Prevención del secuestro de datos

Como el ransomware afecta a los sistemas de seguridad

El robo y "pedido de rescate" de datos comenzó a hacerse popular hace poco tiempo, momento en que comenzó a hablarse de un tipo de virus denominado "ransomware", capaz de tomar información de una entidad y "esconderla" para luego pedir rescate por ella.

Lic. Damián Colaneri
Socio Gerente
T3 Tic Ingeniería SRL
dcolaneri@t3tic.com.ar

Si bien "ransomware" es un término que se está volviendo cada vez más popular, este tipo de código lo vimos hace ya casi 10 años. Se trata de un código malicioso destinado a encriptar toda información que encuentre a su paso, por la que luego pedirán un pago de "rescate" en bitcoins para liberarla. Este código se reproduce y multiplica a través de la red afectando a cualquier medio de información vulnerable a él, según su mutación. ¿A qué me refiero con mutación?: el código de ransomware está libre en internet para que uno lo descargue y analice. Sin embargo, alguien también puede descargarlo, modificarlo para un objetivo concreto y utilizarlo con fines maliciosos. El último código ransomware en volverse popular fue "WannaCry".

¿Cómo afecta a los sistemas de seguridad?: si el ransomware busca datos para encriptar y pedir un rescate, nuestra vulnerabilidad se encuentra en los discos de datos donde almacenemos información importante, como los de almacenamiento de video, sin importar si está basado en un sistema embebido o de base software en un server.

También puede afectar a los discos de un sistema de control de acceso, donde además de perder los datos de todo el personal cargado, podríamos perder todo el log de eventos. Del mismo modo se vuelve peligroso en centrales de alarma y/o monitoreo.

Pensemos, como debemos hacer en seguridad, que "somos" el intruso e imaginemos vectores de ataque: nuestros clientes con mayor información, y a su vez, si esa información es muy valiosa, serán los primeros en ser atacados. Seguramente en lo que primero pensaron fue en bancos y es correcto, ya que el video log de eventos tanto de alarmas como de control de acceso son un jugoso botín para quienes se dedican a esto. También lo pueden ser grandes empresas a las que les instalamos el sistema de seguridad.

Recordemos que aunque nuestro cliente disponga de un área propia o externa de seguridad de la información, a la hora de verse afectado un sistema de seguridad electrónica nosotros deberemos dar las respuestas al problema. Es por esto, que siempre debemos proteger nuestras integraciones, más allá de la seguridad de la red donde nos montemos si esta no es nuestra responsabilidad.

Los primeros sistemas a revisar son los basados en software, del tipo cliente servidor, seguramente en plataforma Windows, aunque también debemos proteger los Linux. Esto es regla básica, siempre estar al día en las actualizaciones del sistema operativo tanto del lado cliente como del lado servidor. Los parches de seguridad no pueden esperar a ser instalados: recuerden que hay vulnerabilidades "cero day" -que es como se clasifican las más peligrosas- y debemos actualizar nuestros equipos en cuanto el fabricante suba el parche. Luego, debemos mantener siempre la última versión del software que corresponda según nuestra integración. Todos los software de gestión de video, alarmas, control de acceso, etc., tienen parches y actualizaciones constantemente y al igual que en el sistema operativo debemos estar al día, siempre que nuestro sistema sea compatible con la actualización. Algunos proveedores de software suelen cobrar un adicional en el paquete de licencias para tener las actualizaciones al día por períodos de 1, 2 o 3 años. Recomendamos contratarlo, ya que por querer ahorrar un pequeño costo que en el total no hará diferencia, nos exponemos a tener problemas de seguridad.

En el caso de sistemas embebidos, y en este apartado incorporamos a las cámaras IP, es importante tener siempre el último firmware disponible para el dispositivo.

Si bien hay menor posibilidad de error humano al momento de implementar, el software embebido no deja de lado la posibilidad de tener fallas en su código, ya que el nivel máximo de seguridad es 99%. También recordemos que los sistemas tienen "backdoors" puestas adrede por los fabricantes con un fin útil, pero que puede ser explotado y muchas veces no sabemos de su existencia.

Finalmente, recordemos siempre revisar la web de los fabricantes en busca de nuevos firmware. Debemos conocer a la perfección lo que implementamos y realizar los cursos de certificación de cada marca para hacer implementaciones seguras. ■