Emite CTPAT boletín de alerta por Ransomware

En el mes de julio de 2021, la Customs and Border Protection (CBP) emitió, a través de su portal de CTPAT, el boletín "Ciberseguridad – Detener el Ransomware" con el fin de comunicarle a los miembros del programa que, debido al aumento de casos de ransomware, el gobierno de Estados Unidos de América ha creado un nuevo sitio web en donde las organizaciones pueden conocer herramientas para protegerse de estos incidentes de seguridad.

El ransomware o secuestro de información es el delito de modificar los datos de los archivos almacenados en un dispositivo a un lenguaje no legible convirtiéndolos en inútiles, así como a lo que los sistemas y software empresariales que utilizan estos archivos para su funcionamiento. Una vez que los datos son obsoletos para la empresa, los grupos delictivos solicitan un rescate monetario para poder revertir los cambios realizados a los archivos con la amenaza de destruirlos permanentemente o liberar los datos en la red.

La página que ha creado el gobierno estadounidense es StopRansomware.gov, la cual ofrece recursos y alertas de ransomware con el fin de brindar a los interesados una orientación sobre la protección, detección y respuesta ante el ransomware. En dicha página, los usuarios pueden acceder a reportes y recursos de distintas instituciones del gobierno americano como lo son la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) del Departamento de Seguridad Nacional de Estados Unidos, la Oficina Federal de Investigaciones (FBI), entre otras instituciones.

Adicionalmente, se publicó una carta por parte del gobierno de los Estados Unidos dirigida al sector privado, en donde se menciona la gravedad del secuestro de información, así como ha afectado a distintas organizaciones alrededor del mundo, como hospitales en Irlanda, Alemania y Francia, así como bancos en Reino Unido.

En dicha carta, el gobierno americano ha compartido una serie de buenas prácticas que los usuarios pueden realizar para evitar caer en un secuestro de información. Los usuarios deben de contar con autentificadores multi factores al momento de acceder a sus cuentas empresariales, así como contar con softwares para la detección de actividades maliciosas en la red y las bloquee. Realizar encriptación de los datos para que, en caso de que sean robados, no puedan ser utilizados y contar con un equipo de sistema de seguridad quien apoye rápidamente en caso de detectar una nueva amenaza.

Asimismo, se les recomienda a los usuarios realizar copias de seguridad de forma constante de los datos y configuraciones, y someterlas a prueba con frecuencia. Es importante que las copias de seguridad no se encuentren conectadas a la red de la empresa para evitar que sean secuestradas en caso de acceder a esta.

También es necesario que los usuarios actualicen constantemente sus sistemas y, en caso de alguna vulnerabilidad detectada, hacer las reparaciones pertinentes lo más pronto posible. Otra buena práctica que puede ser implementada por los usuarios es contar con un plan de contingencia de incidentes cibernéticos y ponerlos a prueba para verificar su efectividad.

Igualmente, se les recomienda a las empresas que comprueben su sistema de seguridad a través de un tercero para verificar su seguridad de los sistemas y su habilidad para defenderse de un ataque cibernético.

Por último, se recomienda segmentar las redes de las empresas de forma que los archivos administrativos y los operacionales no se encuentren en la misma red y pueda seguir funcionando en caso de que una de estas se vea comprometida.

Fuente: División de Certificaciones OEA y C-TPAT, TLC Asociados

Atentamente:

Octavio de la Torre de Stéffano

Vicepresidente de cumplimiento en comercio exterior y aduanas en CANACINTRA Tijuana.

Alan Padilla Castellanos

Coordinador de Comités de trabajo en cumplimiento en comercio exterior y aduanas.