Ransomware: Lo que realmente debe saber

Ya está entre nosotros. Una simple porción de código que ejecuta otra porción de código e inicia un laborioso proceso para cambiar sus datos y transformar sus elementos legibles útiles en basura encriptada. Eso no sucede inmediatamente, sino que se trata de un enfoque insidioso que, finalmente, hace que todos sus archivos no estén disponibles para la persona que más los necesita: ¡usted! Bienvenido al mundo aterrador e impredecible del ransomware.

En 2016, los ataques de ransomware aumentaron más del 167 por ciento y continúan siendo un gran negocio de casi mil millones de dólares pagados al año para solucionar algunos casos, y una cantidad innumerable de otros que se resuelven independientemente o no se resuelven en absoluto.

Entonces, ¿qué es el ransomware? ¿Debería usted preocuparse por ello? Las respuestas son aparentemente sencillas, y las mejores son: "algo malo" y "sí". Primero echemos un vistazo a lo que hace realmente el ransomware. Si su computadora se infecta con ransomware, tendrá un comportamiento alterado, ya que todos los archivos del sistema se ejecutarán a través de un encriptador. Es posible que no se dé cuenta de lo que está sucediendo, pero, a medida que los archivos se encriptan, los que no están encriptados se eliminan del sistema. La consecuencia directa es que la computadora está llena de datos encriptados, pero usted no tiene acceso a ellos sin la clave de desencriptado.

En las primeras etapas, el ransomware tenía errores de enfoque, como dejar la clave de desencriptado en el sistema o tener algún indicador. Hoy en día, es menos probable que suceda eso, ya que los atacantes continúan madurando en su industria multimillonaria. Si usted sufre un ataque, es mucho menos probable que encuentre una salida sencilla. La consecuencia directa será que no podrá utilizar su computadora, y las probabilidades de que esta vuelva a funcionar eficazmente serán muy limitadas.

La pregunta importante que todos se hacen es: "¿Yo corro riesgo?". Muchas personas prefieren pensar que una empresa pequeña no corre riesgo porque no representa una gran ganancia. Eso es falso, ya que los atacantes ahora sacan más provecho de las empresas pequeñas que de las grandes, simplemente porque el vector de ataque es más simple. ¿Para qué van a dedicar días o semanas a planificar un gran golpe si con varios más pequeños pueden tener una ganancia relativamente directa e igual de efectiva, ya que la posibilidad de encriptado es mayor? En pocas palabras, ¿para qué atacar a un grupo bien protegido para ganar $50,000 si pueden ganar lo mismo con diez ataques de $5,000?

Los ataques pueden ser incluso más sencillos. Si bien cualquiera puede sufrir uno de estos ataques indiscriminados y el potencial de infección se distribuye equitativamente, las empresas más pequeñas son el blanco más sencillo porque, con frecuencia, no asignan ni el tiempo ni el dinero necesarios para proteger eficazmente sus sistemas, y no tienen tiempo para mantenerse involucrados o protegidos como las empresas con presupuestos masivos y dataciones de personal moderadas.

Si consideramos el panorama general, se presenta muy sombrío. La mayoría de las empresas analizan la situación y se paralizan tanto con lo que podría suceder que pierden de vista el panorama general y terminan haciendo muy poco para protegerse a ellas mismas o a sus usuarios. Si usted está preocupado, y debería estarlo, aquí le informamos lo que tendría que estar haciendo ya mismo.

1) Revise su estrategia de copia de seguridad y recuperación ante desastres: reconozcámoslo; el ransomware es un desastre. Aunque pague, es posible que no reciba una clave para el desencriptado y tenga que esperar pacientemente por algo que tal vez nunca llegue. Debido a

que el ransomware destruye efectivamente su sistema, la única defensa segura es poder restaurar el sistema rápida y eficazmente. Tal vez se pregunte: “Pero si uso algún producto, ¿no me protegerá?”. Y la respuesta es: “Seguro, pero siempre puede ser una de las primeras víctimas, y no habrá protección contra eso”.

Una buena estrategia de copia de seguridad emplea la regla 3-2-1. Tres copias de sus datos, 2 formas de medios y 1 fuera del sitio. El ransomware presenta una salvedad. La copia de seguridad fuera del sitio no puede ser inmediatamente accesible para su sistema de archivos. Más directamente, la copia fuera del sitio no puede ser una copia de archivos que se guarda en servicios como Box, Dropbox, iTunes o cualquiera que simplemente copie archivos. ¿Por qué?

Recientemente, nos llamó una empresa que había sufrido un ataque de ransomware y usaba Box como copia de seguridad. Tenían mapeada una unidad, y cada noche los archivos se copiaban del servidor a Box. Adivine qué sucedió: cuando el ransomware dio el golpe, encriptó también todas las copias de seguridad y dejó vacía la empresa, sin ningún archivo.

Analicemos también RPO y RTO. RPO es el objetivo de punto de recuperación, o cuántos datos está usted dispuesto a perder. A medida que la cantidad de datos perdidos se aproxima a 0, el costo de la solución es mayor. RTO es el objetivo de tiempo de recuperación, o cuánto tiempo se puede permitir estar inactivo. Cuanto más cerca de 0 se encuentra el tiempo de inactividad, mayor es el costo. Analicemos detenidamente estos dos elementos, ya que la mayoría de las personas afirmarán felizmente que nunca quieren estar inactivos ni perder ningún dato, pero el costo puede ser considerable.

Una buena solución puede costar un poco. Existen excelentes opciones como Veeam y Datto, que también ofrecen soluciones en la nube. Datto incluso ofrece un host temporal en caso de que haya algún problema. La cantidad de soluciones se encuentra en aumento, pero existe otro aspecto de la estrategia de copia de seguridad: ¡probarla!

Si sufre un ataque, la solución es simple: debe restaurar hasta un punto anterior al ataque y evitar pagar sumas excesivas de dinero para restaurar su sistema.

2) Capacite a todas las personas: la mayor amenaza para sus sistemas son usted y su gente. A pesar de todo lo que hay en Internet, si usted hace solo su trabajo y presta atención al modo en que maneja las comunicaciones de Internet, es posible que su riesgo sea bajo; sin embargo, ¿cómo puede hacer para evitar el ransomware si trabaja en forma remota, en computadoras portátiles, o por todos los medios sociales? Nos gusta decir que el sentido común sirve, pero eso solo es cierto hasta cierto límite.

   La concientización ayuda a que los empleados estén preparados para no ser víctimas de un ataque de ransomware. Las pruebas de suplantación de identidad (correos electrónicos falsos enviados a grupos para determinar puntos humanos de entrada a una organización) fallan con más frecuencia que con la que tienen éxito. Esto se debe simplemente a que un solo clic o una sola entrada constituye una falla para todos.

   Existen numerosos recursos disponibles, y SBDC hace un gran trabajo organizándolos para las pequeñas empresas. Tómese un momento y analice cuál es el más adecuado para usted. También existen nuevos productos como KnowBe4, que capacita y evalúa a los empleados con

niveles de complejidad cada vez mayores. El objetivo es detectar el eslabón más débil de la cadena antes de que este pueda hacer clic e infectar a toda la empresa con un ataque de ransomware. Recuerde que la persona que usted olvide capacitar o pase por alto puede ser la que destruya su sistema.

3) Busque protección: existen muchos programas que pueden proteger su sistema contra algunas amenazas, pero no todas ellas pueden manejarse con una sola solución. También hay que tener en cuenta la protección de la red. No se limite a ir a su tienda local y comprar lo primero que ve en los estantes. Por el contrario, pida ayuda para diseñar una solución a su medida. Como mínimo, obtenga un buen cortafuegos de calidad profesional (es decir, no uno de una tienda de descuentos), un buen programa de seguridad de Internet que incluya protección contra virus y malware, y un buen programa de protección secundaria que bloquee los sitios no seguros. Siempre existe la posibilidad de ser el paciente cero; es decir, aunque no exista la cura para algo, si tiene una buena estructura estará seguro en términos generales. También es buena idea considerar la protección contra la intrusión, el encriptado de correos electrónicos y la administración de contraseñas para estar aun más seguro. Independientemente de su enfoque de protección, es probable que deba solicitar ayuda, simplemente porque hay muchos aspectos que se deben tener en cuenta y no existen las soluciones “universales”.

   Nos hemos encontrado con varias situaciones en las que se indicaba a las personas que usaran soluciones gratuitas o de bajo costo. Como dijimos anteriormente, analice el impacto que cualquier problema tendrá en su empresa y cuánto podría costar ese impacto antes de usar un antivirus gratuito, o un cortafuegos económico, o de elegir por el precio. Para elegir, concéntrese en las funciones y las necesidades, y será más probable que pueda mantenerse seguro.

4) En el peor de los casos, sepa a quién acudir: con respecto al tema de pedir ayuda, conviene conocer de antemano a alguien que lo pueda ayudar a solucionar esa terrible emergencia que no había previsto. Muchas personas, demasiadas, piensan en el problema únicamente cuando ocurre y les cuesta encontrar una solución. Recientemente recibimos a un cliente que había pagado una enorme suma de dinero a una empresa en línea de recuperación ante ataques de ransomware. Después de algunos meses, le dijeron: “Lo sentimos, pero no pudimos hacer nada”. Y perdió todo su dinero. El primer día, recuperamos una veintena de archivos y le ayudamos a iniciar el proceso de restauración. Busque una empresa que esté dispuesta a ayudarlo a prepararse y que vaya a estar disponible cuando la necesite. Debe ser una empresa que tenga un registro comprobado de resultados positivos en diversas tecnologías.

   Recuerde que, en última instancia, su empresa depende de usted y sus clientes también. Ya no habitamos un mundo en el que podamos decir: “Eso nunca me sucederá”. Por el contrario, es un mundo en línea plagado de personas peligrosas que quieren robarle su dinero. Tómese un momento y analice cómo podría hacer negocios sin computadoras o sin acceso al mundo en línea. Luego tómese un momento y analice cuánto impacto tendrá la pérdida de sus sistemas en sus finanzas, operaciones, trabajadores y todo lo demás que conforma su empresa.

   Cuando lo haya hecho, analice qué valor tiene no perder todo eso ni la credibilidad asociada con sufrir un ataque de ransomware, o no poder hacer funcionar su empresa eficientemente, y reaccione en función de ello.

Si necesita asistencia, acuda a SBDC o busque acceso a recursos útiles que le enseñen a protegerse contra el ransomware.

Por supuesto, todas estas acciones no son completas y existen procedimientos cada vez más rigurosos que pueden implementarse. Es necesario que decida cuánto está dispuesto a perder y cuánto podría perder para tomar la mejor decisión para su empresa. ¡Tome buenas decisiones para evitar ver la pantalla de bloqueo en su sistema!