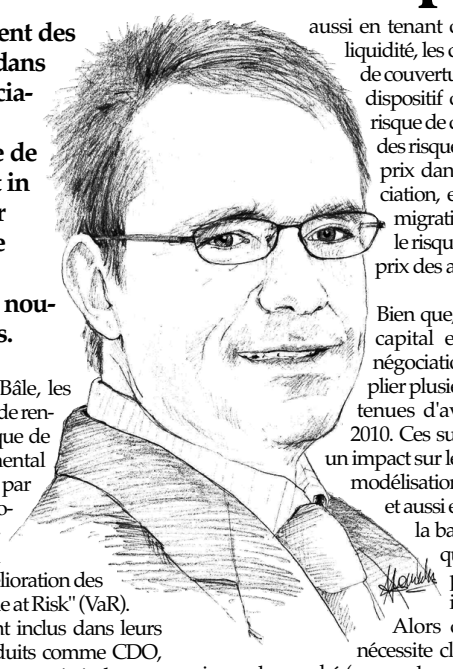
Plates-formes IT : L'impact des nouvelles normes 'trading book'

Les banques qui possèdent des positions importantes dans le portefeuille de négociations sont les plus impactées par la crise. La récente faillite de Lehman Brothers et le rachat in extremis de Merril Lynch par Bank of America ne font que renforcer les arguments en faveur d'une instauration de nouvelles normes réglementaires.



Cependant, à travers le Comité de Bâle, les régulateurs ont déjà essayé d'une part de renforcer les exigences concernant le risque de marché grâce au calcul de l'"incremental default risk" (IDRC), et d'autre part par une approche plus avancée, d'améliorer la mesure de l'exposition des dérivés OTC ; "effective EPE". Tout d'abord le principal intérêt de l'IDRC est l'amélioration des faiblesses de la méthodologie de "Value at Risk" (VaR). Ces dernières années les banques ont inclus dans leurs portefeuilles de négociation des produits comme CDO, CDS et autres produits exotiques, qui sont généralement moins liquides, ce qui entraîne une augmentation du risque de défaut. Ces risques étaient censés être capturés dans des modèles de risque, mais cela s'est révélé difficile à saisir de manière adéquate avec la méthodologie de VaR actuelle. Le comité de Bâle a instauré un nouveau seuil minimum de fonds propres réglementaires, qui reflète le risque de défaut sur un horizon temporel d'un an mais aussi en tenant compte de l'impact de la liquidité, les concentrations et de risque de couverture. Désormais ce nouveau dispositif d'IDRC vise à capturer le risque de défaut ainsi que l'ensemble des risques liés aux mouvements de prix dans le portefeuille de négociation, en particulier le risque de migration de la qualité de crédit et le risque associé aux variations du prix des actions.

Bien que, dans le cas de l'IDRC, le capital exigé de portefeuille de négociation pourrait même multiplier plusieurs fois, les banques étant tenues d'avoir une approche pour 2010. Ces sujets d'actualité vont avoir un impact sur les exigences en matière de modélisation, de gestion de données, et aussi en termes d'architecture de la banque. IDRC est un calcul qui a été ajouté dans Basel II pour compléter le modèle interne de marché VaR. Alors que le calcul de la VaR nécessite clairement des facteurs de risque de marché (ex. courbes de taux, taux de change et courbes de volatilités), l'IDRC exige des données de crédit similaires à celles de l'approche IRB ("Internal Rating Based") comme probabilité de défaut (PD), perte en cas de défaut (LGD), exposition à valeur par défaut (EAD) et enfin le risque de liquidité et concentration. On peut noter une tendance similaire quant aux calculs du risque de crédit (effective EPE) pour les dérivés OTC. Cette approche "effective EPE", plus avancée que l'approche conservatrice, qui se base sur le coût de remplacement avec add-on, est maintenant autorisée pour calculer les expositions potentielles futures des dérivés OTC. Elles prennent en compte les effets du portefeuille de négociation dans l'exposition ainsi que de l'amélioration du traitement de compensation avec déchéance du terme des accords, à l'appui de multiples produits de compensation. Ces changements, au niveau du risque de contrepartie, permettent à une banque de réduire sensiblement les besoins en capitaux dans leurs portefeuilles de négociation. Ces simulations nécessitent un besoin de données de marché important et de techniques de réduction des risques comme la compensation, la gestion du collatéral et des garanties exigent le stockage des données du risque de crédit. Les méthodes de calcul pour des sujets tels que les risques futurs potentiels et les risques par défaut sont généralement mises en œuvre par le biais d'un moteur quelconque. Dans la mesure où ces notions deviennent de plus en plus complexes, la sophistication de ces moteurs commence à se développer et le risque d'infrastructure doit être conçu en suivant cette évolution. Par exemple le moteur qui doit calculer les risques futurs potentiels doit gérer un grand nombre de calculs en fonction du nombre de transactions, simulations et des périodes temporelles.

La simulation soit souvent utilisée par les banques pour les produits dérivés plus simples comme les swap sur taux d'intérêt. En revanche, lorsqu'il s'agit de produits dérivés, plus complexes et structurés, il n'existe aucun travail d'implémentation validé et appliqué. De nombreuses institutions font encore la modélisation de leur exposition sur base de catégories d'actifs silos plutôt que de prendre une vue globale. Le "credit crunch" a considérablement réduit l'appétit pour ces instruments et en particulier les CDO et CDO square. Néanmoins certains instruments restent très populaires ; comme par exemple les CDS. De nouveaux produits sont constamment introduits sur le marché des produits dérivés et l'incapacité à intégrer un nouveau produit et son modèle d'évaluation peut rapidement limiter certaines opportunités pour le front-office. Il est important que les banques puissent facilement introduire de nouveaux produits et mettre en œuvre leurs propres modèles pour les calculs de l'"effective PFE". D'autre part, dans une optique de modélisation des composants de risque de crédit pour l'IDRC comme probabilité de défaut (PD) et de perte en cas de défaut (LGD) la banque ,et plus spécifiquement le front-office, doit être capable d' identifier de façon rapide et efficace l'impact au niveau du capital exigé après l'insertion de chaque nouvelle transaction. Mais en dehors de l'aspect performance, la solution informatique doit également être évolutive, fiable et assez extensible pour être déployée aux nouvelles conditions du "trading book" – y compris celles des futures régulations. On va plutôt vers une architecture modulaire en utilisant "grid computing" pour répondre au besoin de la performance. "Grid computing" qui est uniquement efficace si elle est assez flexible pour tenir compte de hardware supplémentaire. Cette solution devrait en plus inclure des fonctionnalités permettant d'améliorer la transparence pour la banque et pour les régulateurs. En conséquence, les cadres supérieurs, membres du conseil d'administration et les régulateurs devraient pouvoir bénéficier d'une solution informatique, claire et transparente, qui sait clairement identifier, et analyser les expositions vers une contrepartie.

Michel Dorval,
Product Manager Enterprise-wide risk EMEA West, Thomson reuters
Michel.Dorval@thomsonreuters.com

Une première entreprise privée certifiée ISO/IEC 27001 au Luxembourg

La société Codasystem vient d'être certifié ISO/IEC 27001, preuve de la sécurité de ses processus. Le CRP Henri Tudor l'a accompagné dans la voie de la certification.

La sécurité de l'information est devenue une préoccupation importante au sein des entreprises. Dans un contexte réglementaire de plus en plus contraignant en matière de maîtrise des risques et pour répondre à une forte préoccupation des clients, la mise en place d'un système de management de la sécurité de l'information (SMSI) s'impose petit à petit comme une réponse probante. En effet, l'organisation internationale de normalisation (ISO) a publié en 2005 la norme ISO/IEC 27001 qui définit les bonnes pratiques pour la sécurité des systèmes d'information. L'ISO succède au British Standard Institute (BSI), qui fut, en 1995, le premier organisme à publier une norme dans ce domaine. Il est donc aujourd'hui possible de faire certifier son organisation pour apporter la preuve de la sécurité des processus de l'entreprise et accroître la confiance de ses clients.

C'est le choix qu'a fait la société Codasystem, jeune PME d'une dizaine d'employés, créée en 2001. L'activité de cette entreprise, située au Technoport d'Esch-sur-Alzette, repose sur la création d'originaux de photos numériques, qui ne peuvent être modifiés et qui sont conservés dans des conditions de sécurité en garantissant l'intégrité. Ainsi, Codasystem offre la possibilité à ses clients de prendre des photos avec un smartphone, puis en assure le traitement, de manière à donner force probante et permettre l'opposabilité à des tiers. Le matériel et le logiciel forment une solution homogène et légale qui certifie le document, sa date de création et sa localisation. Maîtrisant pour cela chacun des maillons de la chaîne depuis la création du document, jusqu'à son archivage, en passant par sa diffusion au destinataire final. C'est donc la spécificité de son activité et ses enjeux en termes de sécurité des informations traitées qui ont décidé Codasystem à se lancer, début 2007, sur la voie de la certification ISO/IEC 27001. De son côté, le CRP Henri Tudor s'intéresse de longue date à la sécurité des systèmes d'information. Ainsi, dans le cadre de ses projets de recherche Cassis Sécurité et "Information Security Management System pour PME" (ISMS_PME), en partenariat avec le Ministère de l'Economie et du Commerce Extérieur, le concept de "normes comme un élément moteur de l'économie du savoir" est promu. Il vise à proposer aux PME un outil adapté leur permettant de déployer leur système de management de la sécurité de l'information. Le CRP Henri Tudor, qui participe par ailleurs aux travaux du JTC1 (Joint Technical Committee) de révision de la norme ISO/IEC 27001, a donc trouvé chez Codasystem l'opportunité de tester sa démarche sur une PME luxembourgeoise du secteur IT et qui présentaient de fortes contraintes de sécurité.

L'expérimentation s'est déroulée en 8 étapes:
- Constitution et formation de l'équipe projet,
- Sensibilisation du personnel,
- Identification des processus clés, des actifs correspondants,
- Evaluation des risques associés,
- Elaboration de la politique et du plan de traitement,
- Rédaction des principaux documents du système de management (procédures, enregistrements, fiches de fonction),
- Traitement des risques et audit interne,
- Audit externe et certification.

L'entreprise a passé avec succès l'audit final au mois de mai et a obtenu le certificat quelques temps après. La réussite de cette expérimentation résulte de la capacité de la méthode à s'adapter aux spécificités d'une PME, notamment par la réduction de la structure documentaire, la limitation du nombre de processus et la responsabilisation du personnel à toutes les étapes. La démarche s'est, de plus, appuyée sur une équipe dirigeante très impliquée au quotidien dans le déploiement du système, et sur une équipe projet qui a toujours privilégié les solutions simples et pragmatiques pour convaincre le personnel. Du lancement du projet à l'audit final, 18 mois de travail ont été nécessaires. Et à l'heure du bilan, plusieurs constats s'imposent. Pour Codasystem, si l'investissement a été très important, l'implication de la direction, l'étalement dans le temps et la mise à contribution de tous ont permis de maintenir la satisfaction des clients et d'assurer la gestion des affaires courantes. Les bénéfices sont aujourd'hui au rendez-vous avec:
- une meilleure maîtrise des processus et des risques de l'entreprise,
- une approche proactive des incidents,
- un suivi continu des indicateurs clés du système d'information.

Tous ces éléments s'ajoutent au certificat pour faire progresser et promouvoir la sécurité de l'organisation et améliorer la confiance des clients. Pour le CRP Henri Tudor, l'expérience a permis de tester, de renforcer et d'adapter sa méthode de déploiement et le référentiel associé destiné aux PME. La méthode d'analyse des risques, le choix des processus, la documentation et la gestion du projet ont notamment fait l'objet d'une approche spécifique. Ainsi, le projet a grandement contribué au développement d'un guide à usage des PME luxembourgeoises, qui doivent faire face à des menaces numériques grandissantes, sans disposer des meilleures armes pour se protéger. Ce référentiel est en cours d'amélioration, avec le concours de l'ANSIL (Association de Normalisation pour la Société de l'Information du Luxembourg), et plus particulièrement de son groupe CNLSI (Comité de Normalisation Luxembourgeois pour la Sécurité de l'Information), ainsi qu'avec d'autres phases d'expérimentation dans les mois à venir. Issu d'un projet fortement supporté par le Ministère de l'Economie et du Commerce Extérieur, le guide a vocation à être ensuite largement diffusé afin de contribuer à la sensibilisation des PME, à l'accroissement de la sécurité de leurs informations et à la confiance des acteurs du marché.

Pour plus de renseignements sur le projet et sur les expérimentations à venir, vous pouvez contacter Sébastien Pineau (tel: +352 52 59 91 844 | e-mail: sebastien.pineau@tudor.lu) ou Béatrix Barafort (tel : +352 42 59 91 263 | beatrix.barafort@tudor.lu).

Sébastien Pineau (Ingénieur R&D – CRP Henri Tudor) et
Nicolas Mayer (Ingénieur R&D – CRP Henri Tudor)

Clearstream adopte la solution EMX Message System

Clearstream Banking SA a adopté la solution EMX Message System en tant qu'outil de consolidation à compter du 11 août 2008. Vestima+, le service pour les fonds d'investissement de Clearstream, facilitera le traitement automatisé (Straight Through Processing) des ordres passés par les clients étrangers sur la place boursière britannique grâce à ce lien vers la solution EMX Message System.

Philippe Seyll, Director, Investment Funds chez Clearstream a déclaré: "Le lien vers EMX Message System permettra à Clearstream d'offrir un routage d' ordres électronique pour les fonds domiciliés au Royaume-Uni en recourant à l'infrastructure existante du marché. Combiné à l'offre intégrée de conservation et de dénouement de Clearstream, il offrira à l'ensemble de ses clients un routage d'ordres traités intégralement par voie électronique et une solution de dénouement pour les fonds d'investissement domiciliés au Royaume-Uni". Jane Sidnell, Head of Continental Europe au sein d'EMXCo, a ajouté: "Depuis l'ouverture de notre bureau au Luxembourg en 2004, notre activité transfrontalière n'a cessé de croître et je suis ravie d'accueillir Clearstream au sein d'EMX Message System. Voir d'autres établissements de premier ordre, non domiciliés au Royaume-Uni, nous rejoindre pour utiliser notre infrastructure de marché est la preuve de l'étendue de l'aptitude de notre service." En dépit de conditions de marché difficiles, EMXCo a connu une croissance exceptionnelle, plus de 11 millions de messages ayant transité par EMX Message System au premier semestre 2008, soit une augmentation de plus de 20% en glissement annuel.

ESET Smart Security

La protection de l'entreprise

Spywares (logiciels espions), chevaux de Troie, vers, (ro)bots et phishing sont aujourd'hui le lot commun de tous les internautes… et de toutes les entreprises. Pour intercepter ces attaques au premier stade de leur développement, ESET l'éditeur de l'antivirus NOD32 a conçu une suite sécuritaire. Son nom: ESET Smart Security. Son slogan "Zero-Day Attacks". Il en existe aussi une version "Business Edition".

Les risques s'intensifient et les attaques se renouvellent

Chaque mois, l'Anti-Phishing Working Group comptabilise plus de 40.000 messages de phishing. Gartner assure qu'en une année, près de quatre millions d'américains se sont fait escroquer de 3,2 milliards de dollars via le Web, et Google constate qu'un site sur dix est infecté par des maliciels (malwares) prêts à s'installer automatiquement sur les PC des visiteurs. Les dommages mondiaux provoqués par les malwares dépassaient les 13 milliards de dollars en 2006 (Malware Report, Computer Economics) et tout laisse à penser que ces tendances sont à la hausse. Parallèlement aux menaces connues, les analystes observent une recrudescence des botnets, ces réseaux de piratage capables de contrôler des milliers de PC à distance pour lancer des attaques ciblées vers les entreprises et les administrations. Avec pour conséquences d'anéantir leur activité Internet durant des heures, voire des jours, détériorant ainsi leur image et la confiance du public. Une autre évolution est l'augmentation constante des risques dans l'univers Apple/ Mac jusqu'alors protégé, mais la tendance la plus marquante concerne la mobilité : les pirates développent désormais des malwares mobiles qui ont les smartphones pour cibles. Enfin, le phishing -ou ingénierie sociale- basé sur la confiance ou la naïveté de l'utilisateur est en forte hausse pour conduire l'internaute à consulter, volontairement, des sites dangereux et les "sniffeurs" de mots de passe s'en prennent particulièrement aux joueurs en ligne (World of Warcraft) et aux acteurs des mondes virtuels comme Second life. Les applications non désirées (adware et spyware) constituent une autre tendance majeure de pollution des systèmes informatiques. S'ils sont rarement destructeurs, ils peuvent réduire fortement les performances des PC affectés. En revanche, l'usage des fichiers attachés comme véhicule de malwares perd en virulence, même si les anciennes menaces de ce type (Netsky) existent toujours sur les machines non protégées. Source : "The mid-yearly Threat Report- ESETt".

Léger et rapide… même sur d'anciens PC

ESET Smart Security se décline en une suite sécuritaire complète, composée de l'antivirus NOD32 V3.0, d'un antispyware, d'un antispam et d'un pare-feu. Outre une efficacité maximale, les principaux atouts de ESET Smart Security sont un faible encombrement (40 Mo de mémoire disque), un taux de faux positifs (fausses alarmes) très réduit et une parfaite intégration de ses différents composants au sein d'une nouvelle interface. ESET Smart Security s'installe en moins d'une minute sans imposer le redémarrage de Windows et sa procédure de lancement est très courte. Ce qui autorise l'installation de Smart Security sur des PC peu puissants ou disposant d'une mémoire RAM limitée. En début d'année, la suite ESET Smart Security, comprenant l'antivirus ESET NOD32 (élu antivirus de l'année 2006 et 2007 par "AV-Comparative") a été récompensée par une note "Advanced+" par le laboratoire de tests indépendant "AV-Comparatives".

"Zero-Day Attacks": anticiper les menaces pour prévenir les attaques

La philosophie de protection de l'éditeur antivirus ESET repose sur l'anticipation plus que sur la réaction face à ces innombrables menaces. Elle utilise pour cela deux techniques propres: les définitions génériques et la détection heuristique. La détection des signatures génériques plutôt que des variantes d'un même code malveillant, permet de les intercepter toutes, y compris les versions non encore répertoriées. Parallèlement, la détection heuristique est basée sur l'analyse des caractéristiques et du comportement des programmes scannés. L'ambition de cette technologie proactive consiste à identifier les attaques "nouvelles" durant la période de 2 à 3 heures pendant laquelle les filtres basés sur les empreintes connues demeurent inefficaces. C'est ce que ESET nomme le concept de "Zero-Day attacks". Les signatures génériques et l'analyste heuristique associées aux listes de signatures virales conventionnelles permettent d'élargir considérablement le spectre de détection des menaces de tout type.

Veille sécuritaire permanente

La protection logicielle proprement dite est secondée par deux outils de veille technologique. Le premier est l'ESET Threat Center qui étudie en permanence l'évolution des menaces et leur impact sur l'activité des entreprises. Le second, baptisé "Virus Radar" piste l'évolution des menaces en temps réel en scannant le trafic Internet des fournisseurs d'accès dans le monde entier (www.virusradar.com). Les statistiques de scanning du Virus Radar montrent, par exemple, que l'e-mail demeure un vecteur majeur de transmission des URL malveillants.

Business Edition

La Business Edition de la suite sécuritaire permet de gérer la ESET Smart Security au cœur de l'entreprise. Avec l'aide d'une console d'administration centralisée, l'administrateur système peut se constituer des configurations paramétrées du logiciel calquées sur la politique de sécurité de l'entreprise et s'assurer ainsi de la gestion centralisée dans un environnement de réseau.

MGK Technologies