LITORALPRESS

Fecha: 15-11-2023
Medio: La Tercera
Supl. : La Tercera - Pulso
Tipo: Noticia general
Título: Agencia de ciberseguridad del gobierno califica ataque a GTD como un "incidente grave y masivo" y Subtel alista reunión con gerentes

Pág. : 12
Cm2: 774,7
VPE: $ 7.707.128

Tiraje: 78.224
Lectoría: 253.149
Favorabilidad: No Definida

Agencia de ciberseguridad del gobierno califica ataque a GTD como un "incidente grave y masivo" y Subtel alista reunión con gerentes

Hoy existen entidades públicas que recuperaron el sistema y los datos, pero todavía no están funcionado. Ejemplo de ello es el problema que mantiene GTD con un grupo de municipalidades del sur del país, como Puerto Natales, Purranque, Temuco, Lago Ranco, Mariquina y Futrono. A ellos se suman al menos 10 servicios públicos que forman parte del aparato central del Estado que también resultados afectados. Entre ellos están Servicio Civil, Superintendencia de Educación Superior, Subsecretaría de Desarrollo Regional (Subdere), Firma Digital y el Fondo Nacional de Salud (Fonasa). Estos dos últimos recuperaron la funcionalidad de sus sitios.

LEONARDO CÁRDENAS

–Al interior de GTD, uno de los principales proveedores de servicios digitales de internet en Chile y Perú, permanecen en estado de alerta producto de un masivo ciberataque que sufrió la compañía el pasado lunes 23 de octubre.

La compañía controlada por el empresario Juan Manuel Casanueva informó al Equipo de Respuesta a Incidentes de Seguridad (CSIRT), agencia dependiente del Ministerio del Interior, y presentó una denuncia penal ante la Fiscalía Metropolitana Centro Norte. El propio gerente general, Fernando Gana, ha sostenido reuniones con clientes para explicar lo ocurrido y ha encabezado las gestiones para volver a recuperar los sistemas tras el ataque, pero su trabajo no acaba.

A 22 días del ataque del *ransomware*, un tipo de *malware* que bloquea archivos y dispositivos de los usuarios, parte de sus clientes aún no puede acceder a información clave para su operación, como Oddis y Assa Abloy, las cuales presentaron un recurso de protección que sigue pendiente, ahora en la Corte Suprema. La acción legal exige que los ejecutivos de la empresa expliquen el trabajo realizado ante la magnitud del impacto.

Por medio de una declaración por escrito enviada a Pulso, la agencia de ciberseguridad del gobierno (CSIRT) calificó la situación sufrida por la empresa de telecomunicaciones como un "un incidente grave que fue masivo".

Al mismo tiempo, destacó que la compañía notificó el incidente el mismo día en que fue público. El hecho es valorado al interior del organismo de gobierno, debido a que en la actualidad las empresas no están obligadas a efectuar un aviso a la autoridad por un incidente de ciberseguridad.

En paralelo, el equipo del CSIRT informó que adoptó "todas las medidas técnicas y preventivas para aislar a los servicios para evitar cualquier tipo de contagio". En esa línea, "se estableció una coordinación donde reportan diariamente avances del incidente".

"En el caso de los servicios públicos, hubo una decena que fueron afectados, (pero) se fueron recuperando aquellos más críticos. El hecho de que haya afectado a un proveedor implica que la afectación no es sólo de sí mismo sino sobre sus clientes, lo que en volumen es importante", acotó la misma institución.

La compañía, que cuenta con 44 años de historia, se encuentra en un período complejo ante sus clientes. Según su último reporte anual de 2022, GTD cuenta con 277.000 clientes residenciales, mientras que los clientes del área corporativa corresponden a más de 38.000. Justamente este último grupo sería el más afectado con el incidente de seguridad sufrido el pasado 23 de octubre. El 72% de sus ingresos, que llegaron a $426.500 millones en 2022, correspondieron a este grupo.

Felipe Melo, director del Servicio Civil explicó a **Pulso** que "la falla de GTD interrumpió gravemente nuestros procesos críticos. Junto con pedirles disculpas a nuestros usuarios, podemos informar que como Consejo de Alta Dirección Pública ya hicimos la denuncia al Consejo de Defensa del Estado, para que tome las acciones pertinentes ante la gravedad de la situación. Asimismo, gracias a que previamente se había reforzado la seguridad de las plataformas, ya hemos logrado recuperar los respaldos de nuestros portales, por lo que estamos próximos a recuperar nuestro servicio regular".

UN "CIFRADO MUY SUPERIOR A OTROS CONOCIDOS A LA FECHA EN CHILE"

A través de una declaración por escrito, GTD respondió a **Pulso** que cuenta con un programa de ciberseguridad y continuidad de negocio certificado, con estándares internacionales (ISO 27.001/ISO 22.301), además de un proceso continuo de concientización en ciberseguridad para colaboradores, que involucra a toda la compañía. Existen protocolos de seguridad que permiten detectar, contener y erradicar intentos de ataques de ciberseguridad, de forma constante, y con un monitoreo 24/7.

"El pasado 23 de octubre, GTD sufrió un evento de fuerza mayor, correspondiente a un incidente de ciberseguridad que afectó la plataforma IaaS, provocado por una nueva variante de un *malware* tipo *ransomware* conocido como Rorschach (o BabLock) con un nivel de sofisticación y rapidez de cifrado muy superior a otros conocidos a la fecha en Chile y en el mundo. Entre las múltiples medidas que se han tomado, se incluye la desconexión de la plataforma para evitar cualquier riesgo de propagación. A su vez, hemos incorporado especialistas de empresas líderes de la industria a nivel mundial, quienes nos están acompañando en el proceso de respuesta del incidente, e investigación. Desde que detectamos e informamos el incidente al CSIRT y a nuestros clientes, se ha avanzado en disponibilizar sus servicios en un ambiente securitizado y con el mayor resguardo", acotó.

MUNICIPALIDADES

Hoy existen entidades públicas que recuperaron el sistema y los datos, pero todavía no están funcionado. Ejemplo de ello es el problema que mantiene GTD con un grupo de municipalidades del sur del país, como Puerto Natales, Purranque, Temuco, Lago Ranco, Mariquina y Futrono. A ellos se suman al menos 10 servicios públicos que forman parte del aparato central del Estado, que también resultados afectados. Entre ellos están Servicio Civil, Superintendencia de Educación Superior, Subsecretaría de Desarrollo Regional (Subdere), Firma Digital y el Fondo Nacional de Salud (Fonasa). Estos dos últimos recuperaron la funcionalidad de sus sitios.

Sin embargo, a la fecha, no existen cifras oficiales sobre el número de empresas y entidades públicas afectadas por el ataque. Tampoco en el gobierno tienen claridad, aunque existe un activo monitoreo por parte del CSIRT y de la Subsecretaría de Telecomunicaciones (Subtel). Esta última explicó a **Pulso** que ha estado atenta a los reclamos que ingresan los usuarios tras el ciberataque y su División de Fiscalización mantiene "un permanente contacto con la compañía, verificando que este incidente no afecte a usuarios en ámbitos de competencia de Subtel, que son las redes de telecomunicaciones". Subtel también ha colaborado activamente en la coordinación entre GTD y el CSIRT en este tema.

Además, próximamente Subtel recibirá a ejecutivos de la compañía, instancia en que solicitará nuevos antecedentes sobre el ataque y la afectación que puedan tener para los usuarios de telecomunicaciones.