MOTORES DE RIESGO TRANSACCIONALES ¿Solución eficaz para reducir agresivamente el fraude electrónico?

Sarmiento Martínez Cesar Arturo.
Sarmiento892@hotmail.com
Universidad Piloto de Colombia.

Resumen—En este artículo se mostrará una descripción general de cómo los motores de riesgo transaccional, pueden ayudar a reducir las cifras de fraudes electrónicos en el sector financiero a nivel mundial, a partir de un algoritmo de aprendizaje que sea capaz de evaluar desdeuna serie de entradas variables, un patrón de operación, que permita identificar el perfil de usuario, y así validar la autenticidad de quien realiza la transacción.

Índice de Términos—riesgo transaccional—fraude electrónico—autenticidad.

Abstract—This article provides an overview of how engines will display transactional risk , can help reduce the numbers of electronic fraud in the financial sector worldwide , from a learning algorithm that is able to assess from a series variable inputs, a pattern of operation to identify the user profile , and thus validate the authenticity of a transactor .

Index Terms- risk transactional - fraud – authenticity.

I. CONDICIONES NECESARIAS PARA QUE UNA ACTIVIDAD SEA CONSIDERADA COMO UN FRAUDE ELECTRÓNICO

Para que un evento o actividad sea considerada como un fraude electrónico, es necesario que se cumplan una serie de condiciones que permitan establecer la actividad como ilegal, para ello debe existir:

- Un elemento de engaño o de información alterada, modificada o incompleta, que una vez es emitida a la víctima[1] mediante el engaño, busca inducirla a publicar o entregar información transaccional valiosa[2]y de carácter personal.

- Una dimensión y un alcance económico considerable, y determinado en la mayoría de los casos según la normativa de la nación.

- La utilización de sistemas comerciales lícitos, dándole una utilización indebida o comprometiéndolos de tal manera que a partir de ello se genere una pérdida de valor.

II. TÉCNICAS MÁS UTILIZADAS PARA LA EJECUCIÓN DEL FRAUDE ELECTRÓNICO

Las técnicas más utilizadas son el Phishing, el Smishing, el Vishing y el Malware.

- Phishinges una técnica mediante la cual los delincuentes suplantan la página Web de la entidad, envían correos electrónicos o genera una ventana emergente invitando al cliente a ingresar a la página e ingresar sus datos financieros o la autenticación de la cuenta. Sobre la página fraudulenta, el delincuente captura la información del cliente y la almacena para su uso fraudulento

[1] Persona natural o jurídica que se ve afectada intencionalmente en un fraude
[2] Información necesaria para transar electrónicamente

que puede utilizar directamente o vender a otros delincuentes informáticos.

- Smishing es una práctica en la que los delincuentes hacen uso de los mensajes de texto de los celulares y la ingeniería social para engañar a las personas y obtener información financiera o información útil para el robo de identidad.[1]

- Vishing es una técnica similar al Phishing, pero que busca engañar a la víctima no de forma visual sino auditiva a partir de llamadas telefónicas.

- Malware o software espía, es una modalidad en la que los delincuentes monitorean las actividades del usuario del computador, mediante cualquier programa generado con intenciones de dañar, controlar o sacar provecho de las computadoras que están infectadas.

III. ACCIONES QUE PUEDEN AYUDAR A IDENTIFICAR O CLASIFICAR UNA TRANSACCIÓN COMO FRAUDULENTA

1. Monto de la orden de compra elevada: Quien compra con una tarjeta robada o con información de tarjetas de crédito obtenidas de fuentes ilícitas no se preocupa por comprar poco porque simplemente no será quien pague por el pedido.

2. Desinterés por el precio: Nuevamente, como el comprador fraudulento sabe que nunca abonará por lo que compró, no tiene problemas en abonar un producto más caro que en otra tienda online o pagar recargos por intereses de financiación o gastos de envío express.

3. Tiempos de entrega cortos: La idea del comprador fraudulento es cerrar la operación con urgencia. Antes de que el titular real de la tarjeta detecte una compra que nunca hizo, el comprador fraudulento ya se hizo de la mercadería.

4. Información de contacto inconsistente:- Números de teléfonos incorrectos.- Números de teléfono en dónde nadie responde, y que no coinciden con la ubicación geográfica desde donde se realizó la compra.

IV. INTERVENCIÓN INTERNACIONAL PARA IDENTIFICAR Y CONTRARRESTAR EL FRAUDE ELECTRÓNICO

Desde el año 2002, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional CNUDMI[3]"empezó a examinar el problema de las prácticas fraudulentas, que tenía repercusiones económicas muy negativas en el comercio mundial y para las instituciones comerciales que operaban legalmente.

Gracias a una serie de consultas con expertos y altos funcionarios públicos acostumbrados a afrontar y a combatir el fraude comercial y que eran exponentes de diferentes regiones, perspectivas y disciplinas.

La CNUDMI adquirió conciencia de la presencia generalizada del fraude comercial y de su considerable impacto en el plano mundial, independientemente del grado de desarrollo económico o del sistema de gobierno de cada país.

Al examinar las posibles respuestas a esta amenaza, se consideró que la educación y capacitación podían ser medios importantes para prevenirla, y que la especificación de señales e indicadores comunes de peligro de fraude comercial podían ser especialmente útiles para combatirlo."[2]

V. CIFRAS PARA COLOMBIA

"De acuerdo con el estudio realizado por ***TheEconomistIntelligenceUnitpara Kroll ,***una empresa de inteligencia empresarial,

[3] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

titulado ***Global FraudReport,*** Colombia ocupa el segundo puesto en los países más victimizados por el fraude, sólo detrás de China y por delante de Brasil.

El estudio de Kroll establece que el fraude y el hurto de información por primera vez en la historia han superado los otros tipos de fraude en el mundo, y dice que "*el 94% de los negocios colombianos sufrió algún fraude en el último año, en comparación con el 88% global"*.

El 21% está en la categoría de fraudes electrónicos, que incluyen hurto de información y ciber ataques a sitios web e infraestructura de las empresas."[3]

VI. ¿QUÉ ES UN MOTOR DE RIESGO TRANSACCIONAL?

Un motor de riesgo transaccional es una tecnología relativamente nueva en el mundo, orientada principalmente a la disminución del fraude electrónico en el sector financiero, que surge como una necesidad inminente ante el gran crecimiento de delitos informáticos y la tendencia cada vez mayor de la banca móvil y el comercio WEB.

VII. BENEFICIOS DE UN MOTOR DE RIESGO TRANSACCIONAL

1. Reducción de fraudes electrónicos.
2. Equilibra seguridad VS usabilidad.
3. Inspira seguridad en los usuarios.
4. Es una solución pensada a futuro, lo que hace que sea sostenible en el tiempo.
5. Deja de lado el modelo de seguridad, en el que la seguridad del sistema se basaba en la confidencialidad de los datos transaccionales como usuario y contraseña.
6. Es fácilmente adaptable con las tecnologías existentes, lo que hace que no sea un remplazo sino una adición al entorno de seguridad.
7. Es una solución única para todas las unidades de negocio sin importar distancias geográficas.
8. Evita impactar innecesariamente a usuarios genuinos.
9. Brinda una seguridad adaptable por usuario, lo que hace que cualquier cliente encaje de manera personalizada.

VII. ¿CÓMO FUNCIONA UN MOTOR DE RIESGO TRANSACCIONAL?

El motor de riesgos transaccional funciona asignando un score[4] o puntuación de riesgo a cada transacción a partir de variables de entrada que con el tiempo van retroalimentando[5] el aprendizaje del motor, para que este sea capaz de evaluar y asignar tanto la puntuación como el control que se requiere para la autorización de la misma.

En los casos en que el score asignado indica que se debe parar la transacción en línea y realizar una validación.

Las variables de entrada para la evaluación son:

- **Historia transaccional del cliente:**En la historia transaccional del cliente se tienen en cuenta factores como rutinas de pagos efectuadas, fechas en las que se realizan pagos normalmente, montos[6]cotidianos, y las tendencias transaccionales que el usuario presenta, y que han sido aprendidos por el motor de riesgo en una fase inicial de estudio en el cual el mismo no toma decisiones hasta no tener criterios suficientes de rutinas.

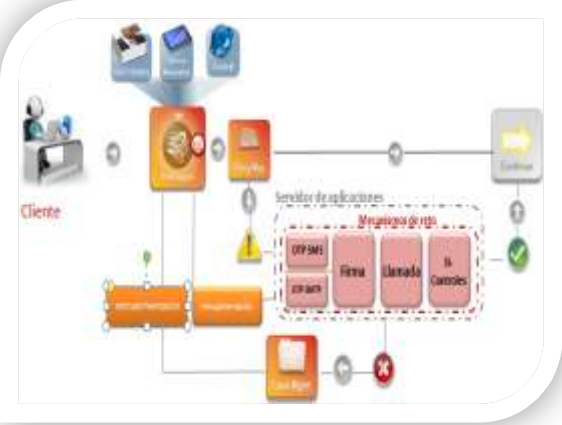
- **Reputación del dispositivo:**La reputación del dispositivo, se evalúa a partir del registro de las direcciones IPs desde donde

[4]Puntuación obtenida después de una evaluación.
[5] Proceso mediante el cual las transacciones, son incluidas en el motor para que este realice el aprendizaje del comportamiento transaccional del cliente, necesario para tomar decisiones y asignar un score acertado.
[6] Topes máximos establecidos por el cliente

normalmente el cliente transa, además de ello se alimenta en tiempo real con las listas negras de mayor confianza.

- **Contexto transaccional:**El contexto transaccional evalúa factores como la ubicación geográfica desde donde se está transando en comparación con las que normalmente efectúan actividad para el usuario y valida si existen cambios considerables que puedan generar una alerta.

Así mismo evalúa el tipo de transacción a realizar, el perfil transaccional del usuario y las restricciones que el mismo usuario haya podido configurar previamente en su entidad financiera, como topes monetarios, número máximo de transacciones, fechas de pagos cotidianos, etc.…



Gráfica 1: diseño estructural del motor de riesgo, elaborado por el autor del documento. [4]

A partir de una validación en donde se comparan los datos iníciales de entrada, con algoritmos de aprendizaje automáticos de comportamiento propios del motor, se definen los controles necesarios para autorizar la transacción.

Cuando el score asignado por el motor a partir de la correlación y el análisis de las variables de entrada da como resultado un comportamiento "normal" según los criterios estipulados en las políticas de cada entidad financiera, la transacción no requerirá de una autorización extra, por tal motivo la misma pasara en línea[7] y no será necesario realizar un reto evidente [8]al usuario.

Mientras que para los casos en que después de realizar la evaluación de las variables de entrada y el algoritmo de aprendizaje del motor, den como resultado un score clasificado como "alto", se requerirá sacar la transacción de línea y esperar a una validación por medio de un segundo factor de autenticación, que permita garantizar la autenticidad de quien está ejecutando la transacción y autorice la misma para que pueda proseguir, en estos casos y según el score obtenido, los controles necesarios irán variando desde los más básicos hasta los más complejos.

IX. TIPOS DE CONTROLES

A partir de una validación en donde se comparan los datos iníciales de entrada, con algoritmos de aprendizaje automáticos de comportamiento propios del motor, se definen los controles necesarios para autorizar la transacción.

Cuando el score asignado por el motor a partir de la correlación y el análisis de las variables de entrada da como resultado un comportamiento "normal" según los criterios estipulados en las políticas de cada entidad financiera, la transacción no requerirá de una autorización extra, por tal motivo la misma pasara en línea[9] yno será necesario realizar un reto evidente [10]al usuario.

Mientras que para los casos en que después de realizar la evaluación de las variables de entrada y el algoritmo de aprendizaje del motor, den como resultado un score clasificado como "alto",

[7] Transacción en línea hace referencia a un curso de la misma en tiempo real.
[8] Reto evidente, hace referencia a una serie de preguntas personales que buscan comprobar la autenticidad del usuario.
[9] Transacción en línea hace referencia a un curso de la misma en tiempo real.
[10] Reto evidente, hace referencia a una serie de preguntas personales que buscan comprobar la autenticidad del usuario.

se requerirá sacar la transacción de línea y esperar a una validación por medio de un segundo factor de autenticación, que permita garantizar la autenticidad de quien está ejecutando la transacción y autorice la misma para que pueda proseguir, en estos casos y según el score obtenido, los controles necesarios irán variando desde los más básicos hasta los más complejos.

Gráfica 2: monitoreo transaccional para determinar el flujo de la transacción, y la necesidad de retar al cliente cuando sea indicado por el score obtenido y el tipo de control que se debe aplicar. [5]

- Autorización por llamada telefónica.
- Autorización por ingreso de OTP[11] enviada por SMS.[12]
- Autorización por ingresó de OTP enviada por SMTP.[13]
- Autorización por Firma electrónica (Códigos QR)[14]para dispositivos Smartphone.
- Tiempos requeridos para continuar con la transacción, como la espera de 24 a 72 horas en algunos casos.
- Autorización por medio de una autenticación fuera de banda, en donde se requiera de un segundo canal transaccional diferente al utilizado en la transacción, como cajeros automáticos, oficinas físicas de la entidad, autenticaciones biométricas etc.

[11] una clave de una única utilización.
[12] Mensajería de texto a teléfonos móviles.
[13] Protocolo de transporte para correo electrónico.
[14] Códigos QR son valoresgráficos únicos.

Grafica 3: Código QR para la firma electrónica, tomada por el autor del documento. [6]

X.CONCLUSIONES

A manera de conclusión, se puede identificar que el motor de riesgo transaccional brinda mucha más seguridad, al exigir para transacciones no identificadas en los perfiles transaccionales de los clientes una autorización fuera de banda que garantice la autenticidad del usuario original.

Sin embargo el motor de riesgo transaccional, no solo sirve para aumentar la seguridad del canal por donde se está transando, sino que a su vez colabora con la no saturación de validaciones para los dispositivos de negocio.

Ya que una vez se identifica una transacción dentro de los patrones cotidianos del perfil transaccional del usuario, se omitirá controles y validaciones de autenticidad a usuarios válidos, por lo que el motor de riesgo solo se concentrará en usuarios realmente potencialmente maliciosos y permitirá una mayor facilidad de uso al usuario legal.

Por ello el motor de riesgo transaccional es una gran herramienta para el comercio electrónico, ya que está diseñado no solo en términos de seguridad sino pensando también es términos de servicio, lo que ayuda con la gran problemática de mantener en un entorno los limites balanceados entre protección y funcionalidad.

Finalmente con el motor de riesgo transaccional se rompe la seguridad basada en la privacidad de la clave y el usuario transaccional, ya que aún un

delincuente contando con estos datos estaría impedido en gran medida para transar con mi cuenta bancaria por comercio WEB, al validarse patrones a través de correlaciones y algoritmos de aprendizaje que permiten identificar patrones establecidos de rutinas transaccionales que permitan identificar intentos de suplantación aún con datos válidos.

XI. REFERENCIAS

[1]http://www.finanzaspersonales.com.co/gaste-eficientemente/articulo/como-suceden-los-fraudes-electronicos/37912.
[2]http://www.uncitral.org/pdf/spanish/xts/fraud/Recognizing-and-preventing-commercial-fraud-s.pdf.
[3]http://www.enter.co/cultura-digital/negocios/colombia-es-subcampeon-mundial-en-fraude/.
[4]Gráfica 1: diseño estructural del motor de riesgo, elaborado por el autor del documento.
[5]Grafica 2: monitoreo transaccional para determinar el flujo de la transacción, y la necesidad de retar al cliente cuando sea indicado por el score obtenido y el tipo de control que se debe aplicar, elaborado por el autor del documento.
[6]Grafica 3: Código QR para la firma electrónica, tomada por el autor del documento.

Autor:

Cesar Arturo Sarmiento Martínez
Ing. de Telecomunicaciones.
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia