

ESPIONAJE DE CORREOS ELECTRÓNICOS

UNA NUEVA ALARMA ENCENDIDA EN LA SEGURIDAD DE LAS REDES INFORMÁTICAS EN EL PAÍS

En los últimos días, la opinión pública de nuestro país se vio sacudida por un nuevo escándalo relacionado con el tráfico de información. En este caso, se trató del espionaje realizado sobre los correos electrónicos de una larga lista de personalidades relevantes de la política, la justicia y la prensa escrita, entre otras actividades.

La facilidad con la que fueron interceptados mensajes de personas que cumplen funciones relevantes en el quehacer nacional, incluyendo al jefe de Gabinete de Ministros del Poder Ejecutivo Nacional, Alberto Fernández, al ministro de la Corte Suprema, Eugenio Zaffaroni, al presidente del Grupo Clarín, Héctor Magnetto, al director de *La Nación*, Bartolomé Mitre y al presidente provisional del Senado, José Pampuro, entre otros, deja al descubierto el grado de precariedad con la que circula la información en las redes informáticas en nuestro país.

Cabe pensar que si los mensajes enviados o dirigidos a estas personalidades tienen tal nivel de desprotección, poco quedará para el resto de los millones de compatriotas que utilizan Internet. Pero además, plantea otra pregunta crucial: ¿cuál es el nivel de seguridad con que se maneja la información estratégica de la Nación?

En la edición anterior de **M.I** alertamos sobre la gravedad del hecho denunciado por el titular de la ANSES, Sergio Massa, quien acusó a funcionarios de esa institución de vender a una empresa privada los archivos de unos 12 millones de personas registradas en ese organismo (Ver en **M.I** 219 *Inseguridad en los datos personales*).

La Argentina carece de un nivel de seguridad aceptable en sus redes y sistemas informáticos. Esta situación se agrava con el correr del tiempo, en la medida que cada vez más información se intercambia utilizando estas tecnologías. El Plan de Gobierno Electrónico impulsado por el Gobierno Nacional

resulta un gigante con los pies de barro con las actuales condiciones de seguridad. Se deben tomar medidas en forma urgente para corregir esta situación.

Lo primero que deberían hacer las autoridades es determinar la responsabilidad que le cabe a cada uno de los que posibilitaron, con su acción u omisión, la interceptación de los mensajes electrónicos. No es cierto que no se puede prevenir el espionaje electrónico. Quienes hoy se sorprenden por haber sido espiados, son el primer eslabón de una cadena de negligencias y omisiones que deben ser precisadas y corregidas.

Si no existen procedimientos de seguridad, deben ser creados. Si las responsabilidades técnicas están diluidas, debe asignárselas a personas concretas. Los niveles de responsabilidad del personal involucrado en la administración de los servidores de correo han aumentado en la misma medida que se incrementaron los mensajes electrónicos y la importancia de los contenidos de los mismos. Esto es especialmente aplicable a los servidores de correo de todas las instituciones oficiales. Son el primer nodo por donde pasan los mensajes antes de salir a la “nube Internet”, y deben ser corresponsables de que se hagan cumplir procedimientos de encriptación efectiva de toda la información sensible que se origine en los ámbitos oficiales. Es un hecho conocido por los profesionales informáticos que en el mundo existen estructuras informáticas que monitorean toda la información que circula por Internet (Ver en **M.I** 219, *La red de espionaje global Echelon*). Pero forma parte de las responsabilidades de los administradores de servidores de correo, proteger la información que se envía desde su servidor.

Una vez concretados estos objetivos, debe proveerse de un sistema de auditoría externa que asegure que esos procedimientos y responsabilidades sean sostenidos en el tiempo. De esta manera, disminuiríamos la posibilidad de operaciones que restan eficacia y estabilidad a las instituciones que un país en serio requiere.

