¿Las estrategias nacionales de ciberseguridad deberían de tener un enfoque civil?

El centro de investigación y desarrollo enfatizó que, si bien la ciberseguridad incluye aspectos de seguridad nacional, debe ser concebida como una preocupación de toda la sociedad y el gobierno en su conjunto, por lo que debería contar con un liderazgo civil.

El desarrollo de una estrategia nacional de ciberseguridad es una necesidad y no una opción para los países. Estas estrategias deben contar con una Oficina Nacional de Coordinación Cibernética, la cual es recomendable que tenga un enfoque civil y no militar, de acuerdo con Cynthia Wright, directora de Ciberestrategia y Política de MITRE.

“Lo que recomendamos es que tengan un enfoque civil. Creemos firmemente que mientras que la milicia y el cumplimiento de la ley tienen un papel en la ciberseguridad nacional, las tecnologías cibernéticas y la ciberseguridad tienen efectos enormes en la economía civil, el gobierno, el ecosistema de inversión, la habilidad de los negocios para competir y el bienestar de los ciudadanos, por lo que fundamentalmente la ciberseguridad es una preocupación civil”, dijo.

Durante la quinta edición del Simposio de Ciberseguridad de la Organización de Estados Americanos (OEA), la investigadora enfatizó que, si bien la ciberseguridad incluye aspectos de seguridad nacional, debe ser concebida como una preocupación de toda la sociedad y el gobierno en su conjunto, por lo que debería contar con un liderazgo civil. El enfoque de MITRE ha sido generado a partir de la relación de este centro con los gobiernos de más de 70 países.

En México, aunque la administración de Enrique Peña Nieto publicó una estrategia nacional de ciberseguridad en 2017, esta tenía su liderazgo en una subdirección de la Secretaría de Gobernación. En la actualidad, bajo la presidencia de Andrés Manuel López Obrador, la Secretaría de Marina publicó su propia Estrategia de Ciberseguridad, mientras que la Secretaría de la Defensa Nacional (Sedena) y el Centro de Respuesta a Incidentes de la Guardia Nacional (CSIRT-MX) han publicado algunos manuales orientados a mejores prácticas de ciberseguridad dentro del sector privado.

De acuerdo con Wright, una estrategia nacional de ciberseguridad sirve para alinear las capacidades organizacionales con las metas y procesos de los gobiernos en materia de ciberseguridad, sobre todo en lo que toca a la protección de infraestructuras y servicios críticos.

“Una estrategia nacional de ciberseguridad es muy importante. Primero porque involucra a todos los interesados (gobierno, industria, academia y sociedad civil) en torno a un contexto nacional específico, para que puedan considerar lo que su país necesita en términos de ciberseguridad. Y luego comunicar esas necesidades a la sociedad”, dijo la investigadora y añadió que cada país enfrenta diferentes riesgos en materia de ciberseguridad, que pueden ser la amenaza de otro estado nación, del cibercrimen o de perder oportunidades para mejorar sus economías.

Instituciones financieras, las más afectadas

De acuerdo con la directora de Ciberestrategia y Política de MITRE, las instituciones que tradicionalmente han sido las más afectadas son las financieras, debido a que son las que concentran los recursos económicos.

No obstante, a partir del comienzo de la pandemia de Covid-19, otras entidades como los hospitales y las instituciones educativas también se convirtieron en objetivos de los cibercriminales, principalmente porque son organizaciones que no pueden perder la información de sus clientes.

"Cualquier tipo de entidad que tiene una necesidad urgente de recuperar su información, como los hospitales y las escuelas, son buenos objetivos para los cibercriminales, porque no pueden costear el tomar las otras alternativas a pagar el rescate por su información", dijo.

Se han contabilizado 60,800 millones de intentos de ciberataques en contra de individuos, instituciones y compañías mexicanas. La principal amenaza de ciberseguridad sigue siendo el ransomware o secuestro de información, cuya actividad mostró un crecimiento de 10 veces en el año más reciente.

Por lo que, de acuerdo con el marco desarrollado por MITRE, además de una Oficina Nacional de Coordinación Cibernética, es preciso que además de una Oficina Nacional de Coordinación Cibernética, es preciso que exista un Centro de Respuesta Incidentes (CSIRT) de alcance nacional junto con centros de respuesta que atiendan a sectores críticos, como el financiero, de telecomunicaciones y de infraestructuras críticas.

Estos centros, junto con las entidades reguladoras encargadas de supervisar las infraestructuras y los servicios críticos; además de los cuerpos de policía, los miembros del Poder Judicial, el ejército y las agencias de inteligencia deben contar con responsabilidades específicas en materia de ciberseguridad que tienen que estar asentadas en un marco legal que es la propia estrategia nacional de ciberseguridad.

Algunas de estas responsabilidades, de acuerdo con Wright, incluyen el contar con expectativas claras, límites y mecanismos de transparencia y supervisión robustos; criterios para identificar infraestructuras críticas, como son las plantas de producción de energía o las centrales de telecomunicaciones; requerimientos de protección de datos tanto para las instituciones gubernamentales, como para las empresas y la sociedad en general; así como requerimientos de notificación de incidentes.

> "La forma de evaluar la efectividad de una estrategia de ciberseguridad tiene que ser desarrollada dentro de la misma estrategia y eso está basado en la efectividad de tus procesos de gobernanza: debes tener una forma de reunir a todos los participantes de la estrategia y observar juntos tanto las metas como las métricas establecidas para medir su avance".

Autor: Rodrigo Riquelme

Fuente de información: www.eleconomista.com.mx