El fraude móvil a escala – El crecimiento exponencial de canales y experiencias digitales.

Autor: Franco Paolo Carranza – Mentor en INNOVA ESAN

El fraude móvil a escala

No hay duda de que hemos visto durante estos largos meses de confinamiento el crecimiento exponencial de canales y experiencias digitales, todas orientadas a acercar productos y servicios a consumidores. Los sectores son diversos, pero sobre todo debemos mirar y estar alertas en el sector financiero.

Este breve artículo debe hacer reflexionar a los líderes que tienen la responsabilidad en el ámbito tecnológico sobre cómo podemos empezar a generar distancia de forma constante entre nuestros productos digitales y los atacantes.

¿Qué están haciendo los atacantes a nivel global?

Desde tratar de hacer que usuarios finales caigan en campañas de phishing, interceptación de SMS, ingeniería social o agregando malware (Software Malicioso) en tu celular disfrazado de aplicaciones útiles, cada día los atacantes en todo el mundo planifican formas de lograr obtener datos sensibles para diferentes propósitos.

¿Qué están haciendo las empresas para resolver esta problemática?

No existe un remedio único que mitigue todos los ataques o resuelva el problema en una sola ejecución. La estrategia y la constancia son claves, pero para ejecutar una estrategia de forma constante se necesita de atributos que claramente no están siendo alcanzados dentro de las instituciones y tampoco en muchas empresas de desarrollo de software.

No hablamos de tecnología millonaria en primera instancia, tampoco hablamos de un programa o licencia que cura todo, hablamos de procesos tan básicos por defecto que pueden ser el inicio de algo mucho mejor para los usuarios y la industria misma.

Según reputadas consultoras globales, las instituciones bancarias, fintechs y otras empresas deben interiorizar sus procesos de enrolamiento y autenticación como parte del análisis a la problemática. No es un camino fácil, pero hay que iniciar, seguimos después de 8 años o más con un proceso de autenticación que no ha cambiado sustancialmente para mejor, estamos seguros de que los usuarios lo apreciará y se adaptarán, pero más importante aún, la tecnología de autenticación y autorización robusta no debe ser un lujo. Debe ser un estándar para todos, disponible siempre como parte del ADN de tus productos o servicios digitales.

Este modelo jurásico y estático de "factor único" es de los más vulnerables en el tema de violación de datos. La implementación de la autenticación multifactor ayuda a mitigar el riesgo de apropiación de la cuenta, pero debemos ver de manera integral el cómo construimos el customer journey desde la perspectiva de la seguridad, para eso Applied Labs es el mejor aliado.

Sabemos que los atacantes tratarán de aplicar diferentes estrategias de forma permanente, pero debemos preguntarnos:

¿Qué estamos haciendo las instituciones de forma permanente para lograr marcar distancia?

Estamos muy concentrados en la superficie y poco en el core, en la arquitectura, los procedimientos y controles que son sin duda muy necesarios actualmente.

Quizá pensamos mucho en lograr cosas como las que sugiere Gartner….

Por ejemplo, Gartner plantea un framework con 5 capas de prevención:

Layer 1: Endpoint-centric

Análisis del comportamiento del endpoint, correlación de la ubicación y la inclusión de la detección de malware y fingerprinting.

Layer 2: Navigation- and Network-centric

Análisis de sesión, red, comportamiento durante la navegación y patrones sospechosos.

Layer 3: User- and Entity-centric (single channel)

Análisis de comportamiento del usuario por canal (Banca en Línea, Banca Móvil,etc.)

Layer 4: User- and Entity-Centric across channels and products

Análisis de comportamiento anómalo correlativo entre los diferentes canales.

Layer 5: Big Data User and Entity linking

Análisis de patrones y relación para detectar crimen organizado y colusión.

En Applied Labs creemos que antes de implementar tecnología debemos interiorizar cómo vamos a desarrollar nuestros productos, esto nos permitirá construir los mecanismos necesarios bajo los estándares mínimos y naturales para que el software por defecto genere la distancia correcta entre el atacante y los usuarios.

Desde ahí podemos crear diferentes puntos de análisis de forma eficiente y no dispersa.

La consecuencia de esto será hacer crecer una plataforma ordenada y robusta por defecto para atender a millones de usuarios y obtener el feedback correcto para mejorar cada vez este journey del que tanto se habla hoy en la vorágine digital.

Según nuestros estudios, desde la banca de mayor tamaño hasta las empresas más pequeñas en otras industrias; el fraude es posible debido a la ausencia de procedimientos robustos tanto en el diseño, desarrollo e integración de servicios que hoy exponen y la intercooperación con datos de personas y empresas.

Esto nos deja un desafío importante como país y es el de para mitigar los riesgos y crear mayor oportunidad de enfocarnos en temas realmente productivos para los consumidores, empresas privadas y públicas.

Recibamos este año con esa tarea en mente y como decimos en Privatia ID.

No te dejes atrapar.

Franco Paolo Carranza

Mentor en INNOVA ESAN