Protege a tu empresa del ransomware

Los **ataques ransomware y robo de datos crecen exponencialmente**. Tan solo entre 2016 y 2017 se sumaron más de 80 mil ataques, según datos presentados durante la Séptima Cúpula Latinoamericana de Analistas de Seguridad, siendo **Brasil el país más afectado, seguido de México.**

"Para tener una idea más clara de lo que fue ese crecimiento, hubo un aumento de dos mil por ciento en el número de ataques, habiendo presentado los dos peores casos de ransomware: el **NotPetya y WannaCry**", aseguran analistas de Comstor en un documento de prensa.

Para la compañía de seguridad, colaboración, networking y centro de datos, la **predilección de los cibercriminales por el uso del ransomware** es prueba de que sigue siendo muy exitoso.

"**En 68 por ciento de los casos de ataque con este malware, tardaron meses o más que eso para ser descubiertos**, a pesar de que 87 por ciento de éstos tienen algún tipo de dato comprometido en minutos. Otra razón muy importante para el crecimiento de estos ataques es justamente el hecho de que muchas de las herramientas necesarias para realizarlos se encuentran en la **Dark Web**, con fácil acceso para muchos hackers", se agrega en el documento.

Los especialistas afirman que 65 por ciento de las empresas que fueron alcanzadas, sufrieron una pérdida severa de datos o no consiguieron más ingresar a sus archivos.

Para evitar un ataque de ransomware, los líderes de TI y seguridad de la información, según Comstor, recomiendan:

1.– Mantener en orden y bien ubicados los inventarios de todos tus activos digitales, para identificarlos con facilidad en una etapa crítica.

2.– Actualizar constantemente todos los software, sistemas operacionales y aplicaciones.

3.– **Hacer un respaldo de toda la información** en forma diaria, incluyendo datos sobre dispositivos de colaboradores, para que puedas restaurar datos criptografiados si fuese atacado.

4.– Utilizar un local externo y seguro para los respaldos de información.
5.– Segmentar tu red: no coloques todos los datos en un conjunto de archivos ingresado por todos en la empresa.

6.– Entrenar al equipo en prácticas de seguridad cibernética, enfatizando la no apertura de anexos o links de fuentes desconocidas.

7.– Desarrollar una estrategia de comunicación para informar a los colaboradores si un virus llega a la red de la empresa.

8.– Antes de que ocurra un ataque, trabaja con tu jefe(a) inmediato(a) para determinar si tu empresa pagará un rescate o iniciar una investigación.

9.– Realizar un análisis de amenazas en la comunicación con los abastecedores para verificar la

seguridad cibernética durante todo el ciclo de vida de un determinado dispositivo o aplicación.

10.– Instruye a los equipos de seguridad de la información para realizar pruebas de penetración con el fin de encontrar vulnerabilidades.