LA RECETA

Para contrarrestar estas crecientes amenazas cibernéticas, los gobiernos latinoamericanos, con el apoyo del gobierno de Estados Unidos y el Comando Sur de ese país, deberían:

1.- Implementar estrategias de ciberseguridad.

2.- Fortalecer la cooperación internacional en materia de ciberseguridad.

3.- Invertir en infraestructura crítica de ciberseguridad.

4.- Capacitación periódica en ciberseguridad para todo el personal.

5.- Establecer equipos de respuesta a incidentes de seguridad informática.

6.- Desarrollar políticas de respuesta claras y eficaces frente al ransomware.

7.- Promulgar y hacer cumplir leyes eficaces contra el ransomware y el hacktivismo.

LA AMENAZA DEL RANSOMWARE

#Ciberseguridad

POR RUBÉN ZERMEÑO
@RubenZermeno

Muchas veces las amenazas contra la estabilidad de un país, son invisibles. Se trata de grupos organizados que utilizan como armas una computadora e internet para vulnerar, secuestrar y/o compartir información valiosa de un gobierno.

A pesar de que la amenaza crece en todo el mundo, Latinoamérica y en México poco se está haciendo para frenar a las pandillas de ransomware y a grupos de hacktivistas.

"Las interrupciones operativas causadas por los ataques de ransomware son graves. Al cifrar datos críticos y exigir rescates para liberarlos, estas organizaciones pueden paralizar servicios esenciales, desde la atención médica hasta la administración pública.

"Esta interrupción no solo afecta a las entidades atacadas, sino que también tiene un impacto negativo en la población que depende de estos servicios", concluye la investigación "Pandillas de ransomware y hacktivistas, amenazas cibernéticas a los gobiernos de América Latina", publicada por el Instituto Jack D. Gordon de Políticas Públicas y elaborada por Juan Manuel Aguilar Antonio, investigador postdoctoral del Centro de Investigaciones sobre América del Norte de la Universidad Nacional Autónoma de México.

Durante la pasada administración, varias dependencias del Gobierno federal fueron víctimas de ciberataques, de secuestro y de robo de información, sin que hubiera responsables ni detenidos.

Por ejemplo, el Servicio de Administración Tributaria (SAT) recibió más ataques que en otros sexenios, la Comisión Federal de Electricidad (CFE) y Petróleos Mexicanos (Pemex) también fueron vulnerados.

El golpe más sonado fue el robo de miles de documentos clasificados y otra información a la Secretaría de Defensa Nacional (Sedena) por el grupo Guacamaya Leaks.

México es el segundo país de América Latina que recibe más ataques de ransomware con el 12 por ciento del total de la región. En promedio, nuestro país recibe alrededor de un millón de ataques de ese tipo al mes

En noviembre de 2019, Pemex fue objeto de un ataque con ransomware del grupo DoppelPaymer. Para liberar la información secuestrada, la organización exigió al Gobierno federal un rescate de 565 bitcoins, alrededor de 777 millones de pesos en la actualidad.

El Gobierno federal informó que no pagaría nada y aseguró que el ataque había sido neutralizado rápidamente afectando a no más del 5 por ciento de sus redes.

Meses después, la Auditoría Superior de la Federación publicó la evaluación al ciberataque y concluyó que no fue cualquier cosa, ya que "piratas informáticos" habían ingresado por lo menos a mil 816 computadoras de la empresa productiva del Estado.

Especialistas, organizaciones y empresas de ciberseguridad dudaron que Pemex no hubiera pagado el rescate de la información.

"Es de suponer que Pemex pagó, pero los representantes de la empresa aún esquivan preguntas sobre el tema", opinó al respecto Banamerica.

Sobre esta situación, la investigación de Aguilar Antonio revela que los costos económicos asociados con los ataques de ransomware son enormes.

"Más allá del rescate exigido, las organizaciones afectadas enfrentan costos de recuperación significativos, que incluyen la restauración del sistema, la implementación de medidas de seguridad adicionales y la compensación por pérdidas operativas".

Pandillas de ransomware y hacktivistas amenazan a México y a América Latina, cobrando rescate por la información robada e incluso paralizando servicios esenciales de la administración pública

Una radiografía del delito

Otras de las afectaciones de estos ciberataques es la vulneración a información sensible tanto de las autoridades como información personal.

"Los grupos de ransomware y hacktivistas como Guacamaya extraen y publican grandes volúmenes de datos confidenciales y sensibles que pueden incluir información personal, secretos de Estado y detalles sobre operaciones de seguridad. La

Las interrupciones operativas causadas por los ataques de ransomware son graves. Al cifrar datos críticos y exigir rescates para liberarlos, estas organizaciones pueden paralizar servicios esenciales, desde la atención médica hasta la administración pública"

Juan Manuel Aguilar Antonio
Investigador postdoctoral del Centro de Investigaciones sobre América del Norte

exposición de esta información socava la confianza pública en las instituciones gubernamentales y puede comprometer la seguridad nacional.

"De manera similar al contexto de seguridad pública, en el que las organizaciones criminales transnacionales explotan las debilidades institucionales de los gobiernos de América Latina para llevar a cabo sus operaciones, las bandas de ransomware y los grupos hacktivistas explotan las débiles capacidades cibernéticas y los marcos legales ineficaces para atacar a países de la región", agrega la investigación.

En el caso de México, es el segundo país de América Latina que recibe más ataques, con el 12 por ciento del total de la región. En promedio, nuestro país recibe alrededor de un millón de ataques con ransomware al mes.

El costo de este tipo de ataques en América Latina se prevé que supere los 90 millones de dólares en 2025, es decir, a nuestro país le costaría al menos 200 millones de pesos este tipo de amenazas.

"Esto se debe a que los países de la región presentan deficiencias significativas en el desarrollo de una política nacional de ciberseguridad, que es crucial para abordar los riesgos y amenazas del ciberespacio que afectan la seguridad gubernamental.

La falta de una estrategia coherente en toda la región ha exacerbado estos desafíos, lo que ha llevado a la categorización de América Latina como una "zona gris" en materia de ciberseguridad global", dice la investigación.

Entre los grupos que estarían operando y atacando cibernéticamente en la región y con total impunidad los principales serían ALPHV/ BlackCat, LockBit 2.0, BlackByte, BlackHunt y Conti, así como el grupo hacktivista Guacamaya.

ARTE: REPORTE INDIGO STAFF