Manual de Procedimientos y preparación. Claves ante extorsiones de ciberdelincuentes: Tanium

- Las empresas no deben limitarse a esperar a que se produzca un ataque para decidir si pagan o no una extorsión de los ciberdelincuentes.

Ciudad de México. 27 de mayo de 2024.- Tanium, proveedor líder de la industria de administración convergente de terminales (XEM), señala que la preparación es fundamental en todas las facetas de la ciberseguridad, y el ransomware es simplemente otro disruptor de las operaciones. Tratar el ransomware como se haría con la escasez de personal o la desconexión de la red, donde existen planes en casos de escenarios catastroficos, es la única forma de manejar con éxito los cada vez más sofisticados ataques.

Por eso es tan importante que las organizaciones no se limiten a esperar a que se produzca un ataque para decidir si pagan o no una extorsión de los ciberdelincuentes. Es necesario contar con un manual de procedimientos detallado que explique paso a paso qué hacer y las personas que deberán estar involucradas y tendrán acceso y comunicación con el equipo que mitiga el problema.

Para Tanium, este manual deberá responder a cuestiones como si el posible pago de un rescate viola el código de ética o los valores fundamentales de la empresa; si es más beneficioso para la empresa pagar; cuál sería la cantidad correcta y si es realmente legal pagar el rescate.

“Comprender el radio de daño del ransomware, o el impacto que tendrá un ataque en una organización, será clave para determinar cómo manejar la situación. Esto es exclusivo de cada organización, pero si una empresa está preparada y se realiza una copia de seguridad de sus datos en consecuencia, no hay absolutamente ninguna razón para pagar una extorsión”, señaló Tim Morris, Jefe de Seguridad de Tanium.

Un paso que puede parecer obvio, pero que en ocasiones las empresas pasan por alto, es verificar que efectivamente se sufrió un ataque. No es raro que los ciberdelicuentes fanfarroneen, y poder denunciarlos puede cambiar completamente el contexto, incluso optar por ignorarlos y seguir adelante por completo.

Por otra parte, si efectivamente la empresa fue atacada y sus archivos fueron cifrados, la dinámica de cómo abordar la situación depende en gran medida de quién participa en la estrategia de respuesta a incidentes: representantes del equipo ejecutivo, asesores legales externos e internos, una aseguradora cibernética y equipos de comunicaciones. Es mejor evitar que los ejecutivos negocien solos (de así haberlo decidido la empresa), y también es importante determinar quién se encargará de los esfuerzos para mantener al equipo alineado en el mejor curso de acción.

Tanium afirma que en una negociación hay algunas cosas que debe determinar: como si algún dato privado o confidencial se ha visto comprometido; qué banda cibernética está involucrada; de qué manera los datos volverán a estar en línea después de que se resuelva el pago; si las autoridades tienen claves de descifrado disponibles de ataques anteriores, por mencionar algunas. Comprender el ataque e iniciar un diálogo con el ciberdelincuente permitirá negociar un mejor acuerdo o comprender cuándo el amenazante está exagerando su poder.

Prepararse para el cambio es inevitable

Para Tanium, la evolución del software y el aumento de la Inteligencia Artificial (IA) generativa están haciendo que el ransomware sea más sofisticado que nunca. Los grandes modelos de lenguaje (LLM) incluso están siendo contaminados para que los ciberdelincuentes puedan convertir un ataque externo en una amenaza interna, por lo que la clave para una negociación exitosa es apegarse al manual.

“La fuerza de una estrategia de negociación y respuesta no debería depender del ataque en sí. El arte de la negociación es atemporal y se adapta a los constantes cambios del panorama de la ciberseguridad. Con el tiempo, podríamos ver un mundo en el que la falta de pago sea la única respuesta y el ransomware se vuelva obsoleto. Desafortunadamente, ese no es el caso en la actualidad, y todas las organizaciones deben estar preparadas para el día en que sean atacadas y quizá se vean obligadas a pagar”, finalizó Morris.