

REFORMA

EL NORTE

MURAL

Denuncian sólo 10% de ciberdelitos

IMPRIM

Jessika Becerra
(26-febrero-2019).-

Sólo 10 por ciento de las investigaciones por ciberdelitos a empresas financieras y de otros sectores llegan a instancias legales, declaró Andrés Velázquez, presidente de Mattica, una empresa dedicada a estudios tecnológicos forenses que trabaja con bancos. El experto forense explicó, en un seminario sobre seguridad financiera, que la mayoría de las empresas que han sufrido ataques a sus sistemas se resisten a presentar denuncias porque temen afectar su reputación.

Además de desconocer el proceso, consideran que les llevará mucho tiempo, y que son insuficientes las pruebas que pueden presentar en su defensa.

"No hay muchas sentencias de vulnerabilidad a los sistemas de información porque se requieren elementos de prueba y casi no los hay", mencionó el presidente de Mattica.

Velázquez agregó que las investigaciones sobre los últimos ciberataques en el sistema financiero (a la Afore Invercap y CI Banco) mostraron la red desde donde se vulneró al sistema, pero no el lugar donde estaba el hacker.

CI Banco informó que el pasado 12 de febrero detectó un virus en el equipo de uno de sus empleados, mientras que el 8 de febrero se ubicó un intento de ataque a los sistemas de una sucursal de Querétaro de Afore Invercap. En ambos casos se activaron los protocolos de seguridad.

El experto destacó que los ataques más frecuentes usan Ransomware, un código malicioso que ingresa a servidores, al internet de las cosas o al móvil para impedir su uso hasta que el afectado pague un rescate y que va en aumento en las empresas mexicanas.

Detalló que la mayoría de los ataques con Ransomware se realizan desde el exterior, ya que sólo se han detectado dos bandas en México, dedicadas a atacar al sistema financiero.

"En Invercap y en CI Banco les cayó Ransomware, y se filtró información de los empleados, un mecanismo que puede ser un distractor para realizar un ataque mayor. Tenemos el precedente de Bancomext", indicó.

En enero del 2018, una banda de ciberdelincuentes norcoreanos intentó robar 110 millones de dólares al atacar los sistemas de Bancomext.

Aunque declinó de dar el nombre de la empresa afectada, Velázquez indicó que el mayor hurto al sistema financiero mexicano fue por 160 millones de pesos a una institución financiera donde el robo se realizó en 15 minutos.

"Fue desde internet y no hubo ninguna colaboración interna en la mayoría de las operaciones", afirmó.

Asimismo, el analista advirtió que seguirán los ataques al sistema financiero y que 30 por ciento de los eventos detectados corresponden a este sector.

La segunda forma de ataque más frecuente proviene de empleados que roban la información para compartirla con la competencia o a quien le sea de utilidad.

En tanto, la extorsión y la pornografía infantil ocupan las siguientes posiciones.

"Los ciberatacantes buscan obtener beneficios económicos o información personal y es contraproducente si las empresas no averiguan qué sucedió, porque entonces les vuelve a pasar", aseguró.

El experto advirtió que la información guardada en proveedores de nubes también son vulnerables, ya que pueden ser atacadas para copiar la información que guardan.

Finalmente, Velázquez mencionó otros mecanismos utilizados recientemente para defraudar a las empresas como hacerse pasar por un proveedor que solicita que sus pagos se realicen en una nueva cuenta bancaria.

Otro mecanismo de fraude es el envío de correos a directores de Finanzas donde se les pide liberar pagos para cubrir ciertos servicios, y si los directivos no confirman la

legitimidad de esa solicitud, caen en la trampa. Copyright © Grupo Reforma Servicio Informativo