



Foto: Freepik

TRAS HACKEO A SEDENA

Urgen por mayor ciberseguridad

Daniel Rojas, director de Marketing para América Latina de BlueVoyant, explicó que, tras el ataque del grupo Guacamaya a la Secretaría de la Defensa Nacional (Sedena), es necesario que el gobierno mexicano empiece a tomar acciones para aumentar todos los niveles de seguridad en todas las entidades, lo que significa la integración de más talento y tecnología. :

LEY DE CIBERSEGURIDAD NO SERA LA PANACEA

SE DEBEN MEJORAR LOS SISTEMAS DE SEGURIDAD

POR AURA HERNÁNDEZ
aura.hernandez@glmm.com.mx

Tras el ataque del grupo Guacamaya a la Secretaría de la Defensa Nacional (Sedena) es necesario que el gobierno mexicano empiece a tomar acciones para aumentar todos los niveles de seguridad en todas las entidades, lo que significa la integración de más talento y tecnología.

Daniel Rojas, director de marketing para América La-



tina de BlueVoyant, recordó que en los últimos meses se ha visto un aumento en los ciberataques a gobiernos de América Latina, aunque no es un fenómeno exclusivo de la región.

“Se debe a una tendencia mundial producto de la combinación de nuevas formas de ataque, vulnerabilidades aprovechadas por parte de los delincuentes y el efecto de una mayor virtualización debido a la pandemia”, explicó al platicar con **Excelsior**.

Los cibercriminales tienen en la mira a varios gobiernos latinoamericanos y muestra de ello son víctimas recientes como el gobierno de Costa Rica, que vio vulnerados varios de sus organismos, la Secretaría de Estado de Finanzas de Río de Janeiro y la Agencia de Inteligencia de Perú.

Luis Corrons, experto en seguridad de Avast, agregó que los piratas informáticos realizan estos ataques porque buscan un beneficio económico o, bien, se trata de agentes pagados por otros estados que buscan información.

“Los atacantes sólo necesitan un único punto de entrada para empezar, normalmente lo hacen a través de sistemas anticuados, mal configurados o con técnicas de suplantación de identidad (phishing) e Ingeniería social”, detalló.

SOBRE EL GRUPO GUACAMAYA:

- El pasado 19 de septiembre, el grupo adelantó que como parte de su Operación Fuerzas Represivas llevarían a cabo filtraciones en Perú,

Salvador, Chile y Colombia, además de México.

- El pasado 6 de marzo el grupo hackeó los sistemas de comunicación del Proyecto Minero Fénix, de la Compañía Guatemalteca Niquel y de Pronico, del conglomerado minero Solway Group.
- El pasado 7 de agosto filtró los documentos de empresas mineras y petroleras de Chile, Ecuador, Colombia y Venezuela.
- El sitio DdoSecrets.com dijo que Guacamaya habría filtrado más de 1 TB de mails de compañías mineras y petroleras.

VÍCTIMAS DE CIBERATAQUES

- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.
- Servicio de Administración Tributaria.
- Banco de México.
- Petróleos Mexicanos.
- Secretaría de Economía.
- Secretaría de la Función Pública.
- Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado.
- Lotería Nacional.
- Instituto Nacional de Migración.
- Plataforma Nacional de Transparencia.

LA ESTRATEGIA

El especialista de Avast Luis Corrons consideró que este tipo de ataques deben tener una respuesta muy puntual, es decir, tan pronto como se identifique la

brecha, hay que aislar los sistemas afectados y realizar un análisis forense para identificar cómo entraron en la red y qué acciones hicieron los atacantes.

Al mismo tiempo, tienen que coordinarse con las fuerzas de seguridad para identificar y perseguir a los autores, así como con la policía cibernética nacional para identificar a otras víctimas, si es que las hay, que podrían haber sido objetivo de los mismos atacantes y para permitir la aplicación de las defensas en otras áreas con la inteligencia recogida.

El director de marketing para América Latina de BlueVoyant Daniel Rojas añadió que se necesitan medidas de contención a corto y largo plazo.

Por ejemplo, los organismos vulnerados necesitan evaluar su ciberseguridad y ciberhigiene, es decir, incluir buenas prácticas como la autenticación multifactor, la capacitación en phishing en todos los niveles de las organizaciones, estudiar y limitar los privilegios de acceso a información sensible y confidencial, así como monitorear constantemente a terceros en la cadena de suministros.

MÁS TALENTO

Para Hiram Alejandro Camarillo, director de información de Seekurity, más que enfocarse en aprobar una Ley de Ciberseguridad, algo que ya está preparando el Congreso de la Unión debido al hackeo de la Sedena, el gobierno debe contar con talento calificado.

“Algo que se tiene que empezar a hacer dentro del gobierno, y que no hemos visto que se realice, es empezar a trabajar e implementar la seguridad técnica”, resaltó también al

platicar con **Excelsior**.

El experto destacó que lo más importante es que se cuente con el personal adecuado para saber cómo proteger y actuar en caso de que se detecte algún incidente, que realmente pueda monitorear y proteger los sistemas.



Éste no es el primero, aunque sí el más reciente ataque a un gobierno en América Latina.”

LUIS CORRONS


EXPERTO EN SEGURIDAD DE AVAST



En los últimos años nos ha demostrado (el gobierno) que no se hace absolutamente nada para proteger toda esta información.”

HIRAM ALEJANDRO CAMARILLO

DIRECTOR DE INFORMACIÓN DE SEEKURITY



Las primeras horas de un ataque son cruciales, se requiere un diagnóstico inmediato de la vulnerabilidad, el dimensionamiento de las consecuencias y la remediación correspondiente, verificando y fortaleciendo su postura de ciberseguridad y ciberhigiene.”

DANIEL ROJAS
DIRECTOR DE MARKETING
PARA AMÉRICA LATINA DE
BLUEVOYANT

