Recomendaciones sobre la política

Prevención de la delincuencia informática moderna

La oportunidad

La combinación del mayor acceso a Internet, el explosivo aumento de los dispositivos conectados y la rápida expansión de los innovadores servicios basados en la nube está creando tremendas oportunidades económicas y sociales para los consumidores, gobiernos y empresas.

El desafío

Actualmente, los gobiernos tienen problemas para enfrentarse a la creciente amenaza, la sofisticación y la prevalencia de los delitos cibernéticos, incluyendo: robo de identidad; fraude en línea; esquemas de distribución de malware; ataques contra la integridad de datos y sistemas; y la distribución en línea de contenidos ilegales.

Cada vez más, estos delitos son cometidos por grupos organizados que operan en un país, pero atacan a víctimas en otro. La naturaleza transfronteriza de los delitos cibernéticos complica la aplicación de la ley, y los marcos legales inadecuados en algunos países han creado refugios seguros para los delincuentes cibernéticos.

El impacto financiero de todos estos delitos cibernéticos es enorme, y está creciendo. En 2015, la compañía de seguros británica Lloyd, estimó que los ciber ataques cuestan a las empresas la friolera de 400 mil millones de dólares USD al año, una cantidad que se espera que aumente en los próximos años.

Además de estos costes económicos, existen impactos menos tangibles, incluyendo la pérdida de confianza en el comercio electrónico, la erosión de la privacidad individual y la disminución de la confianza en los servicios en línea.

Cada uno de estos efectos amenaza con ralentizar la adopción de la innovación basada en la nube y reduce los beneficios de las prometedoras nuevas tecnologías.

Recomendaciones sobre la política

Es esencial la armonización de las leyes contra los delitos informáticos en todo el mundo combinadas con iniciativas para facilitar la coordinación más rápida y efectiva entre las fuerzas del orden. Estos esfuerzos pueden llevarse a cabo en un entorno donde cada país respete la soberanía de otras naciones, y donde se respeten plenamente los derechos fundamentales y las libertades de los ciudadanos. Para reforzar la aplicación de forma equilibrada, los gobiernos deben considerar los siguientes pasos:

Una aplicación estricta y normas equilibradas. Para luchar contra la ciberdelincuencia de forma efectiva, aplicación de la ley y la industria deben tener las herramientas legales necesarias para perseguir delincuentes, estén donde estén. Los gobiernos deben trabajar para actualizar su derecho penal de forma que sean capaces de dar respuesta a las amenazas nuevas y existentes que plantean los delincuentes informáticos. Al mismo tiempo, estas leyes deben ser conscientes para que no afecten negativamente a la innovación o la adopción de nuevas tecnologías. También deberían dar soporte a los esfuerzos de auto regulación de la industria.

Adoptar leyes que sean consistentes con las convenciones internacionales ampliamente aceptadas. La Convención de Budapest del Consejo de Europa proporciona un buen modelo para la legislación de los delitos informáticos que puede ayudar a armonizar las leyes e impulsar una mejor cooperación entre fronteras. Esta coordinación y cooperación internacional ayudarán a eliminar los refugios para los delincuentes, y a reducir al mínimo los riesgos que surgen cuando los intermediarios y otras partes inocentes están sujetos a obligaciones o responsabilidades en conflicto.

Facilitar el intercambio de información. En algunos casos, las empresas con información sobre delitos en línea

se enfrentan a una posible responsabilidad en virtud de la privacidad, la protección de datos y otras leyes si comparten voluntariamente esa información con las fuerzas de seguridad.

Para facilitar y animar una cooperación puntual y oportuna, los gobiernos deberían aclarar las reglas para el intercambio de datos por parte de las empresas con las fuerzas de seguridad. La falta de claridad sobre las reglas para el intercambio de información y los riesgos de responsabilidad civil pueden impedir que las empresas trabajen con las fuerzas del orden, incluso cuando la cooperación podría ser fundamental para prevenir o reaccionar a la ciberdelincuencia. Además, como se describe en las recomendaciones para el acceso del gobierno a los datos, mejorar los procedimientos y mecanismos de cooperación internacional y transfronteriza mediante la modernización de los procesos de asistencia judicial recíproca ayudarán a simplificar los esfuerzos de aplicación y a clarificar las cuestiones importantes relativas a la competencia y el acceso a las pruebas.

Desarrollar nuevas formas de prevenir el crimen cibernético. Los esfuerzos actuales para hacer cumplir las leyes en la materia son inadecuados dada la enormidad del problema. Se necesitan nuevos enfoques para perseguir a los delincuentes. Un ejemplo puede ser un programa piloto lanzado por la policía de la Ciudad de Londres en asociación con bufetes de abogados privados que utilizan los tribunales civiles para embargar los activos de los delincuentes informáticos. Será fundamental encontrar otras formas de aumentar los esfuerzos de aplicación de las leyes.

Trabajar con la industria sobre las mejores prácticas y nuevas cuestiones. Los gobiernos pueden aprovechar la ventaja de la experiencia y los recursos del sector privado en la lucha contra los delitos cibernéticos.

Las oportunidades incluyen trabajar con la industria para formar a los agentes policiales sobre las amenazas nuevas y emergentes que los proveedores de tecnología sufren en el mundo real y que sus clientes ven como prioridades. Los gobiernos a menudo carecen de recursos suficientes para hacer frente con eficacia a los delitos cibernéticos. Trabajar con el sector privado puede ayudarles a conseguir un mayor éxito, que ayudará a fomentar la confianza en la informática en línea.