EL SECUESTRO DE INFORMACIÓN, UN PROBLEMA QUE CRECE

NOTI 257 – 8 de Noviembre de 2016

Para combatir los ataques informáticos es importante:

Prevención: adquiera programas serios de antivirus, anti malware y anti ransomware.

Copias de respaldo: realice copias de respaldo de sus archivos de forma regular y guáderla fuera de línea para prevenir su infección.

Educar: capacite e informe a sus empleados sobre el peligro del Pishing y otras formas de captura de información.

Fuente: http://cotorrera.com/wp-content/uploads/2016/03/encriptacion1.jpg

Esta historia está ocurriendo en nuestro país, no en un lugar lejano. Una mañana temprano, el área de Sistemas de una empresa recibe la llamada de un empleado, quien manifiesta no poder acceder a la información de su computador de trabajo. Luego de hacer las comprobaciones básicas de rutina, las que invariablemente incluyen preguntas como "¿está encendido el PC?"; ¿"está usando su contraseña?"; "¿ya reinició el equipo?", el encargado de servicio al cliente interno se da cuenta que realmente hay un asunto que requiere su atención.

Mientras se prepara para dirigirse al puesto de trabajo con problemas, su teléfono comienza a sonar de manera ininterrumpida. Ahora son todos los usuarios del Sistema, quienes llaman a reportar que no pueden acceder al servidor central. En vista de ello, y convencido ahora que el problema no es local sino de todos, decide revisar el servidor y los canales de comunicación para tratar de hallar el problema y la solución. Luego de unos momentos de revisar sin resultados, se recibe un e-mail en el cual se anuncia, palabras más palabras menos, que la información de la empresa ha sido encriptada, y que solo se enviará el código para desencriptarla si la empresa acepta pagar una elevada suma, usualmente en Bitcoins.

Desafortunadamente, llegados a este momento es muy poco lo que puede hacerse, salvo oponerse al pago de este tipo de extorsión y buscar cómo seguir adelante. Si usted decide pagar, existe una alta probabilidad de no

recuperar la información y perder el dinero pagado a los delincuentes. De ahí la importancia de evitar que este tipo de situaciones ocurra en la empresa.

Existen varios tipos de ataques que terminan en la pérdida de su información.

Scareware: esta modalidad consiste en que los delincuentes fingen ser empresa serias y comienzan a enviar correos advirtiendo que tu servidor está infectado con miles y miles de virus y malware, y que la única manera de retirarlos es comprándoles sus productos. Este es el menos riesgoso de todos, ya que basta con tener en cuenta que una empresa seria de antivirus o anti malware nunca van a tratar de vender causando miedo a sus clientes.

Se recomienda no hacer ningún pago en caso de secuentro de información, ya que esta situación podría repetirse una y otra vez.

Encriptación de información: este es el verdadero problema. En este esquema, los delincuentes realmente logran ingresar a sus sistemas o servidores, procediendo a encriptar su información y exigiendo dinero para desencriptarla. La verdad es que cuando esto ocurre, no existe forma de reversar la situación, a menos que usted acceda a las pretensiones de los delincuentes, y ni siquiera esto garantiza su recuperación. Pese a que en muchos casos las autoridades a quienes se pone en conocimiento de este tipo de situaciones recomiendan pagar, nuestra opinión es que no debe hacerse bajo ninguna circunstancia, ya que ello constituye el pago de una primera cuota. Pude tener la seguridad que el ataque se repetirá.

Entonces, ¿qué puede hacerse para gestionar este tipo de amenazas? La respuesta no puede ser más obvia: prevenga, ya que nada puede hacerse una vez que la empresa ha sido atacada. Nada.

La mejor y más eficaz prevención es la de invertir en programas serios de anti virus, anti malware y anti ransomware. Existen varias ofertas de este tipo de productos, que pueden acomodarse al tamaño y presupuesto de la empresa.

Segundo, por muy incómodo que resulte, se debe implementar un programa real y eficiente de copiado de respaldo de todos sus archivos, de manera regular y obligatoria. Obviamente, las unidades externas en las que se hagan las copias de dichos archivos deberán ser desconectadas físicamente de los demás equipos y de la red, a fin de reducir la posibilidad de que las copias también terminen infectadas. El almacenamiento en la

nube es otra opción, pero exigiendo condiciones claras de encriptación y autenticación de alto nivel.

Sin embargo, nada de esto sirve si no se educa a los usuarios. A todos. La manera más común de infectar equipos es mediante el uso de la denominada Ingeniería Social. Instruya a todos los usuarios acerca de los peligros del Phishing y de otros modelos de captura de información por parte de personas al acecho. Siempre recuerde: si parece demasiado bueno para ser cierto, normalmente no lo es.

Póngase en contacto con nosotros

ASR S.A.S
Carrera 40 N° 10-20
Medellín, Colombia
+57 4 266 33 42
asr@asr.com.co
http://www.asr.com.co/