Soluciones tecnológicas frente al fraude financiero

Este es un documento producido por

www.ituser.es
www.itreseller.es

Accede a nuestras publicaciones digitales

CÓMO USAR ESTE DOCUMENTO

Con el fin de obtener la mejor experiencia de uso de esta revista, es **imprescindible** seguir estos sencillos pasos que te indicamos a continuación:

Paso 1. Asegúrate de disponer de las versiones más actualizadas de Adobe Reader y Flash Player. Si no las tienes instaladas, puedes descargarlas aquí:

Adobe Acrobat Reader y Adobe Flash Player

Paso 2. Accede al enlace de descarga y la publicación se abre en el visor del navegador.

Paso 3. Busca la opción guardar como que, dependiendo del navegador que utilices, podrá ser un icono o estar incluída en la barra de menú, y guarda la revista en la carpeta donde almacenes los documentos en tu equipo.

Paso 4. Accede a dicha carpeta y usa el botón derecho del ratón para hacer clic en el fichero de la revista.

Paso 5. Selecciona Adobe Reader como aplicación predeterminada para abrir este tipo de documentos.

Paso 6. Una vez abierta la revista, habilita la visualización a pantalla completa, y puedes iniciar la lectura de la revista con todas las capacidades interactivas disponibles.

Soluciones tecnológicas frente al fraude financiero

¿Quién es responsable en un fraude financiero?

Las estafas o fraudes financieros son algo que, por desgracia, está a la orden del día. Pero, ¿quién es el responsable? ¿El usuario? ¿La entidad financiera? Los sistemas de detección preventiva pueden reducir o anular la responsabilidad de las entidades financieras, de ahí que sea necesario que este tipo de empresas implementen medidas de seguridad avanzadas. Descubramos más en estas páginas.

Para poder tener toda la información necesaria para tomar la mejor decisión, a petición de F5, el despacho de abogados Abanlex ha realizado un amplio informe sobre esta responsabilidad de las entidades financieras, un documento del que se desprende que, tanto por la normativa existente como por la jurisprudencia, la entidad bancaria es responsable de la estafa informática, incluso cuando el usuario no tome medidas para proteger sus activos y transacciones.

Incremento de amenazas y una legislación favorable al usuario

El volumen de infracciones y daños relacionados con las operativas electrónicas en bancos y en la compra/venta de productos o en la contratación de servicios, crece a ritmos muy elevados en España, lo que permite prever un aumento de las reclamaciones por parte de los usuarios para la devolución de las cantidades defraudadas, con el evidente perjuicio para las entidades.

El proveedor de servicios de pago, o el intermediario financiero que proceda, debe responder de manera inmediata y, generalmente, sobre la totalidad del dinero defraudado al usuario.

La necesidad de estimular el comercio electrónico determina una legislación en la que el usuario que sufre un ataque de fraude electrónico está amparado, aunque tenga el ordenador infectado, porque esto no se considera una negligencia grave, que sería la que determinaría que la responsabilidad recayera en éste. En cambio, las entidades financieras tienen que acreditar la realidad de las operaciones controvertidas, así como la seguridad de sus sistemas informáticos.

Los tribunales de justicia se decantan a favor del usuario por la elevada carga probatoria que corresponde a la otra parte. Por tanto, contar con medios de prueba adecuados es fundamental para las entidades financieras.

El análisis preventivo de los sistemas y dispositivos del usuario es un paso necesario para que la entidad no pueda ser declarada responsable. Disponer del mayor número de medios posibles para evitar las estafas y operaciones no autorizadas se muestra como un factor esencial. El fundamento se encuentra en la recopilación de las evidencias necesarias que permitan acreditar la situación de los sistemas del cliente con el objetivo de trasladarle la responsabilidad.

Finalmente, se establece por los tribunales una obligación de implementar los sistemas técnicos de seguridad conocidos en el sector. Si una entidad conocía la existencia de un sistema o solución de seguridad informática y, a pesar de ello, no lo implantó, se entiende que deberá hacerse cargo de la consecuente responsabilidad económica ante el usuario afectado.

Importancia creciente de los fraudes financieros

En 2015, cada día se denunciaron algo más de 47 estafas informáticas, de acuerdo con los datos de la Fiscalía General del Estado. El número de afectados y el importe sustraído es probable que sea mucho mayor del que reflejan los datos, teniendo en cuenta ese número de víctimas que no denuncia las estafas que sufre, por no saber cómo debe actuar, por no estimar eficiente la inversión de su tiempo en el procedimiento habida cuenta de la cantidad que se le haya sustraído, o porque nunca llega a saber siquiera que ha sido estafado.

La mayoría de las estafas suceden en relación con ventas fraudulentas, phising, carding o actividades engañosas relacionadas con el juego on-line.

La entidad financiera es responsable

La reforma del Código Penal de 2010, ha afectado positivamente a la lucha contra este tipo de fraudes, reconociendo expresamente las conductas de aquellos que "con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro".

La mayor parte de los casos de estafa que se denuncian ante los tribunales son archivados al no ser posible identificar al responsable del delito por falta de pruebas suficientes. En aquellos casos en los que la vía penal se cierra, el afectado suele buscar una reclamación civil contra la entidad financiera, si bien, legislativamente hablando, ambas vías pueden seguirse de manera independiente.

Son pocas las estafas que llegan a los tribunales, porque las entidades bancarias y financieras, como responsables de los medios de pago, asumen directamente las reclamaciones de escasa cuantía; porque los afectados no reclaman porque entienden que los costes del procedimiento judicial no compensan el resultado; o por la incertidumbre sobre el proceso.

Las entidades deben implementar medidas de seguridad avanzadas

La simplificación de los medios de pago y la posibilidad de transferir cantidades de dinero de manera casi inmediata entre Estados miembros de la UE son dos de los aspectos esenciales para la consecución de un Espacio Único Europeo. Para ello, se siguen reglas concretas que impulsan el establecimiento de garantías suficien-

Tanto por la normativa existente como por la jurisprudencia, la entidad bancaria es responsable de la estafa informática, incluso cuando el usuario no tome medidas para proteger sus activos y transacciones

tes para una libre circulación de personas y capitales en Europa. En ese sentido, se aprobó la Directiva 2007/64/CE con el fin de lograr una armonización de legislaciones entre todos los Estados miembros y la eliminación de obstáculos.

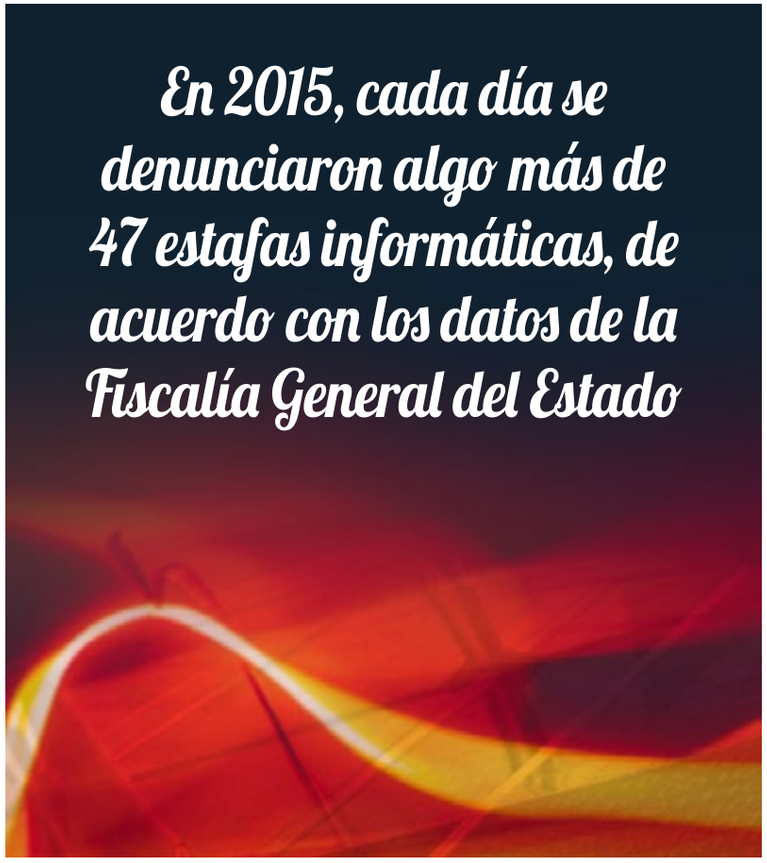
En la UE se diseñó un sistema de implantación rápida de los sistemas de pago por medio de transferencias. Para ello, se pensó en otorgar garantías a los usuarios, con la intención de que pudiesen recuperar de manera inmediata su dinero desde el mismo momento en que fueran conscientes de una transferencia no consentida.

Las normas europeas colocan a las entidades en una situación delicada, ya que sobre ellas pesan obligaciones de asegurar las páginas y los sistemas que gestionan de cara a los consumidores y usuarios. En concreto, la mencionada Directiva coloca a las entidades en una posición ciertamente complicada a través de un incentivo que se ofrece al usuario para que comunique toda pérdida o robo de su dinero. Se anima al usuario a iniciar acciones reduciendo su riesgo y estableciendo que solo debe ser responsable por un importe limitado, entre otras cosas.

Esta Directiva es implementada en España a través de la Ley 16/2009, de 13 de noviembre, de Servicios de Pago, estableciéndose una responsabilidad cuasi objetiva y que incluso invierte la carga de la prueba en relación con la información o a la existencia de comportamiento cualificado en el cliente. Así, se establece la obligación de que sea el banco o la entidad la que deba acreditar ciertos hechos frente al reclamante.

La primera afirmación que encontramos por vía judicial es que las entidades deben adoptar ciertas medidas de seguridad en los sistemas que gestionan de cara al

En 2015, cada día se denunciaron algo más de 47 estafas informáticas, de acuerdo con los datos de la Fiscalía General del Estado



usuario. Sin embargo, las más recientes sentencias sobre estos casos de delitos informáticos señalan que existen obligaciones adicionales a implementar, además de las medidas de seguridad básicas, que se corresponden con la implantación de medidas de seguridad avanzadas y con el aumento de responsabilidad en caso de no haberlo hecho a tiempo. El proveedor de servicios responde, según el artículo 32 de la Ley de Servicios de Pago:

- En caso de pérdida o robo del instrumento de pago, a partir de 150 euros.
- De la totalidad de los importes sustraídos:
  - En las operaciones siguientes a la notificación de la primera no autorizada por parte del cliente que no puedan demostrarse que sean debidas a la actuación fraudulenta del usuario.
  - Cuando no se pueda demostrar que el usuario incumpliera, deliberadamente, o por negligencia grave, las condiciones de uso y custodia del instrumento de pago o no avisase a la entidad, sin demoras indebidas.
  - Cuando el proveedor no disponga de medios adecuados para que pueda notificarse el extravío o sustracción, en todo momento, salvo que se pruebe el uso fraudulento por el usuario.

Sistema de alerta al cliente

Los supuestos más habituales son aquellos en los que la reclamación del usuario proviene de algún tipo de fraude de terceros en el que se han empleado virus, troyanos o técnicas de phising o ingeniería social, para tomar el control de los equipos y los terminales del usuario y hacer uso de sus instrumentos de pago para realizar transferencias o compras. En estos casos, el usuario suele ser alertado por la entidad ante disposiciones no acordes con la operativa habitual del cliente, por intentos de superar los límites de disposición del cliente y otras incidencias.

El hecho de prevenir al cliente al detectar este comportamiento, permite trasladar la responsabilidad al usuario por las disposiciones futuras si no manifiesta nada en contra de las operaciones, pero deberá suponer el bloqueo y la regresión de las posiciones afectadas.

Sin embargo, el problema persiste respecto de las disposiciones iniciales, de las que deberá hacerse cargo la

entidad si no consigue demostrar negligencia grave en las condiciones de uso y custodia de los mecanismos de pago por parte del cliente. Y, evidentemente, no cualquier negligencia se califica como grave. Por ejemplo, los tribunales han considerado que no es una negligencia grave tener un virus en el ordenador, y así lo expresa, por ejemplo, una sentencia de la Audiencia Provincial de Badajoz, de 7 de febrero de 2013.

Como se señala en esta sentencia, no basta con cualquier tipo de conducta que podamos considerar negligente, sino que debe reunir un requisito adicional de gravedad o especial actitud de descuido hacía los sistemas de seguridad.

Ni ordenadores con sistemas operativos no actualizados ni antivirus sin las últimas definiciones de virus o patrones, son suficientes para considerar la negligencia del usuario como grave. Tampoco la utilización compartida de contraseñas por varias personas dentro de una misma empresa, lo que sin duda incrementa el riesgo de que sean comprometidas, es considerado negligencia grave. Así lo señala la sentencia de la Audiencia Provincial de Castellón de 19 de diciembre de 2013.

Necesidad de implementar medidas de seguridad avanzada

Desde los tribunales de justicia se establece una obligación para las entidades de hacer más, en la medida en que disponen de mayor capacidad para implementar mejores medios de seguridad y control. Entre estas acciones adicionales, se estable que las entidades pueden y deben:

- Analizar las operaciones y establecer patrones de comportamiento.
- Analizar las conexiones entre el usuario de los medios de pago y la entidad prestadora del servicio.
- Llevar a cabo análisis remotos de los terminales empleados por los usuarios y sistemas, en la medida en que los primeros lo permitan.

Puede concluirse que estamos en una evolución jurisprudencial que nos lleva a la necesidad de continuar mejorando los sistemas de detección de disposiciones no autorizadas, en cualquiera de sus vertientes.

Sistemas de detección de amenazas

Los tribunales impulsan a las entidades a contar con medios de prueba avanzados que estén activos antes de que el usuario sufra el ataque. Estos medios adicionales, que podrán ser aportados como prueba por las entidades, pueden consistir en los siguientes:

- Pueden hacer descansar en terceros de confianza la recopilación de información sobre las comunicaciones entre las partes.
- Pueden disponer de medidas adicionales de seguridad de la transacción, almacenando un registro de las mismas, así como de los medios técnicos empleados y el estado de los sistemas por ambas partes.

La figura del tercero de confianza mentada se encuentra regulada en el artículo 25 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, y consiste en que personas o empresas ajenas a las partes almacenen las declaraciones de los intervinientes en un contrato.

La consecuencia de la mera declaración del usuario de que una operación no ha sido autorizada por él conlleva la devolución del importe total de la misma y de manera inmediata, y así lo establece claramente el artículo 31 Ley de Servicios de Pago. Esto está relacionado con la necesidad de que el cliente informe a la entidad, sin tardanza justificada, de la existencia de la operación de

DIGITALIZACIÓN Y RIESGOS DE CIBERSEGURIDAD PARA LA BANCA

CLICAR PARA VER EL VÍDEO

pago no autorizada, configurándose, por tanto, como una obligación del usuario del servicio que puede dar lugar a que el cliente no pueda reclamar por operaciones posteriores.

En el supuesto en que concurra un retraso en dicha comunicación, corresponderá al usuario justificar que realizó esa comunicación, pero mayor dificultad tendrá la entidad, que deberá acreditar la existencia de ese retraso en la notificación desde que el usuario conoció el hecho. Esta situación podría darse, por ejemplo, si la entidad pregunta al usuario si ha realizado una operación y éste tarde varios días en responder negativamente.

Así, una solución consistente en un sistema que notifique por SMS, correo electrónico u otra vía una transferencia u otra operación de pago hecha desde las cuentas del cliente, y este último no lleve a cabo ninguna acción durante un plazo determinado limitaría la responsabilidad del banco a las sucesivas operaciones, en tanto que éste podría acogerse a que el cliente conocía su existencia y no comunicó sin demora a la entidad que no había sido autorizada por él. Pero, en todo caso, no debe confundirse la demora en notificar con no ser consciente de la operativa. De hecho, no existe una obligación de consultar el saldo en un período de tiempo concreto, como señaló la sentencia de la Audiencia Provincial de Badajoz de 7 de febrero de 2013. En cualquier caso, la falta de reintegro de las cantidades en el momento en que la entidad es consciente de una operación no autorizada sirve para que puedan ser reclamados posteriormente los intereses desde ese momento.

Disponer del mayor número de medios posibles para evitar las estafas y operaciones no autorizadas se muestra como un factor esencial

El análisis preventivo de los sistemas y dispositivos del usuario se establece jurisprudencialmente como el paso necesario para que la entidad no pueda ser declarada responsable.

Disponer del mayor número de medios posibles para evitar las estafas y operaciones no autorizadas se establece como un factor esencial. El fundamento se encuentra en la recopilación de las evidencias necesarias que permitan acreditar la situación de los sistemas del cliente con el objetivo de trasladarle la responsabilidad.

Este tipo de soluciones de detección y prevención de fraudes para identificar transacciones sospechosas antes de que el proveedor de servicios de pago finalmente autorice las transacciones o mandatos es, asimismo, impuesta como recomendación por el Banco Central Europeo a los operadores en el sector, a través del informe "Assessment guide for the security of internet payments", publicado en 2014.

Los sistemas recomendados por el Banco Central Europeo deben basarse, por ejemplo, en las normas con parámetros (como listas negras de peligro o de datos de tarjeta robados), patrones de comportamiento anormales y un seguimiento continuo del cliente o del dispositivo de acceso del cliente (como un cambio de dirección de Protocolo de Internet (IP) o del rango de IP), comportamientos atípicos para un cliente específico o datos de transacciones anormales. Estos sistemas también deben ser capaces de detectar signos de infección por medio de archivos maliciosos (malware) en la correspondiente sesión web del usuario (por ejemplo, a través de la escritura frente a la validación humana) y escenarios de fraude conocidos. El alcance, la complejidad y la capacidad de adaptación de las soluciones de supervisión, en la medida en que se cumpla con la legislación pertinente sobre protección de datos y de servicios de la sociedad de la información, deben estar en consonancia con los resultados de la evaluación de riesgos.

Soluciones tecnológicas antifraude

La responsabilidad del fraude cae siempre en la plataforma de banca online/e-commerce, y nunca en el usuario final víctima del fraude, sean cual sean las circunstancias. Incluso en casos aparentemente claros en contra del usuario, donde éste no hubiese tomado las más mínimas medidas de protección de su dispositivo de acceso.

En este escenario, nos planteamos: ¿existe esa tecnología que vaya a ser capaz de detectar y mitigar este tipo de fraude en las transacciones online, cuando la entidad no tiene acceso a la plataforma que utilizan sus clientes para las transacciones electrónicas? La respuesta es sí, de la mano de F5 Networks.

Si bien existe hace tiempo la tecnología de Web Application Firewall (WAF), ésta se centra en la protección de la aplicación web frente al uso malintencionado de los usuarios, dejando abierto el camino inverso: la protección del elemento más débil, la plataforma del usuario final, frente a las aplicaciones malintencionadas. Para ello, F5 apuesta por WAF Bidireccional para proteger no solo las aplicaciones frente a los usuarios malintencionados, sino también a los usuarios de las aplicaciones malintencionadas.

Importantes amenazas

El software malicioso y los mecanismos y técnicas de robo de credenciales evolucionan constantemente. Además, los antivirus tradicionales ya no detectan correctamente los virus tipo troyano, ya que se basan, sobre todo, en firmas, y este malware muta muy rápidamente

Estas nuevas versiones de malware, usan todo tipo de técnicas para infectar a los usuarios, operar y mantenerse ocultas en los dispositivos de los usuarios, que abarcan desde técnicas de ingeniería social, o aprovechamiento de configuraciones vulnerables en los navegadores, a ataques complejos con combinaciones de cookies, cachés, keyloggers, phising...

El impacto

Uno de los errores comunes a la hora de analizar el impacto económico de estas amenazas es evaluar el coste de estas acciones de fraude como un hecho aislado con un coste igual a las propias cantidades defraudadas.

En primer lugar, este análisis es incorrecto puesto que una parte muy importante del fraude no es detectado, existiendo actividades delictivas que bien por falta de denuncia del usuario o bien simplemente por la ausencia de herramientas de detección adecuadas, no son adecuadamente detectadas y reportadas.

En cualquier caso, la aparición de estos mecanismos de fraude conlleva otros costes ocultos difíciles de cuantificar, cuyo impacto económico puede ser mucho mayor que el propio fraude cometido. De esta forma, se deben considerar otros costes directamente relacionados y otros muchos ocultos tales como el coste de atención al usuario e incidencias, el coste asociado al cumplimiento normativo e implicaciones legales, costes de gestión del fraude, pérdidas potenciales e impacto en el cliente.

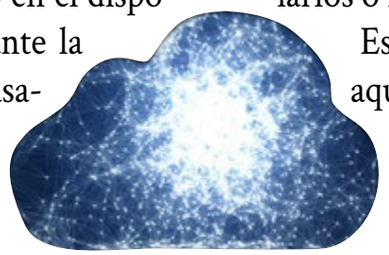
Soluciones antifraude de F5 Networks: WAF Bidireccional

F5 ha decidido abordar la problemática de seguridad del entorno del fraude desde una aproximación completa, que incluye la protección de las aplicaciones y servicios, y la detección de actividad fraudulenta que pueda estar ocurriendo en el lado del usuario que se conecta al servicio. Esta aproximación, llamada WAF Bidireccional, permite a los proveedores de servicios online, entidades bancarias, plataformas e-commerce, agencias de viajes o transporte y otros servicios, protegerse de las tradicionales amenazas a la capa de aplicación, a la vez que permiten detectar posibles intentos de actividad fraudulenta por parte de malware instalado en los dispositivos de los usuarios.

Protección del usuario

Basándose en su producto Fraud Protection Service, F5 permite detectar y bloquear el fraude y la actividad maliciosa que pueda ocurrir en el entorno del cliente o usuario final del servicio. La aproximación no requiere modificar las aplicaciones, ni instalar software en los dispositivos de cliente, permite proteger cualquier tipo de dispositivo y previene frente a amenazas conocidas y desconocidas.

Mediante la inyección del código JavaScript, se detecta la presencia de software malicioso en el dispositivo de cliente. Esto se realiza mediante la creación y mantenimiento de firmas basadas en el análisis de múltiples muestras de malware y ataques a distintos "honeypots", lo cual permite con un análisis heurístico y de comportamiento detectar y calificar rápidamente el malware que se esté ejecutando en el dispositivo remoto. Además, mediante el uso de técnicas de inspección sobre lo que el usuario está visualizando y el origen entregado por la aplicación se realiza un chequeo de integridad que es capaz de detectar en tiempo real si un usuario está siendo atacado mediante algún tipo de inyección de código, inyección de formularios o inyección de enlaces o URL a otros sites.



Esta comparación dinámica permite detectar aquellos ataques y malware que dinámicamente descargan de sus "Command and Control" el ataque específico a cada site, por lo que se mitigan las amenazas, tanto conocidas como desconocidas, basándose en el comportamiento y lo que está visualizando el usuario.

Cifrado de la capa de aplicación

El cifrado aplicativo evita el robo de credenciales. Estos malware dedicados a "credential grabbing", están a la escucha a nivel de navegador para ciertos dominios, y cuando ven un formulario, capturan lo que el usuario está introduciendo (credenciales, DNI, tarjetas de crédito...) y lo mandan a una "drop zone" para que el hacker las recoja. También hay malware que escucha en todos los dominios parámetros en los formularios con nombres muy descriptivos, como password, username, credit_card. La tecnología de F5 también es capaz de anular esto, utilizando HFO (HTML Field Ofuscation).

La gran problemática a la que se enfrentan los desarrolladores de aplicaciones es la asunción de que el mecanismo de cifrado de la capa de transporte (TLS/SSL) es suficiente para securizar el intercambio de información. Y esta asunción puede ser cierta para cualquier elemento intermedio que quiera inspeccionar el tráfico entre usuarios y aplicaciones, (suponiendo que se carece de las claves privadas de los servidores). Sin embargo, cualquier elemento añadido al código en ejecución de los navegadores tiene total visibilidad de lo que visualiza y escribe el usuario, de manera que puede copiar esta información y enviársela a un tercero.

F5 previene estos ataques dinámicamente, sin necesidad de modificar la aplicación. Cuando se conecta un usuario al servicio se genera dinámicamente una clave privada y una clave pública, esta última se envía al usuario que mediante el código JavaScript introducido y esta

Las compañías tardan una media de 120 días en parchear una vulnerabilidad, y la probabilidad de que una vulnerabilidad sea explotada es del 90% tras los primeros 40 a 60 días

clave, cifra aquellos campos sensibles. Como el descifrado solo puede realizarse con el par de claves generadas por F5, cualquier copia de la información que el usuario introduzca en el navegador es inútil para los hackers.

Protección anti-phising

Otro de los ataques tradicionales a los usuarios es la creación de copias de las páginas de las aplicaciones para después reconducir a los usuarios al site falseado mediante ataques de spam o cualquier otra técnica de redirección. La tecnología de F5 permite detectar los ataques de phising en todas las etapas del desarrollo de un ataque, incluso antes de que el ataque se haya producido.

Además de lo anterior, la solución propuesta por F5 también evita las técnicas de web scraping, que utilizan programas de software para extraer información de sitios web.

Protección frente transacciones automáticas

Otra de las capacidades de protección de la solución es la detección de actividad automatizada realizada por usuarios conectados. El vector de ataque es simple, se espera a que el usuario se haya conectado al servicio, y, sin que el usuario pueda detectar esta actividad, se lanzan transacciones automáticas para transferir fondos a las cuentas de los atacantes o la realización de pedidos automatizados.

La protección de F5 permite detectar que las transacciones realizadas por los usuarios sean lícitas, detectando eventos propios del uso de la aplicación por un usuario, tales como movimientos de ratón, tecleo de los campos individualmente... De esta forma, si un usuario lícito del servicio se conecta con un malware que realice estas transacciones automáticas, no solo se detectan estas transacciones, sino que, además, se puede establecer una comunicación con el usuario para alertarle de la existencia de estos eventos.

Protección de las aplicaciones

Las aplicaciones son el mecanismo de comunicación de facto con usuarios, clientes, empleados, proveedores, se han convertido en la imagen de las compañías, y su disponibilidad es uno de los factores más críticos en la continuidad del negocio. Además, la información contenida en los sistemas de información que soportan estos aplicativos es también crítica.

La exposición de las aplicaciones hacia el exterior es extrema y por ello es el punto de ataque de inicial de cualquier ataque cibernético. Según el 2015 Cisco An-

nual Security Report, el objetivo del 75% de los ataques son los servicios web. Se estima, además, que el 86% de los sitios web tienen al menos una vulnerabilidad expuesta y que la media de vulnerabilidades por site es de 56 (Whitehat Security Statistics Report 2013), lo cual justifica claramente que las aplicaciones sean el objetivo principal de los hackers.

Si a esto añadimos la incesante demanda de desarrollo sobre las aplicaciones, requerida por su fuerte vínculo con negocio, la gestión de la seguridad de estas aplicaciones adquiere una complejidad imposible de incorporar en los departamentos de desarrollo, que ajenos a estas problemáticas, se encuentran ya por sí mismos ahogados en los requisitos de inmediatez de sus ciclos de desarrollo, además de carecer del conocimiento experto en seguridad requerido para bloquear los ataques específicos de los aplicativos web.

La tecnología de F5 permite detectar los ataques de phising en todas las etapas del desarrollo de un ataque, incluso antes de que el ataque se haya producido

Según las estadísticas (Kenna Securities, sept'15), las compañías tardan una media de 120 días en parchear una vulnerabilidad, y la probabilidad de que una vulnerabilidad sea explotada es del 90% tras los primeros 40 a 60 días, lo cual da una visión muy clara de la amplitud y peligrosidad de estas ventanas de exposición.

La solución propuesta por F5 incluye capacidad para identificar y detener ataques de denegación de servicio dirigidos a la capa de aplicación (DDoSL7).

ASM Application Security Manager

F5 comercializa una solución de WAF (Web Application Firewall) bajo el nombre comercial de Application Security Manager (ASM), módulo activable en cualquier plataforma BIG-IP mediante licencia software.

El módulo ASM permite garantizar la seguridad y disponibilidad de las aplicaciones, reducir los costes y ayudar a obtener el cumplimiento normativo, desplegar políticas prediseñadas para las aplicaciones más comunes del mercado, y flexibilizar la implementación.

Enlaces relacionados

- V ¿Sabes quién te vigila?
- W Protección contra el fraude online
- I Soluciones de F5 contra el fraude online: Websafe y Mobilesafe
- I Dridex, el malware que te acecha
- I Trickbot, el último malware especializado en Banca
- W En la mente de un hacker: 10 formas de proteger tu negocio
- W IDC: The blind state of rising SSL/TLS traffic: Are you cyber threats visible?
- W Dispositivos IoT, los nuevos secuaces de los ataques DDoS
- W Application Security in the Changing Risk Landscape
- W DDoS Attacks Trends