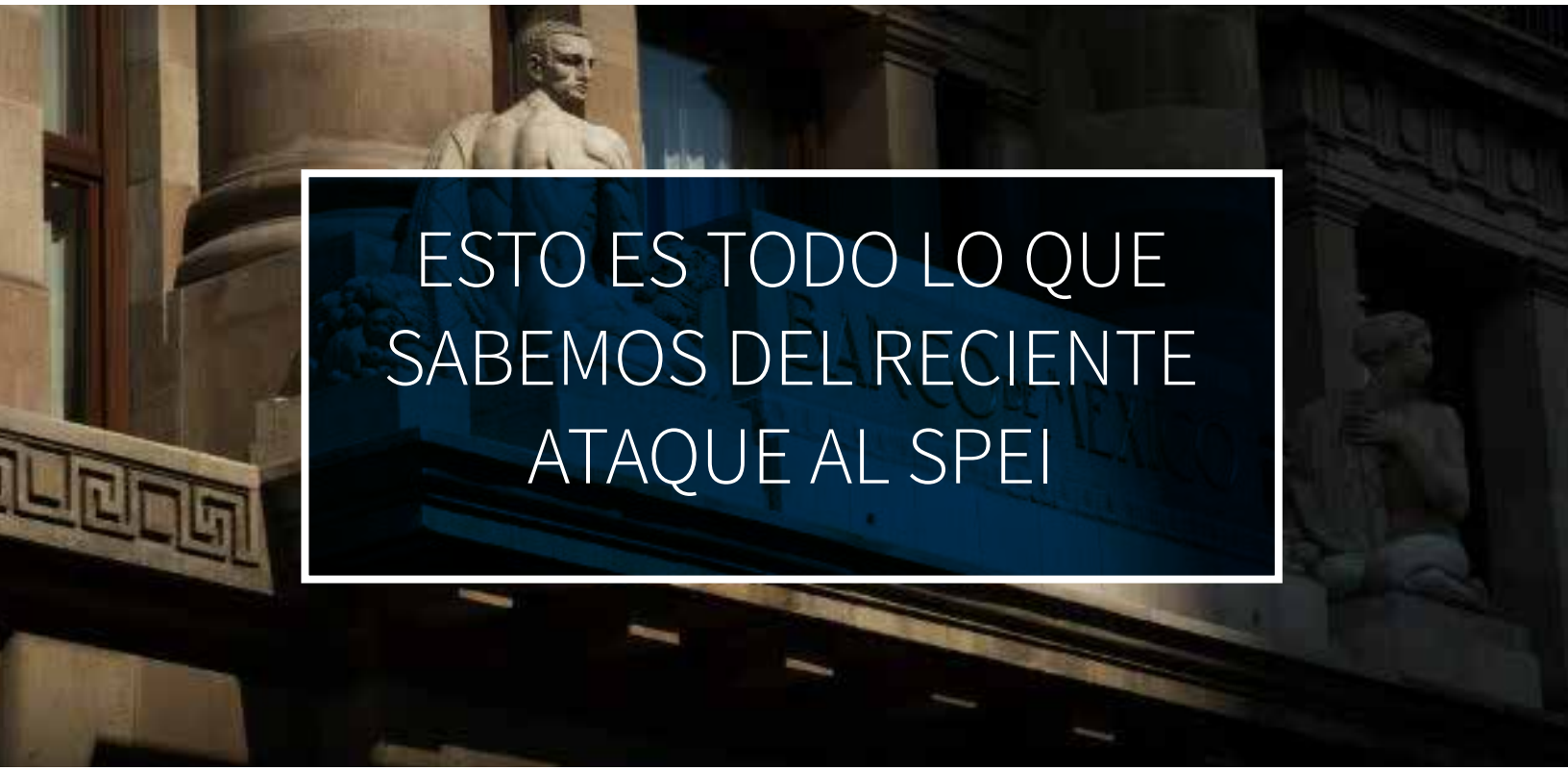
Managed secure IT | no matter what



ESTO ES TODO LO QUE SABEMOS DEL RECIENTE ATAQUE AL SPEI

Un grupo aún desconocido de cibercriminales, robó entre 300 y 400 millones de pesos de cinco importantes instituciones bancarias mexicanas mediante cuentas falsas y transacciones no autorizadas.

El modus operandi

El ataque, cuya naturaleza aún no se conoce del todo, fue dirigido a la plataforma digital que conecta a los bancos con el Sistema de Pagos Electrónicos Interbancarios que transfiere dinero entre bancos y asegura el flujo de dinero para el pago de nóminas y la transferencia de fondos entre usuarios.

Desde los bancos afectados, los ciberdelincuentes enviaron órdenes para mover dinero a cuentas falsas en otras instituciones bancarias para, posteriormente, dejar que otros cómplices sacaran el dinero en efectivos desde docenas de sucursales de todo el país para evitar levantar sospechas.

Se cree que el dinero sustraído en cada transacción fue de entre 70 y 100 mil pesos y que esta operación manual se llevó a cabo a lo largo de varias semanas por distintos delincuentes.

Las autoridades tampoco descartan que los retiros se hayan hecho con ayuda del personal de algunos bancos.

¿Cuántos bancos resultaron afectados?

De acuerdo a autoridades de Banxico, al menos cinco bancos sufrieron la sustracción ilegal de fondos. Entre los más importantes destacan Citibanamex, que al principio negó que los problemas con sus transacciones electrónicas fueran consecuencia del ciberataque; Banorte, el único banco en notificar a las autoridades y a sus usuarios que se había convertido en víctima de hackers, y BanBajío.

Además de estos bancos, Banxico reportó que al menos una casa de bolsa resultó afectada por el ataque, pero que el robo millonario, a pesar de los estragos que provocó, pudo contenerse en la medida de lo posible.

¿El dinero de los cuentahabientes resultó afectado?

Si bien Banxico ya aclaró que el dinero de los cuentahabientes no está en peligro y que son los bancos los que tienen que reponer cualquier cantidad que se haya perdido por este importante ataque a la banca mexicana, el evento nos deja algunas lecciones que todo CIO debería tomar en cuenta al momento de proteger los assets más importantes de la empresa o negocio para el que trabaja.

El dinero robado le pertenece a las entidades bancarias afectadas y solo a estas. Los ahorros de las personas y sus nóminas permanecen intactas.

Security

¿Qué permitió que se llevara a cabo el robo?

La carencia de información respecto a la escala real del ataque (aún se desconoce a ciencia cierta cuánto fue robado y a dónde fue a parar), deja en claro que aún falta mucho por hacer para proteger los protocolos de seguridad de las instituciones bancarias y las empresas pues así como sucedió con SPEI, un ataque como el que sufrió recientemente, pudo haberle sucedido a una empresa o negocio de cualquier escala.

La falta de monitoreo en la forma en la que el dinero es transferido de SPEI al software de cada banco creó varios agujeros de seguridad que acabaron siendo explotados por los hackers que robaron el dinero.

El ataque se registró en la aplicación que usan tres proveedores que comunican a las cinco instituciones bancarias afectadas con la plataforma de Banxico, así que habría que revisar exactamente cómo se pudieron explotar sus fallas y quién estuvo a cargo de su blindaje digital.

La falla en la comunicación entre los bancos y sus usuarios también evitó que Banxico actuara eficazmente para contrarrestar el ataque. Afortunadamente, el artículo transitorio vigésimo octavo del reglamento del SPEI, que entrará en vigor el próximo 29 de junio, hará obligatorio que “en aquellos casos en que la infraestructura tecnológica de un participante presente un evento que afecte los servicios relacionados con el SPEI que preste a sus clientes, los participantes deberán notificar a sus respectivos clientes afectados”.

¿Qué se hizo para contener el ataque?

Por el momento el Banco de México (Banxico), recomendó a los bancos afectados usar un sistema de emergencia que se activa solo durante emergencias de alto impacto, para evitar la demora de pagos de nómina y la pérdida de dineros entre transferencias electrónicas de fondos.

Banxico también ordenó que las transferencias mayores a 50 mil pesos sean validadas por los bancos y que el usuario que quiera extraer esa cantidad en ventanilla, no obtenga más de esta cifra por día.

¿Qué lecciones se aprendieron del robo millonario?

Tras el ataque, se inauguró la nueva dirección de ciberseguridad que se encargará de evitar que un robo millonario de la magnitud del más reciente, vuelva a suceder.

Este organismo trabajará junto a la Coordinación de la Información y de Sistemas, así como la gerencia de seguridad de Tecnologías de la Información y la dirección general de Tecnologías de la Información del Banxico.

El Banco de México también dijo que reformaría su reglamento interior para, de nueva cuenta, reforzar la seguridad de sus procesos y blindar los sistemas con los que funciona SPEI.

Por ende, quedó en claro que un monitoreo de seguridad mucho más férreo deberá establecerse para que todas las instituciones y proveedores que quieran conectarse al sistema de pagos electrónicos del Banco de México, se adecúen a los nuevos protocolos de blindaje digital.

Síguenos en nuestras redes sociales:

MexisMX

Servicios Administrados Mexis, S.A. de C.V.

Mexis TI

Servicios Administrados Mexis, S.A. de C.V.