LOS DELITOS INFORMÁTICOS SON IMPACTANTES, PERO NO SON COSA DE PELÍCULA

NOTI 253 – 6 de Julio de 2016

"Esto está ocurriendo en nuestro país, no en su televisor. Las personas que manejan los sistemas y equipos de procesamiento de datos de las empresas tienen la obligación de entender que la seguridad de los mismos depende en gran medida de las precauciones que ellos tomen al momento de conectarse"

Fuente: cristianysublog.wordpress.com

LOS DELITOS INFORMÁTICOS SON IMPACTANTES, PERO NO SON COSA DE PELÍCULA

Todos estamos acostumbrados a las escenas de las películas sobre tecnología: robots espías, drones, cámaras que nos siguen a todas partes, imágenes satelitales detalladas, etc. Llega un momento en el que asimilamos todo esto a un mundo de fantasía, creado para entretener y no para asustar.

La imagen romántica del hacker, un nerd con problemas de sobrepeso, grasa en el pelo y poca vida social, llega incluso a generar algo de simpatía por estos excluidos de la vida.

Pero, mucha de esta fantasía es copiada de la realidad. No debemos pensar que estamos a salvo de esos sofisticados ataques solo porque habitamos en un lugar considerado pobre, del tercer mundo, al cual ningún hacker en sus cabales se animaría a atacar, dada nuestra extrema miseria.

Lamentablemente, no todos los siniestros magos de la tecnología son iguales; y algunos viven y actúan precisamente entre nosotros, trabajando a una escala menor que la que vemos en Hollywood. Veamos un caso.

"No debemos pensar que estamos a salvo de esos sofisticados ataques solo porque habitamos en un lugar considerado pobre, del tercer mundo"

En una empresa mediana, de las muchas que en nuestro país dependen de la tecnología para conectar a sus empleados con las bases de datos de la sede central, se habilitaron los sistemas de tal forma que algunos de los colaboradores pudieran conectarse de manera remota a la red de la empresa y acceder a sus archivos y programas. Esta facilidad permite optimizar el tiempo de trabajo y evita la necesidad de estar físicamente en la sede de trabajo o cargar con gran cantidad de información en condiciones inseguras. El sistema funcionaba adecuadamente y los empleados hacían uso frecuente de esta herramienta tecnológica, con los esperables problemas de conectividad que se suelen presentar a veces.

Fuente I http://danielcastellanosm.blogspot.com.co/

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/

Un día, los empleados comenzaron a llamar a la Mesa de Ayuda del área de Sistemas de la empresa, a quejarse porque no podían acceder a sus bases de datos. Prontamente, el encargado de solucionar este tipo de situaciones se puso al frente, tratando de identificar y resolver el asunto con la mayor celeridad posible.

Luego de varias horas de estar intentando de forma infructuosa todas las posibles soluciones, seguía sin poder acceder al servidor y a la información contenida en el mismo. En ese momento, recibió en su correo un e-mail en donde unas personas le comunicaban que su empresa había sido atacada, que toda la información había sido encriptada por ellos; y que exigían el pago de una elevada cantidad de BITCOINS, la moneda virtual de moda, a cambio de desencriptar la información.

El ingeniero de sistemas ya se había imaginado que algo similar era el problema que tenía, por lo que procedió a responder el e-mail, tratando de establecer comunicación o de rastrear a los autores del mismo; obviamente sin resultados positivos. Como último recurso, les pidió garantías de que ellos efectivamente cumplirían su palabra una vez recibido el pago y liberarían la información. Su respuesta fue la típica de un extorsionista: tiene que confiar en nosotros. Además, si no nos paga, la vamos a publicar como ocurrió con los famosos papeles de Panamá.

Horas más tarde, en la dependencia de la Fiscalía en donde le recibieron la denuncia, el funcionario la manifestó que no era el primer caso en esa semana; y que poco o nada podían hacer ellos, por falta de conocimiento sobre el tema.
Esto está ocurriendo en nuestro país, no en su televisor. Las personas que manejan los sistemas y equipos de procesamiento de datos de las empresas tienen la obligación de entender que la seguridad de los mismos depende en gran medida de las precauciones que ellos tomen al momento de conectarse, tanto como al usar, cambiar y guardar sus claves de acceso.

Como primera medida, debe entenderse que estos equipos se ponen a disposición del empleado para el desarrollo del objeto social de la empresa y que NO se debe almacenar ninguna información personal en los mismos, no solo porque ello constituye un abuso de los recursos de la empresa, sino también para garantizar que su información íntima no vaya a ser hurtada en un ataque contra la empresa.

Las claves deben ser cambiadas de manera periódica y no pueden ser predecibles, como la fecha de cumpleaños o el nombre del cargo o del hijo mayor. Los accesos desde cafés internet, aeropuertos o sitios públicos son vulnerables. Los firewall y otros mecanismos ayudan a proteger la información, pero distan de ser 100% seguros. Por último, las copias de seguridad no pueden consistir en un disco externo que el gerente o el jefe de Sistemas se llevan para la casa de vez en cuando. Se requiere de una verdadera estrategia para copiar de manera regular los datos, y que el medio magnético utilizado para dicha copia se guarde en condiciones de humedad relativa, temperatura y seguridad física aceptables.

Contar con una copia de la información y de los programas que se utilizan, protege a la empresa contra este tipo de amenazas, limitando la cantidad de daño que los delincuentes puedan hacer.