Los desafíos en la detección contra el fraude financiero

El progreso de las nuevas tecnologías da apertura a un campo de acción más amplio para que se presente el fraude financiero. Las empresas tienen información con un generoso volumen de contenidos que deben ser procesados a través de la implementación de tecnologías que hacen parte del periodo y la detección de la ilegalidad.

Hay dos variables muy importantes a considerar, según los especialistas de DigiCert: los consumidores; su identificación, tarjetas de crédito, tarjetas de descuento, etc. y los canales de comunicación para hacer transacciones como las aplicaciones web, terminales, cajeros automáticos, puntos de venta, etc. Toda esta información va a ir una aplicación multicanal que se encarga de realizar todas las transacciones.

"Los bancos, cooperativas de crédito y otras instituciones financieras son los **principales objetivos de los ataques de phishing y otras estafas dirigidos al robo de identidad dentro del ámbito financiero.** Por tanto, es primordial brindar la importancia necesaria a los **certificados TLS de alta seguridad y PKI para proporcionar un cifrado y una autenticación de identidad** que son vitales para las transacciones comerciales en la web.

"Para ello DigiCert innova y trabaja para avanzar en soluciones basadas en SSL y PKI, para asegurar a las empresas y los mercados emergentes con el IoT, la nube y DevOps, respaldando sus necesidades con s**oluciones de seguridad avanzadas y basadas en PKI** que escalan y ahorran costos", afirmó Manuel Pavón, gerente de Canales para América de DigiCert.

Ahora las compañías no solo se deben preocupar por la protección de elementos internos y físicos en la organización, sino tener en cuenta la variable de la tecnología y el aumento de los puntos de ataque. **Los fraudes cada vez se vuelven más técnicos, especializados**, difíciles de entender y de detener.

Consejos

Los empresarios del sector bancario y financiero se enfrentan diariamente con retos en sus plataformas tecnológicas transaccionales de compra en línea y pagos, que están en alto riesgo de ciberataques y movimientos fraudulentos.

"Algunas recomendaciones para brindar un sistema de seguridad reformada son las siguientes. La tecnología adaptarse a la compañía. Las empresas hoy en día tienen que adecuarse a los clientes para así obtener un óptimo rendimiento económico. Se deben instaurar técnicas tecnológicas de prevención para la operación eficiente", asegura Pavón.

Explica que hay que conocer a la compañía y su funcionamiento, lo cual es primordial en este proceso. Tener en cuenta cuáles son los modelos y procesos normales del día a día. Aspectos como el número de transacciones y conductas que están dentro del rango normal dentro de la empresa.

"Conglomerar toda la información dentro de una plataforma que no sea rigurosa, que permita ser

movible y trabajada con tener múltiples conectores y tener procesos y técnicas de expansión y preparación de información. Reubicar la mayor cantidad de información donde se trabajan estos contenidos en la organización", agregó.

Además, se señala que el perfil de los usuarios es vital. Esto permitirá identificar las tendencias y valores de compra, si compra más en determinados periodos de tiempo, si estos montos de compra son normales en el usuario, etc. Esto genera una mayor alerta y respuesta a ciertos procesos de fraude con un mayor rango de cobertura.