CONSIST
Business Information Technology

Prevención del Fraude Interno en Entidades Gubernamentales

Intellinx
Insider Threat Intelligence

Los Desafíos
Los siguientes son algunos ejemplos:

Fraude en el reembolso de Impuestos
Un empleado del Departamento de Ingresos cambia el número de cuenta bancaria de un contribuyente, procesa un reembolso y luego cambia el número de cuenta bancaria nuevamente. ¿Cómo se puede evitar?

Fuga de Información confidencial
Un empleado de la Policía vende información sobre la investigación de un caso de homicidio a uno de los sospechosos. ¿Cómo se puede detener a tiempo?

Un usuario con privilegios del área de Tecnología coloca una bomba lógica dentro de un sistema
Un programador descontento de una Agencia Estatal escribe código malicioso dentro de un programa que, esporádicamente, borra las cuentas de los contribuyentes. Para ocultar sus rastros compila el programa, elimina el código malicioso del programa fuente, y luego lo guarda quedando éste sin la codificación malintencionada. ¿Cómo revelar lo que hizo?

La Amenaza Interna

Las agencias gubernamentales alrededor del mundo están afrontando una creciente amenaza para sus patrimonios de información. Esta amenaza muchas veces proviene desde sus empleados, funcionarios, agentes, etc. Debido al conocimiento que estas personas tienen sobre la información que manejan, pueden causar un daño mucho peor que si el fraude proviniera de terceros. Es grave cuando internamente se mal utilizan deliberadamente las capacidades y controles que se tienen para manipular los sistemas internos o se deja escapar la información con fines malintencionados. Las numerosas actividades fraudulentas realizadas internamente incluyen la manipulación de transacciones financieras, malversación de activos, venta de información privada de ciudadanos, y otros más. Más allá de este tipo de fraude podrían existir también transacciones fraudulentas bajo forma de errores de sistema o cambios de información de tipo intencional.

El Desafío: Que la Auditoría Pueda Seguir el Rastro

La FISMA (Federal Information Security Management Act), HIPAA, y otras entidades reguladoras, exigen a las Agencias Gubernamentales mantener un rastro de Auditoría detallado sobre el acceso a datos confidenciales de sus sistemas de información. Esta exigencia es un desafío, en especial para las Organizaciones que tienen plataformas heterogéneas que incluyen sistemas legacy ya que generalmente éstos no proporcionan el suficiente registro de acceso a las aplicaciones. El desarrollo de incluir tal mecanismo en los sistemas existentes, implica un gran esfuerzo y costo, ya que se deberían alterar o cambiar la codificación de miles de programas. Por otra parte, los mecanismos de rastreo que proporcionan las bases de datos corporativas tampoco son suficientes, dado que los mismos generalmente llevan un track de las transacciones de actualización, pero no capturan el acceso a la información de “sólo lectura”. Además, las bases de datos generalmente carecen de la capacidad de capturar al User-Id real que tuvo acceso a la información, dado que la mayor parte de aplicaciones utilizan el User-id genérico al ingresar a la base de datos.

Intellinx: La Solución para Detectar el Fraude Interno a Través de Todas las Plataformas que Tengan los Gobiernos.

Intellinx marca un hito en la detección y prevención de fraudes internos. Primero en su tipo, proporciona un sistema de vigilancia sobre la actividad de los usuarios finales de las aplicaciones permitiendo definir patrones de comportamiento de los mismos. Obtiene una visibilidad sin precedentes de las actividades de los usuarios autorizados de los sistemas de la Organización. Intellinx proporciona una infraestructura fundamental para la lucha contra el fraude interno y fugas de información, haciendo a los usuarios autorizados responsables de sus acciones. Resumiendo: Intellinx es el único producto en el mercado hoy en día que proporciona lo siguiente:

Mayor información: argentina@consist.com.ar

Intellinx
Insider Threat Intelligence

Disgregación de Funciones
En la Administración de Seguridad Social, se requiere la aprobación de un Administrador para un cambio en el estado de un beneficiario. Un empleado intenta introducir la contraseña de su Superior, pero falla y no se llega a completar la transacción. ¿Cómo se averigua?

Fuga de información sobre la salud de Celebridades
Un empleado de la Administración de Seguridad Social averigua o descubre información confidencial sobre la salud de alguna celebridad y lo filtra a la prensa, lo cual genera un escándalo. ¿Cómo encontrar a quién lo hizo?

• Visión sin precedentes de las actividades de los Usuarios Finales - Proporciona una visualización completa de la actividad del usuario final, reproduciendo exactamente cada pantalla por la que pasó, las teclas de función que fueron pulsadas por él, como así también los mensajes de las aplicaciones cliente/servidor emitidos. Intellinx registra y hace visibles todas las acciones, incluyendo no sólo las actualizaciones sino también las CONSULTAS u operaciones de 'read only' efectuadas. Realiza un seguimiento de todos los tipos de usuarios finales, incluyendo aquellos con privilegios, como ser los Administradores de Sistemas y los Administradores de Bases de Datos, siendo que estos grupos podrían representar un riesgo mayor, al poseer mayores niveles de autorización.

• Pista de Auditoría completa - Intellinx registra la actividad completa de los usuarios (24x7) en tiempo real y no solamente los hechos detectados como sospechosos. Esto es fundamental para que los usuarios finales se hagan responsables de sus acciones. Además permite no solamente que las reglas se apliquen en el momento exacto de producirse un evento ilícito, sino que también la información pueda ser accedida o consultada por una investigación forense en un momento posterior.

• Seguimiento y búsqueda de ilícitos a través de distintas plataformas tecnológicas incluyendo los sistemas legacy - Intellinx es una solución única para el seguimiento/control de las acciones de los usuarios independientemente de la plataforma tecnológica en la que se encuentren. Monitorea aplicaciones mainframe, iSeries, web, cliente/servidor, y más. Permite hacer búsquedas por cualquier valor específico expuesto en la pantalla de cualquier usuario. Las reglas de Intellinx realizan un seguimiento de los procesos de negocios sin importar en qué plataforma se encuentren. Por ejemplo, un proceso registrado por Intellinx puede iniciarse en un iSeries, continuar en una aplicación cliente/servidor y finalizar en la Web.

• Patrones de Comportamiento de los usuarios finales a nivel de aplicación - Intellinx es la única solución del mercado que analiza la actividad del usuario a nivel de pantalla de aplicaciones (y no a nivel de redes o bases de datos). Las reglas de Intellinx realizan un seguimiento de todas las teclas pulsadas por el usuario como así también todas las pantallas que fueron visitadas por él, detectando así qué valores de los procesos relevantes de negocios han sido accedidos o modificados. Esta información está disponible en tiempo real por lo que se pueden generar alertas sobre comportamientos sospechosos en el mismo instante en el que ocurren.

Intellinx Out-of-the-box

Intellinx Out-of-the-box provee un excelente valor agregado ya que inmediatamente luego de su instalación y puesta en marcha (proceso que toma unas pocas horas) comienza a capturar toda la actividad de los usuarios finales autorizados a operar con las distintas aplicaciones, sin importar en qué plataforma tecnológica se encuentren, permitiendo a los auditores internos u oficiales de seguridad informática puedan comenzar a realizar búsquedas sobre eventos que consideren sospechosos. Las organizaciones pueden inmediatamente y sin ninguna demora comenzar a investigar situaciones de dolo sin agregar ni una línea de código a sus aplicaciones existentes.

Resumen

Intellinx es una solución de avanzada que permitirá a las instituciones gubernamentales lo siguiente:

- Detectar potenciales usuarios fraudulentos ya que todas sus acciones y comportamientos son grabados.
- Proteger la reputación de las instituciones de gobierno del daño que pudiera generar la mala publicidad dada por alguna filtración de datos o identidades reservadas.
- Reducir las pérdidas generadas por los fraudes internos u otras acciones malintencionadas, detectando en tiempo real actividades sospechosas.
- Cumplir con las reglamentaciones de las distintas Organizaciones que regulan las operatorias gubernamentales.
- Mejorar la efectividad de la auditoría interna, alertando en tiempo real ante comportamientos sospechosos de usuarios autorizados.
- Detectar si los usuarios están consultando información que no es de su competencia.

Argentina - www.consist.com.ar
Av. Corrientes 345, 4º Piso (C1043AAD) Buenos Aires, Argentina. Teléfono: +54-11-4313-1747
argentina@consist.com.ar

Chile - www.consist.cl
Av. 11 de Septiembre, 2134 5º Piso, Santiago de Chile, Chile.
Teléfono: +56-2-233-5901- info@consist.cl

Uruguay - www.consist.com.uy
Washington 258, Montevideo (11100), Uruguay.
Teléfono: +598-2-916-0522 - linobessonart@gmail.com