Biometría conductual: combata el fraude, no la productividad

Cómo IBM Security Trusteer Pinpoint Detect ayuda a combatir el fraude con menos procesos

Aspectos destacados

Uso del aprendizaje artificial para la detección cognitiva de fraudes y la verificación dinámica de identidad

Uso de servicios de inteligencia en tiempo real para ayudar a detectar fraudes y reducir falsos positivos

Procesamiento mediante aprendizaje artificial para distinguir a los clientes reales de los defraudadores en el momento de iniciar la sesión

Empleo de un enfoque simplificado para ayudar a detectar y prevenir el fraude a lo largo de todo su ciclo de vida

¿Pueden las instituciones financieras distinguir un cliente real de un defraudador en sus sistemas de banca online? Los clientes esperan encontrar una experiencia rápida, sencilla y eficiente cuando interactúan con sus bancos online. La verificación fiable de usuarios legítimos permitiría al banco dejar de molestar a los clientes con solicitudes de autentificación para acceder a su cuenta. Las funciones de biométrica de comportamiento de IBM® Security Trusteer® pueden ayudar a combatir el fraude sin restringir la productividad.

El análisis biométrico físico convencional estudia las características físicas del usuario mediante identificación de voz, comparación de huellas dactilares, escáneres retinales y tecnología de reconocimiento facial. Se basa en la teoría de que es imposible copiar las características físicas individuales con la misma facilidad que las credenciales de una cuenta. Es una tecnología eficaz que, sin embargo, tiene limitaciones y puede prolongar el proceso de autentificación. La implantación de escáneres retinales y de huellas dactilares, por ejemplo, puede ser costosa, mientras que los rasgos faciales cambian con el paso del tiempo, reduciendo la precisión del reconocimiento. La biométrica de comportamiento, por el contrario, identifica al cliente sin requerir que demuestre quién es, sino analizando sus *acciones*.

Las funciones de biométrica de comportamiento de IBM Security Trusteer Pinpoint™ Detect, por ejemplo, detectan y rastrean sutiles movimientos del ratón. De este modo, aprende y analiza el comportamiento del cliente a lo largo de múltiples sesiones. Esto ayuda a los bancos a simplificar sus procesos de autentificación y ofrecer al cliente una experiencia fluida al tiempo que contribuye a reforzar su capacidad para detectar y mitigar las actividades fraudulentas.

Distinguir con exactitud un usuario real de un defraudador

La satisfacción del cliente es prioritaria para las instituciones financieras, que trabajan sin descanso para proteger a sus clientes y, al mismo tiempo, mantener unos procesos de autentificación discretos. La biométrica de comportamiento es un método de verificación no invasivo que cumple exactamente ese fin. Añade una capa de protección adicional sin imponer nuevos pasos al cliente. Cada año, los informes señalan que el fraude representa un riesgo constante para las instituciones financieras. Según IBM X-Force®, "en 2015 la organización cliente media monitorizada por IBM Security Services experimentó aproximadamente 53 millones de incidencias de seguridad anuales".[1] En 2015 "se produjeron 1.966.324 avisos registrados de tentativas de infección con malware cuyo fin era la sustracción de dinero mediante el acceso online a cuentas bancarias".[2] Algunos bancos han adoptado normas de contraseñas extremadamente estrictas, mientras que otras envían códigos de verificación de un solo uso a través de mensajes de correo electrónico o SMS. Aunque son útiles, repercuten en la experiencia del usuario, alargando el proceso de inicio de sesión y menoscabando la conveniencia de la banca online. Trusteer Pinpoint Detect proporciona una capa de protección adicional imperceptible desde el punto de vista del usuario.

La biométrica de comportamiento es invisible para el cliente; no limita su experiencia ni añade nuevos pasos al inicio de sesión. Tampoco ralentiza ni interrumpe la interacción con la banca online, sino que las capacidades de la solución usan el aprendizaje artificial y el procesamiento de lenguaje natural para la detección cognitiva de fraudes y evaluaciones dinámicas de identidad que identifican a clientes y defraudadores conocidos durante el acceso. Estudia los movimientos del ratón, correlacionando el modo en el que los clientes interactúan con sus cuentas online con el fin de detectar conductas anómalas.

¿Qué supone esto para las instituciones financieras y sus usuarios?

La posibilidad de distinguir entre el comportamiento de un cliente real y un defraudador conocido es tremendamente útil. Defraudadores y ciberdelincuentes pueden robar los datos del usuario, pero reproducir su comportamiento no es tan sencillo. Esto representa una ventaja para las instituciones financieras. El despliegue, utilización y análisis de indicadores de seguridad de biométrica de comportamiento es un modo avanzado de verificar a los usuarios legítimos con escaso impacto para estos.[3]

La biométrica de comportamiento de Trusteer ofrece un enfoque fundamentalmente diferente que puede ayudar a las organizaciones financieras a detectar fraudes, reducir falsos positivos y rebajar el número de alertas de seguridad, sin que esto afecte al usuario final. La combinación de indicadores de riesgo propios del usuario y de las funciones de biométrica de comportamiento de Trusteer Pinpoint Detect confirman las virtudes del enfoque adoptado por IBM para la detección de fraudes, basada en tres principios básicos: visibilidad, inteligencia de amenazas global y diseño ágil.

Visibilidad

El corazón de Trusteer Pinpoint Detect es un motor que correlaciona una amplia variedad de indicadores de fraude críticos para detectar intentos de phishing, infecciones de malware, credenciales comprometidas y métodos de evasión avanzados por medio de modelos mejorados de dispositivos, geolocalización y transaccionales para ayudar a detectar con mayor precisión las actividades fraudulentas.

Red de inteligencia de amenazas global

Para combatir el fraude, el alcance, profundidad y rapidez de la recogida de información son factores críticos. La red de inteligencia de amenazas global de IBM X-Force analiza información proveniente de cientos de millones de terminales. La red procesa constantemente la inteligencia de seguridad que X-Force utiliza para crear modelos digitales dinámicos. Armado con esta inteligencia, el análisis de amenazas de Trusteer emplea tecnologías analíticas de vanguardia para investigar amenazas específicas propias del sector y la organización. Las instituciones financieras pueden mejorar sus defensas por medio de actualizaciones automáticas, sin ningún esfuerzo adicional por parte de la organización. Trusteer Pinpoint Detect hace uso de esta inteligencia, que incluye numerosos atributos de sesión, datos e indicadores de fraude, para ayudar a detectar fraudes con mayor exactitud dentro de inmensos conjuntos de datos.

Diseño ágil

El tiempo es oro en la prevención de ciberdelitos, por lo que Trusteer Pinpoint Detect cuenta con una arquitectura ágil que facilita y agiliza el proceso de respuesta. Empleando tecnologías basadas en el cloud, la solución es capaz de detectar, analizar y compilar y desplegar contramedidas con rapidez en respuesta a nuevas amenazas emergentes. Las instituciones financieras también pueden utilizar defensas en función de la aplicación especialmente adaptadas a sus necesidades y las amenazas que afrontan. Esto puede contribuir a incrementar aún más la exactitud de la detección para reducir costes de explotación.

¿Por qué IBM?

La plataforma IBM Security proporciona inteligencia de seguridad para ayudar a las organizaciones a proteger de manera holística sus clientes, datos, aplicaciones e infraestructuras frente a amenazas para la seguridad. IBM ofrece soluciones para la gestión de identidades y accesos, información de seguridad y gestión de incidencias, seguridad de bases de datos, desarrollo de aplicaciones, gestión de riesgos, protección contra intrusiones de nueva generación, etc. IBM opera una de las organizaciones de investigación y desarrollo más grandes del mundo.

Información adicional

Para obtener más información sobre IBM Security Trusteer Pinpoint Detect, póngase en contacto con su representante IBM o IBM Business Partner, o visite: **ibm.com**/security

Además, IBM Global Financing ofrece numerosas opciones de pago para ayudarle a adquirir la tecnología que necesita para que su negocio crezca. Ofrecemos gestión de todo el ciclo de vida de productos y servicios de IT, desde la adquisición hasta la eliminación. Para saber más, visite: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Producido en los Estados Unidos de América
Octubre 2016

Recicle este documento

[1] "Reviewing a year of serious data breaches, major attacks and new vulnerabilities", *IBM Corp*., abril 2016. https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03133usen/SEW03133USEN.PDF

[2] "Kaspersky Security Bulletin 2015: OVERALL STATISTICS FOR 2015", *Kaspersky Labs*, 2015. https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf

[3] "Why adopt behavioral biometrics as part of your multi-modal strategy", *Zighra*, 22 de junio de 2015. http://www.zighra.com/blog/behavioral-biometrics-and-multi-modal-biometrics

WGS03090-ESES-00