¿Pagar el rescate? Los abogados corporativos dicen que satisfacer las demandas de algunos hackers puede valer la pena

La sabiduría convencional dice que las víctimas del ransomware no deberían pagar a sus atacantes, pero un panel de expertos legales sugirió el jueves que la firma permanente no siempre es la mejor opción en el mundo real.
Funcionarios del FBI, grandes corporaciones y jefes de seguridad del sector público en los últimos años han aconsejado a sus colegas que mantengan sus billeteras cerradas cuando llegue el ransomware. No hay honor entre los ladrones, la lógica continúa, e incluso si le pagas a los piratas informáticos para que se larguen, ¿quién puede decir que cumplirán las promesas de desbloquear datos cifrados? Pero hay escenarios en los que las pequeñas y medianas empresas deberían considerar cuidadosamente su decisión, dijeron Mark Knepshield y Matthew Todd durante una mesa redonda en la conferencia Legalweek en Nueva York.

"Yo diría que, si se trata de una pequeña cantidad, pague", dijo Knepshield, vicepresidente de la aseguradora McGriff, Seibels y Williams. "Es probable que sea la forma más fácil de salir de tu situación".
En una encuesta que encuestó a los asistentes de Legalweek, el 86 por ciento dijo que no pagaría un rescate si los atacantes amenazaban con publicar material robado en línea dentro de las 24 horas. Eso sigue el consejo legal tradicional, con el FBI alentando a las empresas pirateadas a no pagar, en parte porque satisfacer las demandas de los extorsionadores podría ayudar a los ladrones a expandir sus operaciones.
"La aplicación de la ley debe tener una política, y esa debe ser su política", dijo Todd, consultor principal de Full Scope Consulting y ex director de seguridad en el sector financiero.
Sin embargo, la evolución de los ataques de ransomware en el último año ha obligado a las empresas a reconsiderar, dijo Todd. Las organizaciones criminales con buenos recursos han reemplazado las operaciones de "pago y pago" comparativamente de bajo nivel. Esos grupos dejan un rastro de evidencia que las aseguradoras, los abogados y los equipos de seguridad corporativa pueden investigar rápidamente para comprender sus posibilidades de recuperar información robada.

"Al igual que con la ciudad de Atlanta, con el código fuente que estaba llegando, incluso si hubieran pagado el rescate, no creo que las personas que lanzaron el ataque hubieran tenido la sofisticación para poder deshacer el [cifrado] claves ", dijo Todd. "Necesitas meditarlo con cuidado".
Pagar pequeños rescates también puede ayudar a los jefes de seguridad frustrados a evitar que los superiores se preocupen más por reanudar los negocios que por examinar la evidencia forense en medio de un ataque. La pérdida de $ 500 a los piratas informáticos podría acelerar el proceso y otorgarle a los jefes de seguridad de la información un acuerdo con su jefe.

Fuente https://www.cyberscoop.com