Intellinx
Insider Threat Intelligence

Con el objetivo de alcanzar el plazo final de conformidad con la nueva regulación y economizar recursos, Banco Leumi buscó una solución de software lista para usar, que incluyera las capacidades de registro de acceso, alertas y soporte a las regulaciones, sin incurrir en cambios en las aplicaciones legadas. La única solución que el equipo encontró fue IntellinX, nueva tecnología de IntellinX Ltd., empresa líder en la provisión de soluciones de integración de aplicaciones.

El Banco Leumi utiliza nueva tecnología para conformidad con la regulación equivalente al Basel 2.

Siguiendo un esquema de fraude en gran escala que prácticamente llevó al fracaso a los bancos menores de Israel, el supervisor de banco de Leumi aprobó la regulación 357 basada en el Acuerdo Basel 2 - bastante similar a la ley norteamericana Sarbanes-Oxley. En vigor desde el 1 de julio de 2004, la nueva regulación requiere que los bancos mantengan un conjunto computarizado de datos de auditoría (logs) de los accesos, de las aplicaciones y de las consultas realizadas en sus sistemas de información. Los registros deben incluir la identidad de la persona que está accediendo los sistemas, el lugar, la hora y particularidades de la transacción, como el número de cuenta accedida y el tipo de acceso (o sea, lectura, actualización, exclusión). Los sistemas de administración de registros también deben avisar a las partes responsables dentro de la organización sobre los intentos de actividades externas no autorizadas, así como actividades poco comunes de diversos tipos de usuario, conforme a lo definido por la dirección del banco.

Fundado en 1902, el Banco Leumi es un grupo financiero de Israel, líder internacionalmente, con 250 agencias en 19 países, más de 1,7 millones de clientes y bienes por un valor superior a 100 mil millones de dólares. En el inicio de 2004, cuando el Banco de Israel publicó la nueva regulación, el vice-presidente senior y jefe de la división de operaciones del Banco Leumi, Sazón Mordechay, asignó a un grupo de gerentes altamente experimentados la tarea de coordinar e implementar el proyecto de conformidad con la nueva regulación en todo el banco. Uno de los principales desafíos identificados por el equipo fue crear un juego completo de datos de auditoría de las aplicaciones legadas del banco, que funcionaban en un mainframe IBM central. A diferencia de los dispositivos de red y sistemas de infraestructura, ese tipo de sistemas normalmente no posee herramientas para analizar las actividades del usuario a nivel de aplicación, principalmente cuando las aplicaciones son desarrolladas o personalizadas internamente. En el caso del Banco Leumi, muchas de sus aplicaciones no contaban con el recurso de registro de accesos, entonces para que se creara un registro de todas las acciones realizadas por los usuarios finales serían necesarias modificaciones en diversos programas en decenas de aplicaciones. El equipo estimó que esta tarea llevaría 100 meses de dedicación de un programador para ser ejecutada.Además de eso, serian necesarios recursos adicionales de programación para mantener actualizada la facilidad de “registro de acceso” durante el curso natural de mantenimiento en el correr de tiempo de vida de esas aplicaciones.

Con el objetivo de alcanzar el plazo final de conformidad con la nueva regulación y economizar recursos, Banco Leumi buscó una solución de software lista para usar, que incluyera las capacidades de registro de acceso, alertas y soporte a las regulaciones, sin incurrir en cambios en las aplicaciones legadas. La única solución que el equipo encontró fue IntellinX, nueva tecnología de IntellinX Ltd., empresa líder en la provisión de soluciones de integración de aplicaciones. IntellinX registra todas las interacciones (pantallas exhibidas y comandos accionados por el usuario) entre los usuarios finales y las aplicaciones legadas en tiempo real. Realiza, de forma no invasiva y sin dejar vestigios, el análisis de las trasmisiones de la red a partir de la cual las pantallas originales y los comandos del usuario son reconstruidos. El contenido de las pantallas grabadas es analizado en tiempo real, reconociendo automáticamente los encabezados de las pantallas, valores y título de los campos y comandos del usuario. Los datos son analizados usando reglas predefinidas que identifican acciones sospechosas del usuario o patrones de comportamiento, disparando alertas instantáneos para las personas responsables. Esos alertas permiten que el auditor se concentre de inmediato en sospechosos específicos y revea todas las acciones realizadas. Las sesiones grabadas son almacenadas por el sistema, solicitando que nuevas reglas de negocio sean aplicadas después de lo ocurrido.

Intellinx
Insider Threat Intelligence

Mordechay aprobó la recomendación del equipo para evaluar Intellinx durante una corta "Prueba de Concepto". El producto, instalado en el ambiente de pruebas del banco, comenzó a registrar inmediatamente las actividades del usuario en el referido ambiente. Como IntellinX funciona en un servidor separado y no requiere la instalación de software o hardware adicional en el servidor o en los clientes, no hay impacto de performance en el servidor, clientes o red, y tampoco hay riesgos para las operaciones tradicionales de IT. La "Prueba de Concepto" provee un juego completo de auditoría exigido por las regulaciones del Banco Central de Israel. Como ese juego de datos de auditoría consiste en datos sensibles, fueron evaluados diversos aspectos de seguridad. IntellinX adhirió a los requisitos estrictos de seguridad del banco, incluyendo codificación y firma digital de los datos grabados que pueden ser aceptados para utilizarlos en acciones legales ante la justicia. Como los resultados de la "Prueba de Concepto" fueron positivos, el Banco Leumi decidió cambiar rápidamente, adquiriendo el producto y utilizándolo en su ambiente de producción. La conformidad con la nueva regulación fue obtenida el 1 de julio de 2004, con registro 7x24 de todos los usuarios de mainframe. Inicialmente, el producto fue usado en su formato original, permitiendo la exhibición de sesiones de usuarios específicos y consultas como "¿qué usuarios tuvieron acceso y a qué cuentas de clientes específicos dentro de un determinado periodo de tiempo?". Subsecuentemente, la unidad de auditoría interna definirá las reglas de negocio para rastrear el comportamiento del usuario, disparando alertas instantáneos. Definir nuevas reglas de negocio es un proceso constante, pues nuevas reglas pueden ser aplicadas a datos grabados previamente con el objetivo de identificar cualquier irregularidad que haya ocurrido.

Por razones obvias, el Banco Leumi no puede revelar las reglas exactas que utiliza para detección de fraudes. Sin embargo, abajo hay ejemplos de reglas normalmente aplicadas en escenarios bancarios:

Ejemplo 1. En tanto las cajas de los bancos normalmente acceden detalles de la cuenta del cliente a través del número de la cuenta, raramente la búsqueda es realizada por el nombre del cliente. IntellinX puede detectar en tiempo real la caja que frecuente o continuamente busque los detalles de la cuenta a través de los nombres del cliente en una frecuencia tres veces superior a la media.

Ejemplo 2. Las cuentas de las celebridades o gerentes del banco son típicamente tratadas como cuentas de clientes comunes (no celebridades) y no son atribuidas a empleados específicos. Cuando un usuario accede continua o excesivamente a esas cuentas especiales, IntellinX puede enviar un e-mail instantáneo al auditor responsable, avisándole sobre la actividad sospechada o planes mal intencionados de explorar informaciones confidenciales del cliente.

Ejemplo 3. Los empleados del banco están autorizados a adicionar beneficiarios o cambiar el domicilio del cliente en los registros. En el caso de que el empleado frecuentemente ejecute esas acciones o en el caso que un nuevo domicilio o beneficiario sea el mismo para diferentes clientes, IntellinX puede enviar un SMS al auditor responsable.Además de eso, el sistema almacena todos los cambios hechos por el usuario en una base de datos de auditoría separada, permitiendo que el auditor verifique si los cambios fueron previamente aprobados por el cliente o si forman parte de un intento fraude.

En tanto que las reglas mencionadas pueden detectar tentativas fraudulentas, el hecho de que todas las acciones del usuario queden registradas puede impedir que ellos cometan fraude.

Luego de ejecutar el registro de IntellinX por varios meses y crear un completo juego de datos de auditoría de 10.000 usuarios finales, el Banco Leumi constató que la solución no causa impacto en el desempeño de su servidor, clientes o red y que los datos grabados (debido a su formato extremadamente compacto) ocupan menos que el disco de una PC standard. El ejecutivo además agrega "estamos muy satisfechos tanto con la funcionalidad que nos provee IntellinX como una solución no invasiva, conforme a la nueva regulación y para la detección del fraude; como así también con el soporte que recibimos de IntellinX. Ahora estamos extendiendo el uso de IntellinX como la solución principal de registro de acceso, para diferentes tipos de aplicaciones cliente/servidor".