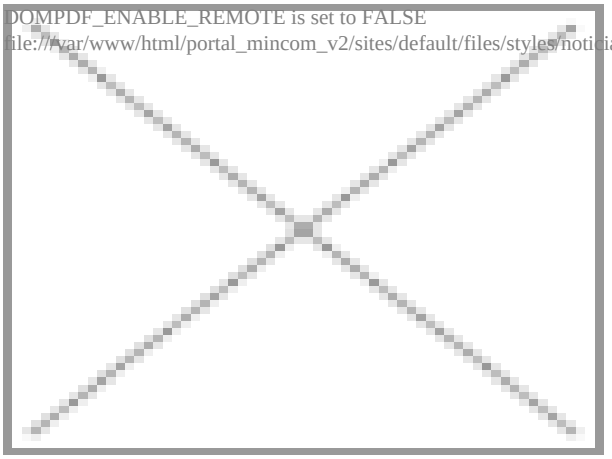

Source:
tynmagazine

Para lograr el desarrollo y avance tecnológico en 2021 en el sector de seguridad, es necesario mirar hacia atrás y hacer un análisis de todos los retos que afrontamos. La retrospectiva tiene la facultad de proporcionar un contexto para la toma de decisiones a futuro, lo cual nos ayudará a ser comprensibles y nos permitirá ser asertivos en cada paso que demos.

Si bien la pandemia por COVID-19 se había apoderado de Asia antes de finales de 2019, pocos habrían predicho el enorme impacto que tendría en todo el mundo a lo largo de 2020. En un corto periodo de tiempo, nuestra forma de vida, prácticas laborales y operaciones comerciales tuvieron que tomar un rumbo diferente. Las restricciones de viaje, las reglas de distanciamiento social, el aumento de los requisitos de higiene y la presión sobre los servicios de salud afectaron todos los negocios.

2020 fue un año que nos presentó constantes desafíos, tanto económicos como operacionales, donde tuvimos que buscar las mejores formas para garantizar la continuidad del negocio y procurar el bienestar de nuestro equipo de trabajo, sin embargo, también vimos surgir diversos casos de uso para nuestra tecnología y soluciones, además de nuevas formas de trabajo híbrido, ideas y formas de mantenernos unidos que nos abrieron una importante oportunidad en el mundo digital. No obstante, ante el panorama que vivimos, sabemos que los retos no se terminaron.

En Axis estamos conscientes de hoy más que nunca el avance tecnológico continúa y, como hemos visto en los últimos años, en lugar de presagiar la aparición de tecnologías completamente nuevas, las tendencias que vemos para 2021 están determinadas por el cómo y por qué se utilizan las tecnologías, además de las implicaciones asociadas a las soluciones de video.

1. La confianza como primera tendencia de seguridad

Anteriormente hemos hecho principal hincapié en que la confianza es uno de los ejes rectores del desarrollo tecnológico, en toda la cadena de suministros, pero hoy se ha vuelto aún más crítico este tema. Hay muchos factores que contribuyen a mantener la confianza bajo más escrutinio, ya que los clientes y usuarios finales exigen transparencia sobre cómo se utiliza la tecnología y cómo se gestionan los datos, que se almacenan en la vigilancia. Esto, junto con la necesidad de mantener la privacidad, será un desafío clave. Las discusiones renovadas sobre la confianza impactarán directamente en cómo las organizaciones de todos los sectores demuestran activamente por qué son confiables. Debido a su naturaleza, el sector de la seguridad se verá aún más forzado para redoblar sus esfuerzos en esta área y garantizar el correcto uso y desarrollo de la tecnología para brindar aún más seguridad y rendimiento.

2. El mundo se vuelve horizontal

En los últimos años se han visto aplicaciones y servicios diseñados en gran medida para entornos específicos, ya sea basados en servidores, en la nube o en el borde, todos impulsados por el deseo de lograr un rendimiento, escalabilidad y flexibilidad óptimos, junto con los beneficios de acceder y usar datos en cualquier momento y desde cualquier lugar.

Es así que 2021 verá un impulso hacia la integración horizontal entre entornos, pues se implementarán aplicaciones y servicios cada vez más inteligentes en las tres instancias (servidor, nube y borde) empleando las mejores capacidades de cada una, con el fin de mejorar el rendimiento y la eficiencia de las soluciones. Por ejemplo, el análisis de borde en una cámara de vigilancia potencialmente enviará un mensaje a un operador con una alerta, el operador luego accederá a la transmisión de video en vivo a través de una aplicación basada en la nube para verificar y responder. Este cambio a un enfoque horizontal aumentará la velocidad y precisión de la seguridad y la vigilancia, pasando de reactivo a proactivo, de manual a automatizado, al tiempo que reducirá el ancho de banda, energía y costos.

3. Ciberseguridad: la tendencia continúa

La tendencia anterior, está directamente relacionada con la seguridad cibernética, pues los servicios inteligentes demandarán una ciberseguridad sólida (una cadena, después de todo, es tan fuerte como su eslabón más débil) y la evolución constante del panorama de amenazas consolida su relevancia año tras año. Debido al potencial de altos rendimientos financieros y la interrupción de la infraestructura crítica, continuarán surgiendo nuevas capacidades, tácticas y amenazas que requerirán una vigilancia constante.

La inteligencia artificial será empleada por los ciberdelincuentes tanto como en cualquier sector, lo que fortalecerá su capacidad para encontrar y explotar vulnerabilidades. Las falsificaciones profundas se volverán aún más sofisticadas y realistas, lo que podría poner en duda la evidencia de videovigilancia. Como resultado, se requerirán más desarrollos en los métodos para verificar el contenido, los dispositivos y las aplicaciones a fin de mantener la confianza en su autenticidad. Los avances en el ciberdelito también se extenderán a métodos probados y verdaderos, como los señuelos de phishing, que serán más difíciles de detectar. Como resultado, los empleados serán aún más susceptibles a este tipo de ataques y, como siempre, se necesitará de educación constante y recordatorios de las mejores prácticas en ciberseguridad.

Por lo tanto, se acelerará el paso a redes de confianza cero, donde el perfil de seguridad para cada dispositivo y aplicación se evalúa de forma independiente. La confianza se entregará a través de la comunicación de dispositivo a dispositivo y / o aplicación a aplicación a través de firmware firmado, actualizaciones de software, arranque seguro, datos o video encriptados e identidad segura. Puede parecer una acusación de la época en la que vivimos, pero la única forma de confiar en la seguridad de cualquier cosa es no confiar en nada.

4. La realidad de la Inteligencia Artificial

Hemos estado hablando del concepto de Inteligencia Artificial (IA) durante tanto tiempo que algunos podrían cuestionar su validez como tendencia. Pero con el aprendizaje automático (ML) y el aprendizaje profundo (DL) ahora ampliamente disponibles en la tecnología de vigilancia, las implicaciones de su uso serán un factor en 2021. El desarrollo tecnológico nos ha permitido tener ejemplos concretos de varios casos de uso de la IA en la vigilancia, pero como hemos visto en otros sectores, el impacto positivo de la IA puede verse compensado por la atención que se presta a fallas específicas.

Las narrativas tienden a centrarse en los errores de la automatización, y sin duda este también será el caso en el sector de la vigilancia. Sin embargo, esto no debería actuar como un disuasivo y no debemos perder de vista los casos de uso potenciales positivos del aprendizaje automático y el aprendizaje profundo en la vigilancia. Por ejemplo, el uso de estas capacidades en dispositivos periféricos puede ayudar a identificar objetos y reducir las falsas alarmas. Como resultado, los expertos en seguridad pueden pasar a una forma de

trabajo proactiva y basada en eventos, en lugar de un monitoreo manual continuo.

5. Las tecnologías de bajo y sin contacto pasan a primer plano

Las regulaciones, reglas y hábitos de consumo establecidos durante este año se convertirán en algo común en 2021. La tecnología apoyará la forma en que la nueva dinámica social y normas de sanidad se monitorean y garantizan su cumplimiento. Como resultado, aumentará la implementación de tecnologías de contacto bajo o nulo, especialmente en áreas como el control de acceso. Además, las soluciones de vigilancia con capacidad de conteo de personas se convertirán en la norma para garantizar el cumplimiento de los protocolos de sanidad en todo el mundo.

6. Reinventando la sostenibilidad

Una preocupación durante la pandemia ha sido la reducción del enfoque en el medio ambiente y la sostenibilidad. Varios incidentes ambientales importantes han llevado estas discusiones a un primer plano, y se espera que en 2021 la sostenibilidad recupere su posición como un área de interés principal. En Axis somos conscientes de la relevancia que tomará este tema en el desarrollo de productos, por ello, los materiales utilizados en la producción y su duración siguen siendo dos de las áreas de mayor impacto.

Si bien se han dado pasos importantes para reducir el uso de plásticos y PVC en los productos y aumentar el nivel de uso de materiales reciclados, todos los fabricantes pueden seguir innovando para disminuir la huella de carbono. El periodo de vida de los productos también será un factor crítico para la toma de decisiones de los clientes, pues
es mucho mejor para el medio ambiente (y la economía) especificar un producto de alta calidad con una larga vida útil anticipada, que uno que requiere reemplazo después de unos pocos años.

La constante del cambio

Los eventos de 2020 demostraron por sí solos los riesgos que corremos al tratar de predecir qué sucederá el año siguiente y no tomar en cuenta las eventualidades. Sin embargo, estamos seguros que las tendencias descritas anteriormente son lo suficientemente amplias como para aplicarse incluso en el contexto de un entorno turbulento para dar respuesta a las necesidades de hoy y de mañana. Lo que seguirá siendo cierto es que los períodos de incertidumbre subrayan la importancia de la agilidad y un enfoque adaptable para la resolución de problemas, independientemente de lo que depare el futuro.

Disponible en:
https://www.tynmagazine.com/seis-tendencias-tecnologicas-que-afectaran-a... [1]

Links
[1] https://www.tynmagazine.com/seis-tendencias-tecnologicas-que-afectaran-al-sector-de-la-seguridad-en-2021/