TÉCNICOS CONTRARRELOJ

Hackeo en el Senado: El sistema del Congreso sigue afectado

El mes pasado el sistema del Senado Nacional sufrió un hackeo y a menos de 15 días se la sesión preparatoria todavía no logran recuperar todos los datos.

U24

Por **URGENTE24**

El hackeo que sufrió el senado ocurrió el pasado 12 de enero.

Un hackeo en la página oficial del Senado de la Nación Argentina dejó claro lo débil del sistema, que hoy, casi un mes después del inconveniente, sigue sin resolverse.

Aunque oficialmente se informo que el sistema del Senado había sido recuperado del hackeo, **fuentes parlamentarias aseguran que la página oficial de la Cámara Alta no se recuperó del todo y que varias secciones aún no fueron habilitadas.** Así las cosas, al día de hoy, los problemas se están solucionando por partes, pero siguen sin funcionar los sistemas en plenitud.

Es importante señalar que el 24 de este mes está pautada la sesión preparatoria del Senado, **en donde se elegirán a las autoridades de la Cámara y de los bloques que la conforman.**

Según comentaron legisladores de bloques opositores **"se están habilitando por partes"** los sistemas, luego de que en enero no pudieran utilizar ni siquiera sus casillas de correo electrónic o.

"Están trabajando y van comunicando a partir de lo que se puede utilizar. Si lo comparamos con lo que fue a principios de enero, cuando nos avisaron que no podíamos ni entrar al correo electrónico, estamos mucho mejor, pero aún persisten los problemas", explicó un senador al portal Infobae.

Hace menos de un mes, el Senado informó oficialmente que días atrás había sufrido un ataque realizado por piratas informáticos, pero precisó que **"se logró recuperar la mayoría de la información relevante"** que había sido encriptada por los hackers.

El ciberataque se perpetró el 12 de enero a las 4 de la madrugada bajo la modalidad definida como "ransomware**",** la instalación de un virus que impide a los usuarios acceder al sistema o a sus archivos.

Conforme precisó en aquel momento la Cámara alta que preside Cristina Kirchner, a través de la cuenta oficial de Twitter, "los piratas secuestran la información y luego piden un rescate", pero **"en el caso del Senado de la Nación toda la información sustraída es pública y se encuentra al alcance de todos y todas dentro del sitio de transparencia".**

Frente a una versión que circuló sobre pérdida de datos, fuentes de la presidencia de la Cámara alta señalaron que **"no se perdió nada".**

Y en las últimas horas insistieron en que, a causa de eso, no hubo pedido de dinero de parte de los hackers para devolver información que pudiera haber sido perdida.

"Hasta el momento se logró recuperar la mayoría de la información relevante y aislar el equipamiento sensible, lo que nos permitirá recuperar la operatividad a la brevedad", agregaron las fuentes a dicho medio.

> El Senado de la Nación sufrió el 12 de enero a las 4 AM un ataque realizado por piratas informáticos. Este tipo de ataques, denominados ransomware, fueron perpetrados en los últimos meses contra diversos organismos públicos, del Poder Judicial y empresas de primera línea.
>
> — Senado Argentina (@SenadoArgentina) January 14, 2022

Qué es el ransomware

El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito.

¿Cómo puede infectarse?

El ransomware puede infectar su ordenador de varias formas. **Uno de los métodos más habituales actualmente es a través de spam malicioso, o malspam, que son mensajes no solicitados que se utilizan para enviar malware por correo electrónico.** El mensaje de correo electrónico puede incluir archivos adjuntos trampa, como PDF o documentos de Word. También puede contener enlaces a sitios web maliciosos.

El malspam usa ingeniería social para engañar a la gente con el fin de que abra archivos adjuntos o haga clic en vínculos que parecen legítimos, aparentando que proceden de una institución de confianza o de un amigo. Los ciberdelincuentes emplean la ingeniería social en otros tipos de ataques de ransomware, por ejemplo presentarse como el FBI para asustar a los usuarios y obligarles a pagar una suma de dinero por desbloquear los archivos.

Otro método de infección habitual, que alcanzó su pico en 2016, es la publicidad maliciosa. La publicidad maliciosa consiste en e l uso de publicidad en línea para distribuir malware con poca interacción por parte del usuario o incluso ninguna. Mientras navegan por la web, incluso por sitios legítimos, los usuarios pueden ser conducidos a servidores delictivos sin necesidad de hacer clic en un anuncio. Estos servidores clasifican los detalles de los ordenadores de las víctimas y sus ubicaciones y, a continuación, seleccionan el malware más adecuado para enviarlo. Frecuentemente, ese malware es ransomware.