Mauricio Andrés Burgos Navarrete
Dir. carrera Auditor e ICG UAutónoma de Chile(Tco)

Ransomware o no en BancoEstado?

Economía, 08/09/2020

Los ciberataques y sus efectos pueden alcanzar a empresas y personas, provocando daños de distinta índole, que pueden llegar a ser irrecuperables. Ello obliga a tomar medidas preventivas y de resguardo.

Estamos en un momento de la historia en que la tecnología está cada vez más presente en nuestras vidas, y en la cual la inter operatividad y comunicación entre dispositivos adquiere ribetes impensados. Así, la masificación en distintos estratos, también amplifica los riesgos. Y particularmente, si no adherimos a determinados protocolos de resguardo y seguridad, podemos llegar a una instancia demasiado tardía, en la podríamos estar llorando sobre la leche derramada.

Es bueno recordar que hace unas semanas atrás, la reconocida empresa Garmin, dedicada a la producción de GPS y wearables, sufrió de un ataque informático que la mantuvo inactiva en su sitio web durante algunos días. Luego de especulaciones varias, se insinuó que habría sido afectada por un ransomware, esto es el secuestro de datos para extorsionar al titular a su pago, denominado WastedLocker, ligado a un grupo de hackers que se da a conocer bajo el nombre de Evil Corp, los cuales tendrían su sede en Rusia.

Como no se ha proporcionado una comunicación oficial al respecto, se ha planteado que habría recuperado su operatividad luego de haber pagado un rescate multimillonario para poder acceder nuevamente a sus equipos e información almacenada, pero dado que de haber acontecido esta situación la expondría a sanciones por parte de entidades gubernamentales, habría utilizado a un tercero para el pago del rescate.

Cabe mencionar que la empresa como medida de precaución, procedió a solicitar a sus empleados apagar las computadoras, particularmente aquellas que puedan conectarse a información relevante, a fin de evitar que sean encriptados. Asimismo, también se ha señalado que no hay evidencia de que los ciberdelincuentes hayan tenido acceso a información privada tanto de usuarios como de empleados.

La reciente situación experimentada por Banco Estado, y que lo llevó a suspender parte de su atención cotidiana, abre la idea

de que lo acontecido podría haber sido resultado de un evento similar, máxime cuando una autoridad trató de explicar de manera simple que el ataque se basa en virus que encripta información, inhabilitando el acceso a esos dispositivos.

Además, si bien se ha planteado que los dineros de los clientes del banco no han sido afectados, queda la duda de que ello sea así. Basta recordar lo sucedido años atrás con Banco Chile.

Por otra parte, es importante considerar que en el Global Risk Report 2020, preparado por el World Economic Forum, en su Panorama de Riesgos, ubica a los ciberataques como una situación de alta probabilidad de ocurrencia e impacto en las organizaciones, lo cual se mantiene respecto al 2019.

Finalmente, sea o no ransomware, lo que queda claro es que a fin de evitar daños reputacionales y monetarios se debe tener una actitud preventiva, y para lo cual algunas ideas que normalmente se recomiendan son: a) no hacer clic en enlaces no confiables; b) evitar abrir archivos adjuntos de emails que no sean de confianza; c) descargar archivos solo de sitios web de confianza; d) no facilitar datos personales a fuentes no confiables; e) utilizar el análisis y filtrado de contenido del servidor de correo electrónico; f) no utilizar dispositivos USB desconocidos o que hayan sido utilizados en equipos de dudosa funcionalidad; g) mantener actualizados el software y sistema operativo; h) utilizar una VPN al hacer uso de una red Wi-Fi pública; i) utilizar software de seguridad; j) mantener el software de seguridad actualizado; k) realizar copias de seguridad de la información con cierta regularidad; l) estar atentos al surgimiento de nuevas versiones de virus o ataques que se produzcan; m) capacitar a los colaboradores; y n) establecer una cultura de seguridad preventiva.

Mauricio Andrés Burgos Navarrete