La solution Intellinx pour les menaces internes sur AS/400

Le défi

De plus en plus de cas de fraude interne en entreprise sont rendus public, c"est la raison pour laquelle les entreprises sont davantage consciente, aujourd'hui, des menaces internes contre leurs actifs, provenant de leurs propres employées ou de leur direction, que des menaces externes. Les menaces internes proviennent essentiellement d'entités bénéficiant d'un accès autorisé aux systèmes internes et ayant la capacité de les manipuler à des fins personnelles. Ces entités internes utilisent les mêmes commandes, auxquelles elles ont accès, pour frauder et pour effectuer leurs tâches quotidiennes ; il est donc très difficile de détecter les quelques actions malveillantes parmi les très nombreuses actions honnêtes.

Les entreprises qui reposent sur la plate-forme System i (AS/400) pour leurs processus métier de base sont confrontées à des défis d'une extrême difficulté pour protéger leurs applications, développées il y a plus d'une dizaine d'années et qui n'ont pas été conçues avec les mécanismes de contrôle nécessaires pour faire face aux environnements ouverts actuels et pour se conformer aux règlementations sur la confidentialité. Ces règlementations (PCI, GLBA, HIPAA, etc.) exigent des entreprises la mise en place d'une piste d'audit de l'accès de l'utilisateur aux données sensibles du client, notamment les transactions de mise à jour et les interrogations. La piste d'audit doit comporter des informations détaillées qui permettent le suivi des utilisateurs qui ont accédé aux données d'un client donné, de l'heure des consultations et du poste de travail. Le développement d'une solution interne pour répondre à ces exigences peut réclamer d'immenses efforts car des milliers de programmes d'application de ces entreprises risquent de devoir être modifiés.

Les différentes solutions

Différents types de solutions sont maintenant disponibles sur le marché pour gérer les menaces internes et créer des pistes d'audit d'accès de l'utilisateur sur les systèmes AS/400. Certaines solutions reposent sur des sorties du système d'exploitation System i. Ces solutions sont invasives et peuvent causer des dommages et entraîner des temps d'inactivité très coûteux sur le serveur du System i. D'autres solutions proposent d'enregistrer et de relire des écrans d'utilisateur sur le protocole 5250. Ces solutions ne fournissent néanmoins que des capacités de recherche limitées de contenu d'écran enregistré, ce qui pose un problème pour assurer l'efficacité de la piste d'audit. Par ailleurs, la relecture d'écran est limitée sur la plate-forme System i et elle ne peut prendre en charge aucune autre plate-forme. Cela affecte les performances et absorbe d'énormes espaces disque très coûteux du System i. D'autres types de solutions reposent sur le journal d'audit du System i qui fournit des informations sur l'accès de l'utilisateur aux tables de la base de données ; en revanche ce journal ne fournit pas d'informations détaillées sur les champs spécifiques auxquels a accédé l'utilisateur. Ces solutions s'avèrent donc insuffisante et peuvent entraîner des temps d'inactivité également. Citons un dernier type de solution, basé sur l'analyse des journaux de la base de données et qui fournit des informations sur les transactions de « mise à jour » uniquement et non sur les interrogations et les actions en « lecture seule ».

La solution Intellinx

Intellinx est une révolution dans la détection et la prévention des menaces internes. Intelllinx présente un système de surveillance multi-plateforme, unique en son genre, pour une visibilité inégalée de l'activité de l'utilisateur final sur la plate-forme System i et d'autres plates-formes de l'entreprise. La solution Intellinx fournit une infrastructure stratégique permettant de lutter contre les fraudes internes et les fuites d'information responsabilisant ainsi les utilisateurs autorisés. Intellinx est la seule solution du marché proposant les fonctionnalités suivantes :

- **Visibilité inégalée de l'activité de l'utilisateur final** – Visibilité complète de l'activité de l'utilisateur final grâce à la reconstitution visuelle de chaque écran, de chaque frappe sur clavier et de chaque message client/serveur, sur chacune des applications des principales plateformes, notamment System i, Mainframe, Web, Client/Serveur, MQ, etc. Toutes les actions sont visibles, y compris les mises à jour et les actions en lecture seule. Tous les types d'utilisateurs finaux sont suivis, y compris les utilisateurs finaux privilégiés tels que les administrateurs système et les administrateurs de base de données qui peuvent exposer leur société à des risques majeurs puisqu'ils disposent d'un niveau de permission plus élevé.
- **Piste d'audit complète** - Intellinx enregistre toutes les activités des utilisateurs, 24 heures sur 24, 7 jours sur 7, ce qui est essentiel pour responsabiliser les utilisateurs. Que des règles de détection appropriées soient en place ou non au moment d'un événement, la relecture post-événement permettra, ultérieurement, une enquête judiciaire.
- **Recherche sur multi-plateforme y compris sur système patrimonial** - Intellinx propose une solution unique de suivi de l'activité de l'utilisateur sur toutes les plates-formes principales existantes telles que System i, Mainframe, Web, Client/Serveur, MQ, etc. Il vous permet de rechercher une valeur donnée affichée sur un écran d'utilisateur multi-plateforme à partir d'un simple écran de recherche. Les règles Intellinx suivent les processus

métier multi-plateforme. Par exemple, un processus métier suivi par Intellinx peut commencer sur une plate-forme iSeries, continuer sur une application client-serveur et finir sur le Web.

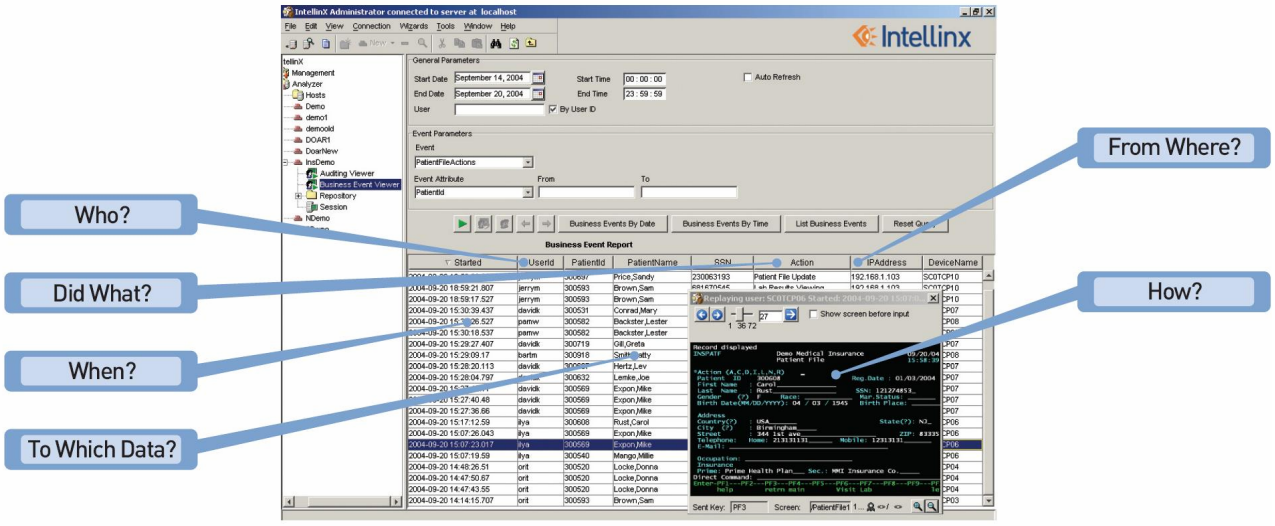
- **Suivi du comportement de l'utilisateur au niveau de l'application** - Intellinx est la seule solution du marché qui analyse l'activité de l'utilisateur au niveau de l'écran d'application (et non au niveau du réseau ou de la base de données). Les règles d'Intellinx suivent toutes les frappes sur clavier et le flux d'écrans auxquels a accédé l'utilisateur, en détectant le processus métier approprié, y compris chaque valeur de champ atteinte ou mise à jour. Ces informations sont reliées, en temps réel, à l'activité d'autres utilisateurs finaux, avec d'autres activités et d'autres types d'informations, générant des alertes en cas de comportement suspect en temps quasi réel.

La solution prête à l'emploi d'Intellinx

Intellinx propose une valeur métier exceptionnelle, prête à l'emploi. Immédiatement après l'installation (en quelques heures seulement, en général), Intellinx commence à capturer l'activité de l'utilisateur dans l'entreprise, permettant aux auditeurs internes d'effectuer des enquêtes approfondies grâce à une relecture visuelle complète. Les agents de la sécurité peuvent rechercher immédiatement tous les écrans d'utilisateur sur lesquelles certaines valeurs données sont apparues, pendant une période donnée, sur chacune des applications de chaque plate-forme principale de l'entreprise. Les entreprises profitent immédiatement des avantages de la solution Intellinx qui n'exige aucune intégration, souvent prenante en termes de temps, aux systèmes de l'entreprise ni aux configurations de l'application.

Une implémentation sans risque

- La technologie en instance de brevet et sans agent d'Intellinx intercepte la communication entre les utilisateurs finaux et les serveurs de l'entreprise en reniflant les transmissions réseau sur les différents commutateurs réseau. Ainsi, Intellinx **n'altère pas les performances des hôtes ou des réseaux, de quelque manière que ce soit.**
- L'architecture Intellinx est souple et extensible, offrant ainsi une solution rentable aux entreprises comptant de 500 à 100 000 employés.
- Il n'est pas nécessaire d'installer un autre logiciel ou du matériel supplémentaire sur l'hôte ou les clients.
- Les enregistrements de fichier sont chiffrés et comportent une signature numérique, les rendant ainsi potentiellement recevables auprès des tribunaux.
- Le processus d'installation rapide (en quelques heures) ne présente aucun risque pour les opérations IT courantes.
- Intellinx fait le suivi de l'activité de l'utilisateur sur les toutes les plates-formes principales : mainframe, iSeries, Client/ Serveur, Web (Intranet), etc.
- Les enregistrements sont stockés sous format très condensé, permettant ainsi la surveillance de dizaines de milliers d'utilisateurs finaux au sein de l'entreprise, sans aucune conséquence sur l'espace disque.



Valeur métier unique

Intellinx offre un retour sur investissement aux entreprises, leur permettant ainsi d'ajouter des contrôles sans augmenter la charge sur la plate-forme très coûteuse System i ou d'autres serveurs hôtes. Grâce à la valeur métier unique d'intellinx les grandes entreprises internationales peuvent :

- **Réduire les pertes liées aux fraudes internes** en décelant les fraudes et autre activité malveillante en temps réel. Dans son rapport 2006, l'Association américaine Certified Fraud Examiners estime que les sociétés américaines perdent, en moyenne, 5 % de leurs revenus annuels en fraude interne, commises, pour la plupart, par des employés des sociétés eux-mêmes. Economiser ne serait-ce qu'une partie des pertes dues à ces fraudes grâce à Intellinx, justifie l'investissement lié à l'implémentation d'Intellinx.
- **Se conformer à la norme PCI et aux autres règlementations** en générant une piste d'audit détaillée, multi-plateforme de tout accès aux données sensibles du client sans avoir à changer une seule ligne de code.
- **Renforcer l'efficacité de l'audit interne** en lançant une alerte à la détection d'un comportement suspect et en procurant une visibilité complète aux auditeurs internes de toutes les actions de chaque utilisateur final suspect donné, comme s'ils regardaient par-dessus son épaule.
- **Faire valoir les consignes de sécurité d'entreprise** en diagnostiquant les brèches de sécurité et les exceptions.
- **Décourager les utilisateurs frauduleux potentiels** en les informant simplement que leurs actions sont enregistrées.
- **Protéger la marque** et la valeur marché contre les dommages causés par la mauvaise publicité qu'entraînent les cas de fuite d'information et d'usurpation d'identité.

A propos d'Intellinx Ltd.

Intellinx Ltd. est le leader des solutions de suivi du comportement de l'utilisateur final pour protéger les entreprises des menaces internes. La solution Intellinx permet aux grandes entreprises de faire face au défi que constituent les fraudes internes commises par des utilisateurs finaux autorisés à accéder aux applications métier internes. Intellinx détecte les tentatives de fraude et les fuites d'information en temps réel en générant une piste d'audit légale très détaillée de l'accès de l'utilisateur aux données et aux applications de l'entreprise. Cela permet aux entreprises de se conformer aux règlementations gouvernementales telles que PCI, GLBA, HIPAA, Sarbanes-Oxley et Bâle 2. La technologie en instance de brevet et sans agent d'Intellinx est sans risque pour l'infrastructure de l'entreprise et n'entraîne aucun temps d'inactivité.

Intellinx Ltd. a été fondée en janvier 2005 à partir de Sabratec Ltd., leader des solutions d'intégration patrimoniale, à la suite de l'acquisition de Sabratec Ltd. et de sa division d'intégration patrimoniale par Software AG, La division Intellinx de la société fut alors recréée en société, Intellinx Limited, concentrant ses activités sur le développement, la prise en charge et la commercialisation des solutions de suivi du comportement de l'utilisateur final. Les produits d'Intellinx Ltd. sont vendus et pris en charge directement par la société, sa filiale américaine, Intellinx Software, Inc., ainsi que par son réseau international de distributeurs et de partenaires en Amérique du Nord, en Amérique latine, en Europe, en Afrique du Sud et en Asie Pacifique. Parmi la clientèle d'Intellinx à travers le monde, citons de grands établissements financiers, organismes de santé et autres entreprises gouvernementales.