Suite d'Audit et de Sécurité chez Banque de Luxembourg

CASE STUDY

A propos de Banque de Luxembourg

Banque de Luxembourg est l'une des plus importantes banques privées au Luxembourg, avec un bilan de 12,8 milliards d'euros en 2006 et plusieurs implantations au Grand-Duché. Créée en 1920, Banque de Luxembourg a acquis un savoir-faire et une expertise uniques en gestion de patrimoine et offre à ses clients un large éventail de solutions de gestion de portefeuilles.

Elle a été parmi les premières à utiliser l'e-banking et elle a mis en place une plateforme Internet ultramoderne pour fournir l'accès aux comptes, relevés bancaires et placements 24/24 7/7. Ce système a très vite représenté une part importante de l'ensemble des opérations bancaires effectuées et la banque enregistre actuellement plus de 30 000 accès distants sécurisés par jour.

Face au développement des services à distance mis à la disposition des clients, les responsables se sont très vite rendu compte de la nécessité d'adapter le niveau de sécurité à ces services pour les années futures.

En 2003, Banque de Luxembourg a réuni une équipe d'experts pour évaluer la possibilité de renforcer la sécurité de son système pour atteindre deux objectifs primordiaux :

- Permettre à la banque d'augmenter l'activité de sa capacité d'audit pour répondre aux demandes croissantes sur ses serveurs System i.
- Proposer une méthode centralisée pour contrôler et gérer de manière sécurisée les accès des utilisateurs et notamment les accès via ODBC, FTP, TELNET, IFS, etc pour les utilisateurs à distance.

BANQUE DE LUXEMBOURG

« Notre mission est de surveiller et de sécuriser les accès à notre plate-forme bancaire. Parmi tous les outils testés, le couple QJRN/400 - CONTROLER est de loin le plus efficace, facile à implémenter et à paramétrer, n'affectant pas les ressources machine, et personnalisable.

La réactivité de Cilasoft pour répondre à nos besoins ou problèmes est incomparable tant par la rapidité que par la qualité.

C'est devenu un outil précieux et incontournable pour nous ».

René CHEVREMONT
Responsable Sécurité Informatique

La problématique

Outre la gestion de plus de 750 utilisateurs dans plusieurs pays, le nombre élevé des opérations réalisées en ligne et enregistrées quotidiennement ou de manière hebdomadaire par la banque constituait une problématique importante pour l'équipe IT. Le volume des données enregistré par jour dans les récepteurs des journaux pouvait dépasser 15 Gigabytes pour la base de données et 5 Gigabytes pour les évènements systèmes. Le logiciel de sécurité choisi devait s'adapter aux applications en place et rester compatible avec ce niveau d'activité sans affecter les performances ou accroître les besoins de stockage en ligne.

L'autre point important était la nécessité d'installer une solution compatible avec les applications métier et le système de Haute Disponibilité utilisés par la banque : OLYMPIC Banking System, le logiciel bancaire d'ERI BANCAIRE, et le produit de Haute Disponibilité de VISION.

L'accès aux applications bancaires était déjà contrôlé par une ancienne solution. Cependant, comme la banque poursuivait le développement de ses divers services et généralisait l'accès à ses serveurs System i, il était évident qu'une meilleure gestion des accès des utilisateurs s'imposait. Au-delà de l'accès 5250 traditionnel, la banque a anticipé le besoin de prendre en compte un certain nombre de points d'exit (FTP, DDM, ODBC, DRDA, etc) dans son système. En plus de la flexibilité demandée pour couvrir les différents points d'exit, la solution de sécurité devait aussi présenter un niveau d'automatisation qui minimiserait les ressources nécessaires pour gérer les points d'accès, les droits et les applications.

Adaptabilité, performance et compatibilité étaient trois des caractéristiques majeures que Banque de Luxembourg devait prendre en compte pour sa solution de sécurité.

Le choix

Les responsables ont établi une liste des priorités concernant les besoins et ils ont évalué pendant quelques mois diverses solutions de sécurité pour leur System i. Dès le début, ils ont étudié les meilleures technologies, mais ils se sont rendu compte de l'avantage que présenterait l'utilisation d'une seule interface s'ils parvenaient à trouver une solution capable de répondre à leurs besoins complexes à la fois en termes d'audit et de contrôle d'accès.

Après une évaluation détaillée, Banque de Luxembourg a sélectionné la Suite d'Audit et de Sécurité de Cilasoft qui comprend **QJRN/400**, solution d'audit, et **CONTROLER**, logiciel de contrôle d'accès. Leur choix a été motivé par un certain nombre de critères, parmi lesquels :

- La capacité de **QJRN/400** à auditer aussi bien la base de données que les évènements systèmes.
- L'impact sur les performances de la machine – Au terme de la longue période d'évaluation des différentes solutions, il a été constaté que la suite logicielle de Cilasoft n'avait pas d'impact sur les performances de l'ensemble du système.
- Solution complète qui comprend également **CONTROLER** pour la gestion des programmes d'exit.
- La possibilité de sécuriser les accès au System i de manière sécurisée quel que soit le protocole utilisé.
- Les divers formats de rapports - **QJRN/400** offre de nombreuses possibilités de planification de rapports, d'alarmes et d'alertes email dans un format personnalisable pour pouvoir répondre aux besoins spécifiques des auditeurs externes et du personnel de l'entreprise.

Le résultat

La première étape de mise en œuvre du système de sécurité a été complètement réalisée en moins de deux semaines et au cours des deux années suivantes le système a été amélioré au fur et à mesure pour prendre en compte un nombre important de vulnérabilités supplémentaires.

La banque a très vite utilisé **QJRN/400** de manière efficace pour générer divers rapports standards et personnalisés pour les auditeurs, des emails et des fichiers PDF envoyés en fonction des besoins. Les rapports sur les données sensibles, par exemple, sont adressés uniquement aux personnes faisant partie du « Governance Committee », alors que d'autres rapports sont distribués au « Support Group ».

CONTROLER a également été installé par la banque dans le cadre de son projet de sécurité. Aujourd'hui, **CONTROLER** gère les accès au System i : tous les évènements sont logués, compressés et isolés dans une log mensuelle et stockés en ligne pendant six mois. Comme **QJRN/400**, **CONTROLER** peut générer des alertes pour des évènements et des commandes sensibles spécifiques. Le Responsable de la Sécurité crée des alertes de manière sélective et planifie leur déclenchement.

En janvier 2006, Banque de Luxembourg a adopté le module d'Audit des moteurs SQL/QRY nouvellement intégré dans **CONTROLER**. Grâce à cette nouvelle fonctionnalité, la banque peut désormais avoir une vision globale de tous les accès aux fichiers de production via STRSQL, WRKQRY, RUNQRY, RUNSQLSTM, DRDA, etc. Bien que contrôler les accès via SQL soit une tâche difficile, **CONTROLER** a réussi sans impact sur l'ensemble des performances du système.

Conclusion

Les réactions qui ont suivi l'installation de la Suite d'Audit et de Sécurité de Cilasoft ont été très positives. Les auditeurs internes et externes ont été satisfaits de la capacité des solutions à générer des rapports précis et synthétiques. De plus, aujourd'hui le processus d'audit et de mise en conformité a été considérablement automatisé, ce qui permet aux équipes IT de ne plus consacrer de temps à la collecte des informations, à la gestion des accès des utilisateurs et à la restitution des données dans des rapports lisibles et compréhensibles pour les auditeurs.

IBM Business Partner

IBM Server Proven

CILASOFT
ZI les Iles, 190 route des Sarves – F-74370 Metz Tessy – FRANCE
Tél : +33 4 50 69 45 98 | Fax : +33 4 50 69 45 99
Email : contact@cilasoft.com | Web : www.cilasoft.com