**¿Hacia dónde deben mejorarse las medidas de seguridad actuales?**

En México, la iniciativa privada y los gobiernos locales han comenzado a trabajar en estrategias y soluciones para garantizar la protección de ciudades y disminuir los altos índices de delincuencia que prevalecen alrededor del país, aunado al incremento de ciberataques, extorsiones o robo de identidad que cada día son más frecuentes.

Actualmente las acciones que se implementan no prevén la vulnerabilidad en otros niveles, en el ciberespacio por ejemplo, en donde el sector financiero es el más propenso a sufrir múltiples ataques, principalmente porque continúan usando sistemas antiguos. Las repercusiones se reflejan en pérdidas financieras y en la reputación de las organizaciones atacadas.

Ante esta situación, el concepto de Estados Seguros e Inteligentes ha empezado a cobrar relevancia ya que busca proteger la integridad y derecho de los ciudadanos previniendo delitos a través de tres elementos: personal capacitado, tecnología adecuada y procedimientos definidos. Cualquier falla en la cadena podría permitir espacios vulnerables que podrían ser aprovechados por atacantes internos, externos, físicos y virtuales.

“Como empresa especializada en áreas como la seguridad, inteligencia y seguridad cibernética, desarrollamos diferentes herramientas a través de tecnología de punta y experiencia en el rubro. Ofrecemos a los Estados la certeza de que obtendrán un servicio de apoyo para la gestión de sus procesos de protección implementando una estrategia 360º que incluyan procesos, tecnología y capacitación especializada Se trata de un trabajo en conjunto, tanto con las autoridades como con la ciudadanía”, aseguró Javier Sánchez Serra, Director de Tecnología de Mer Group.

No es novedad que cada día los métodos de fraude cibernético van evolucionando, provocando pérdidas anuales de 100 mil millones de dólares, a nivel mundial. Tan sólo este año, los bancos mexicanos, a través de un ataque al Sistema de Pagos Electrónicos Interbancarios (SPEI) perdieron de 400 a 800 millones de pesos. Pero, ¿cómo lo lograron? Las autoridades no están seguras del origen del incidente, pues pudo haberse llevado a cabo desde el extranjero, pero pudo haberse dado por medio de perfiles usurpados de cuentahabientes de dichos bancos.

“La posibilidad de ser víctima de un delito cibernético o de un asalto en la vía pública es igual de alto con los niveles de criminalidad que prevalecen actualmente, lo que necesitamos hacer es implementar medidas que abarquen cualquier escenario con el fin de disminuir los riesgos considerablemente”, comentó Sánchez Serra.

La ciberseguridad y la inteligencia se unen para perfeccionar plataformas ya existentes. Un ejemplo de esto son las Patrullas Inteligentes; vehículos con sistemas de video móviles integrados para mejorar la labor en campo.

Por otra parte, se han desarrollado equipos habilitados para establecer una comunicación efectiva en caso de emergencia. A través de una red independiente, en donde no haya cobertura, las autoridades pueden conocer y compartir información relevante para ayudar en situaciones inesperadas, como desastres naturales.

Los avances tecnológicos traen consigo importantes beneficios en diferentes ámbitos, sin embargo, también conllevan retos para los gobiernos y la ciudadanía quienes deben actuar en conjunto para garantizar que los niveles de vulnerabilidad sean mínimos, ya sea las ciudades o de manera virtual en el ciberespacio.