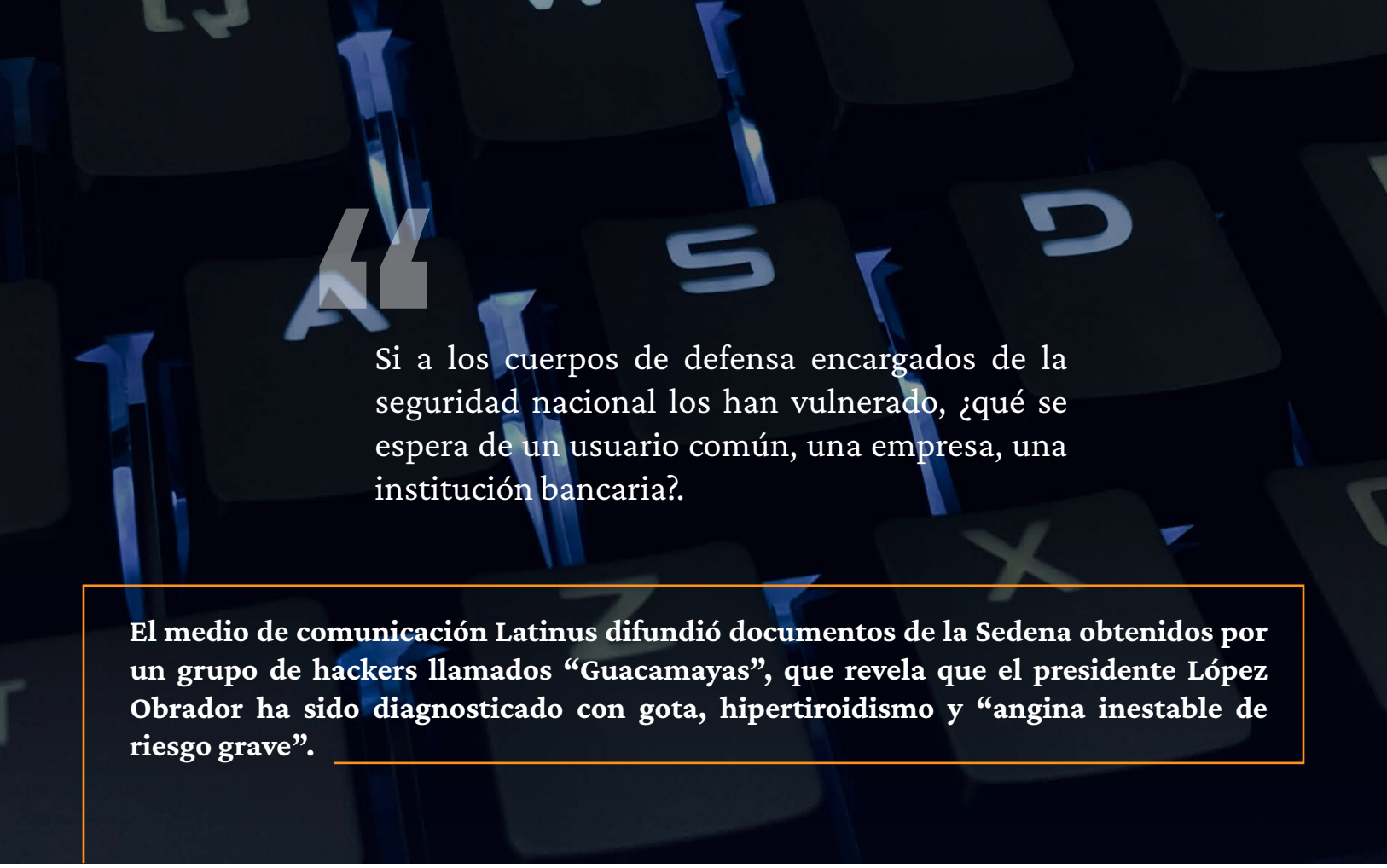
Las lecciones que comienzan con el hackeo a la Sedena

mexis aggity



> Si a los cuerpos de defensa encargados de la seguridad nacional los han vulnerado, ¿qué se espera de un usuario común, una empresa, una institución bancaria?.

El medio de comunicación Latinus difundió documentos de la Sedena obtenidos por un grupo de hackers llamados "Guacamayas", que revela que el presidente López Obrador ha sido diagnosticado con gota, hipertiroidismo y "angina inestable de riesgo grave".

(Expansión) - Hace unas semanas me encontré con material sobre un grupo hacktivista llamado #Guacamaya, el cual ha logrado obtener información de fuerzas armadas de distintos países latinoamericanos; entre la información me encontré temas relacionados con la Secretaría de la Defensa Nacional (Sedena), sin embargo, por otros temas no tomé mayor atención sino hasta el día 29 de septiembre.

El periodista Carlos Loret de Mola reveló información confidencial encontrada en esos leaks de Guacamaya . Desde mi trinchera he logrado comprobar algunas de las cosas contenidas, sin embargo, analizar 6tb de textos es una tarea titánica.

Las lecciones que comienzan para crear capacidades internas mayores en sentido de ciberseguridad son varias y empezarán a emerger en los días venideros. Primero debemos hacer especial énfasis en que, si a los cuerpos de defensa encargados de la seguridad nacional los han vulnerado, ¿qué se espera de un usuario común, una empresa, una institución bancaria? Quizá la más nula e inexistente conciencia de ciberseguridad y el valor de su información.

No es lo mismo hablar de ciberseguridad en una escala empresarial -donde hay lineamientos, directrices, políticas, y ejemplos de recuperación post incidentes-, que hablar de una vulneración escala seguridad nacional; aquí no se permite siquiera el hecho de hacer un contraste o comparación, eso simplemente denotaría la inexperta de una opinión vertida. La seguridad nacional en materia de ciberseguridad funciona de manera distinta, con matices de impacto mayores y daños muchas veces irreparables.

Se habla de que a raíz del golpe digital a la Sedena, se requiere dar impulso a la iniciativa del "Centro Nacional de Seguridad Cibernética", la cual ya ha tenido un avance; sin embargo, estamos lejos de poder hablar de una entidad así, pues para hablar de infraestructura se requiere presupuesto e inversión, no austeridad.

Para hablar de legislación, se requiere política pública, no dejar en el olvido lo que se ha construido en años anteriores como la Estrategia Nacional de Ciberseguridad, en la cual colaboró directamente la OEA para fortalecer las capacidades de ciberseguridad del Estado mexicano.

Para los oportunistas que piensan que esto será la solución a todo, están muy lejos de razonar que se carece de una temática que logre salvaguardar áreas relacionadas a la ciberseguridad, en estos niveles no es como instalar un antivirus o vender una solución de seguridad, se trata de pensar en las capacidades internas de un país y los matices políticos que impregnan en la actualidad, bajo el entendimiento de la consolidación de políticas públicas como base de todo.

Iniciamos el mes de la ciberseguridad, octubre, con algunos incidentes nacionales internos que requieren atención, si dejamos como usuarios a la ciberseguridad en manos de una simple solución de software o pensamos en que a nadie le interesaría conocer nuestra información confidencial, estamos perdidos, cada dato vale, y la ciberseguridad comienza al reconocer que la información es valiosa, casi incuantificable.

Invito a los lectores a la reflexión, a 'securizar' su entorno, a adentrarse en el ecosistema digital en donde hoy tenemos una convergencia global, y si tienen alguna duda pueden acercarse, para contar con mayor ciberseguridad.

Que comiencen las lecciones del hackeo a la Sedena...

Autor: Carlos Ramírez Castañeda
Fuente de información: expansion.mx