LA INFORMACIÓN "HACKEADA" AHORA PUEDE SER MANIPULADA, ALERTA EXPERTO

DIANA LASTIRI

Los documentos de la Sedena que fueron *hackeados* y publicados por el colectivo Guacamaya fácilmente pueden ser alterados por el simple hecho de permanecer en internet; además, al conocer tan poco sobre quién está detrás de esta vulneración, México debe estar atento a la posibilidad de que se trate de una intervención extranjera.

Así lo advierte Luis Miguel Dena Escalera, CEO de Cyber Black y especialista en seguridad cibernética. En entrevista con **Proceso** también consideró que la vulneración a la Sedena y a la seguridad de otros cuatro países latinoamericanos (Perú, El Salvador, Colombia y Chile) es el escenario más catastrófico que la comunidad internacional ha temido desde 1999, cuando se popularizó internet.

El *hackeo* del colectivo Guacamaya mantiene en la red más de cuatro millones 144 mil correos electrónicos internos y externos de la Sedena, enviados entre enero de 2010 y hasta el 3 de septiembre último, y aunque el grupo que se atribuyó el ataque cibernético ha afirmado que sólo comparten la totalidad de la información con periodistas, investigadores y defensores de derechos humanos, Dena Escalera asegura que los *hackers* ya no tienen el control sobre la información que robaron, lo que abre la puerta al riesgo de que esos datos puedan ser manipulados.

El problema de ello, explicó, es que se generó un proceso de aceptación de todos los datos robados después de que el presidente Andrés Manuel López Obrador confirmó la veracidad de la información *hackeada* sobre su estado de salud.

Pese a que se sabe poco sobre la identidad del colectivo de ciberatacantes, cabe la posibilidad de que se trate de una intervención extranjera en la seguridad de México, así como en los demás países vulnerados que, por cierto, todos son de alineación política izquierdista, destaca.

"Cómo lograron penetrar hacia la información de cinco países, cómo están esos países en el índice global de dimensión de ciberseguridad... Que nosotros estemos en el lugar 84 u 85, y Chile en el lugar 59 y fue vulnerado quiere decir que también otras potencias como China, Rusia, EU e India podrán seguir vulnerando a otros países que no son tan fuertes en el tema cibernético.

"Simplemente es una hipótesis no descabellada: pones una pantalla de guacamaya o de loro para hacer una distribución no controlada de la información. Una vez que está en el ciberespacio, si ellos pudieron *hackear* a la Sedena, otros podrán *hackear* a Guacamaya y eso hace que sea vulnerable en el ciberespacio toda esa cantidad de información".


Index of /sedena

Name	Last modified	Size	Description
Parent Directory		-	
03.-RESUMEN DE NOVED..>	2022-09-19 17:28	212K	
03.-RESUMEN DE NOVED..>	2022-09-19 17:28	206K	
0687 6 MAR. 2022 CON..>	2022-09-17 17:16	223K	
6 FEB. 2022 SEGUIMIE..>	2022-09-17 17:34	95K	
7 JUN. 2022 AMPLIACI..>	2022-09-17 14:22	88K	
17ZM_SERGIO JERONIMO..>	2022-09-17 16:13	2.9M	
23 NOVIEMBRE 2021 SE..>	2022-09-17 17:27	95K	
867 EZLN.docx	2022-09-17 16:59	213K	
1046 VISITA.docx	2022-09-17 15:33	241K	
20220805192536564.pdf	2022-09-17 16:30	474K	
ANEXO FCA 1145 2 Mar..>	2022-09-17 16:11	9.1M	
Campos del Poder Ago..>	2022-08-29 11:02	13M	
DIYA 1 MAR. 2016.pdf	2022-10-01 19:10	1.4M	
DIYA 24 FEB. 2016.pdf	2022-09-17 11:44	1.7M	
DIYA 29 DIC. 2015.pdf	2022-09-17 16:01	1.7M	
DIYA 29 FEB. 2016.pdf	2022-10-01 19:09	1.5M	
DR. LUMBRERAS ACTIVI..>	2022-08-29 11:28	2.3M	
DR. LUMBRERAS EZLN_T..>	2022-08-29 11:28	1.1M	
ES-249 25 Ago 2021 M..>	2022-09-17 15:47	847K	
ES-254 28 Ago 2021 A..>	2022-09-17 15:47	4.3M	
ES-256 31 Ago 2021 A..>	2022-09-17 16:55	2.6M	
EZLN.docx	2022-08-29 11:25	23K	
EZLN_2.docx	2022-08-29 11:25	69K	
Eventos Sociales.pptx	2022-07-01 15:30	1.6M	
LIDERES SOCIALES.pptx	2022-06-30 14:23	2.4M	

Algunos de los archivos militares robados.

Riesgo en el internet de las cosas

Dena Escalera comentó que México está en vías de consolidar la estructura 5G y millones de ciudadanos utilizan dispositivos IOT (Internet de las cosas), que son susceptibles de *hackeo* porque no tienen *softwares* actualizados y los fabricantes no son responsables de la vulneración de los datos sensibles de sus usuarios, más que con normas internacionales, pues México carece de una legislación interna que ayude a sancionar este tipo de interferencias.

Por ello, dijo que México debe dar continuidad a los esfuerzos iniciados a escala mundial desde 1999 en acciones de ciberseguridad, para evitar que ocurra otro *hackeo* de este nivel, pues siempre habrá una brecha entre las medidas de protección y las amenazas cibernéticas que son cada vez más complejas.

Riesgo de más ataques

En su informe sobre la revisión de la Cuenta Pública 2020, la Auditoría Superior de la Federación advirtió que de 2013 a 2019 no hubo una fiscalización a la Sedena en el área de tecnologías de la información, y encontró deficiencias en los controles de ciberdefensa que ocasionaron pérdidas para el erario, lo que para Dena pudo ser la puerta de entrada al *hackeo* de Guacamaya.

"Si la Presidencia de la República, si el Gabinete de Seguridad Nacional, el económico y social no comprenden que requerimos de herramientas y un ecosistema de ciberseguridad, estaremos en un grave problema para poder seguir en este mundo digital que ya es mucho más complejo, evolutivo, sofisticado y de largo alcance", advierte el especialista.

Para el CEO de Cyber Black, lo ocurrido en la Sedena puede ser tomado como una invitación a que cualquiera intente *hackear* otras instituciones mexicanas. Así, alertó sobre la posibilidad de que existan más ciberataques.

"Hoy gana la movilidad social, la rebelión, los terceros interesados, la inestabilidad y el conflicto (...) y no tenemos una estrategia nacional de ciberseguridad que esté a la altura de estos incidentes", agregó. ●