Información sobre ataque a un Participante del SPEI en octubre

Banco de México

Noviembre, 2018

BANCO DE MÉXICO

1. Resumen del incidente

2. Acciones para contener el incidente

3. Comunicación con el público

1. Resumen del incidente

- El 22 de octubre, con base en elementos detectados en el monitoreo del funcionamiento del sistema financiero, el Banco de México solicitó a los participantes de los sistemas de pagos mantener los niveles de alerta, esquemas de vigilancia, procesos de conciliación de operaciones y esquemas para detectar cualquier anomalía que pudiera presentarse en su operación con los sistemas de pagos.
- El 23 de octubre una entidad no bancaria participante en el SPEI reportó inconsistencias en la conciliación de sus cuentas de tesorería con propósitos de pago.
- Si bien las investigaciones aún están en curso, la información preliminar apunta a que se trata de un ataque dirigido al aplicativo que utilizaba la institución afectada para conectarse al sistema SPEI, similar al modus operandi de los eventos que presentaron algunos participantes durante los meses de abril y mayo.
- Conforme a la información proporcionada por la institución afectada, los recursos vinculados por el incidente fueron 160 operaciones por un monto de alrededor de 60 MDP que habían salido de su aplicativo SPEI hacia otros participantes.
- De acuerdo a la información disponible no hay indicios de que los recursos de los clientes del sistema financiero se hayan visto afectados.
- De igual forma que en los eventos registrados en abril y mayo, el sistema central del SPEI, que opera el Banco de México, no se vio afectado y no fue blanco de ningún ataque.

2. Acciones para contener el incidente

- Con base en los lineamientos que el Banco de México ha emitido para mitigar riesgos a los participantes y usuarios del sistema financiero, el 23 de octubre se activaron todos los protocolos de seguridad, para minimizar potenciales afectaciones.
- De acuerdo al protocolo de reacción diseñado para eventos con estas características, se elevó el nivel de alerta a rojo y se identificaron elementos de riesgo que pudieran resultar comunes a otros participantes del SPEI, con base en lo cual se les requirió a 18 participantes, en adición a la institución afectada, a operar a través de un mecanismo alterno. En particular, se requirió a esas instituciones que para operar a través del SPEI, debían realizar las acciones necesarias para conectarse mediante el esquema alterno para hacer transacciones en el referido sistema (COA-SPEI).
- Si bien la medida señalada reduce los riesgos al tratarse de una infraestructura distinta a la que se ha visto afectada, por tratarse de un esquema de operación semiautomático, hace que las transferencias no se envíen y/o abonen en tiempo real, por lo que los niveles de servicio pudieran verse afectados.

3. Comunicación con el público

- El 23 de octubre el Banco de México, en conjunto con CNBV y SHCP, informaron a través de un comunicado publicado en Internet, entre otras cosas, el evento que reportó una institución sobre inconsistencias en la conciliación de su cuentas de tesorería con propósitos de pago, que se elevaba el nivel de alerta de seguridad informática a rojo y que como medida precautoria a las instituciones con el mismo nivel de riesgo se les requirió operar en contingencia.

- El Banco de México ha continuado actualizando diariamente la información operativa del SPEI, entre la que se incluye el número y proporción de operaciones que actualmente se están operando mediante mecanismos alternos, la cual puede ser consultada en el micro sitio del SPEI, ubicado en la siguiente liga:

http://www.banxico.org.mx/spei/informacion-importante-situac.html


BANCO DE MÉXICO
www.banxico.org.mx