MAÎTRISE DES RISQUES

Gérer l'ouverture du SI en toute sécurité

Yoann Le Corvic
Consultant sécurité
Aedian SI
En collaboration avec Ibrahim Mouci

Les politiques de sécurité doivent s'adapter à l'ouverture des systèmes d'information aux clients via la banque en ligne et à des partenaires de plus en plus nombreux, fournisseurs ou sous-traitants. Elle doit aussi couvrir les prestations externalisées de l'établissement.

Les SI bancaires et financiers sont de plus en plus ouverts : portails *corporate*, institutionnels, opérations de Bourse, de virement, relations avec les organismes de place ou de tutelle, croissance des paiements en ligne, externalisation accrue des traitements du patrimoine applicatif pour satisfaire aux exigences d'optimisation (entrée dans l'air du *cloud computing*). Cette tendance à l'ouverture est appelée à s'accélérer : les utilisateurs sont demandeurs et s'appuient de plus en plus sur de nouveaux outils qui les impliquent davantage dans la chaîne de valeur du SI : les architectures orientées services, les solutions de bus d'entreprise et de BPM contribuent largement à tisser des liens qui transforment petit à petit l'environnement de l'entreprise en l'amenant à fonctionner dans un modèle d'interconnexions avec des partenaires, des fournisseurs, et des clients. Ainsi, les frontières du SI sont plus floues.

ÉLARGIR L'HORIZON DE LA POLITIQUE DE SÉCURITÉ

Augmentation des flux, ouverture du SI, délégation d'un sous-ensemble du SI à un partenaire, fonctionnement dans un mode d'entreprise éclaté ou en réseau : l'organisation de la sécurité au sein de l'entreprise doit s'adapter à ces évolutions et la politique de sécurité doit élargir son horizon afin d'embrasser plus de disciplines et jouer un rôle de gardien avancé et de protecteur de l'information.

« Dans le cadre d'une activité externalisée, il faut limiter au strict minimum l'accès par le prestataire aux données confidentielles de l'entreprise. »

C'est pourquoi malgré un contexte économique complexe, les établissements financiers ont fait de la sécurité de leur SI une de leurs priorités.

L'OUVERTURE CONTRÔLÉE DES SI

Les enjeux généralement pris en compte dans les volets sécurité des démarches projet sont le plus souvent :
– le respect du cadre réglementaire et légal (*cf.* CRBF, Bâle II, Sox, CNI, PCI/DSS…) ;
– l'image de marque ;
– la continuité d'activité ;
– la lutte contre la fraude et les autres types de menaces.
Dans une démarche de gestion des risques liés à l'ouverture croissante du SI, l'expérience démontre l'intérêt de prendre en compte quatre points clés :
– la politique de sécurité ;
– le catalogue de solutions ;
– la sécurité dans les projets ;
– le contrôle permanent.

LA POLITIQUE DE SÉCURITÉ

Une organisation sécurité claire s'impose, à partir de laquelle sont définies des politiques de sécurité détaillant les axes stratégiques de la protection de l'information. Il est vital de couvrir également les aspects « externalisation » d'une partie de SI.

LE CATALOGUE DE SOLUTIONS

Des moyens techniques, financiers et humains permettant l'étude, la définition, la mise en œuvre et l'exploitation de solutions de sécurité transversales sont nécessaires.

Les banques ont pour ambition de transformer leur informatique en centre de profits. Cela se traduit par la mise en place d'une offre de service de plus en plus complète qui devrait permettre à court terme aux maîtrises d'ouvrage et maîtrises d'œuvre projet de sélectionner les modules de sécurité « à la demande », sous réserve que le module soit présent dans le catalogue. Dans la pratique, ce catalogue de services est encore à l'état de préparation pour nombre d'établissements bancaires, mais le principe est bien là.

LA SÉCURITÉ DANS LES PROJETS

La prise en compte de la sécurité par les MOA et MOE de tout projet (bancaire ou technique) requiert une analyse de risque adaptée et si nécessaire l'utilisation de services de sécurité standard.

Si, par exemple, une maîtrise d'ouvrage souhaite proposer un service de consultation de données bancaires en ligne, la maîtrise d'œuvre sera très probablement contrainte d'héberger des briques applicatives (la partie exposée du service) sur une architecture de sécurité existante et pourra sélectionner dans un catalogue, dans la limite de l'offre, les services de sécurité disponibles pour répondre aux besoins exprimés.

En fonction de la criticité du service proposé, il sera alors possible de choisir un module « disponibilité » permettant de garantir un taux de disponibilité plus ou moins élevé en fonction des options retenues : de la simple redondance des équipements réseau jusqu'à de la haute disponibilité de l'infrastructure, des systèmes et des applicatifs avec possibilité de gérer la répartition de la charge pour optimiser les performances.

« Les banques ont pour ambition de transformer leur informatique en centre de profits. Cela se traduit par la mise en place d'une offre de service de plus en plus complète qui devrait permettre aux MOA et MOE de sélectionner les modules de sécurité « à la demande ». »

De la même manière, la maîtrise d'œuvre pourra choisir parmi plusieurs modules « authentification » pour positionner le curseur sur le niveau de sécurité le plus adapté : un accès en mode anonyme ou bien des modes d'authentification plus adaptés à la consultation de données sensibles allant jusqu'à l'authentification forte par *token*.

Partant du même principe, la maîtrise d'œuvre pourra aussi sélectionner des modules « intégrité », « confidentialité », « preuve/traçabilité » et d'autres modules associés à toutes les fonctions de sécurité permettant de réaliser l'exploitation au quotidien du nouveau service mis en œuvre (détection d'intrusion, filtrage(s), protection contre les virus, supervision, sauvegarde, inscription au plan de secours...).

Compte tenu des coûts associés à chaque service de sécurité, il est assez fréquent que des arbitrages soient nécessaires et que la décision soit prise de renoncer à certains services. La responsabilité de l'entité sécurité est alors double : d'une part s'assurer que les moyens de sécurité sélectionnés par la maîtrise d'œuvre couvrent bien les besoins exprimés par la maîtrise d'ouvrage ; d'autre part informer la maîtrise d'ouvrage des risques résiduels qui devront être acceptés avant la mise en production.

CONTRÔLE PERMANENT : LE CHALLENGE DE L'EXTERNALISATION

Un contrôle permanent par le biais d'audits internes et d'inspections n'est pleinement efficace qu'à la condition d'inclure un périmètre large : aspects organisationnels et techniques de la sécurité et, surtout, parties externalisées du SI qui sont, par nature, les plus difficiles à contrôler au jour le jour. Faire appliquer une politique de sécurité sur un site externalisé est plus complexe qu'au siège et cette complexité s'accroît avec l'éloignement.

Le contrat d'externalisation doit être clair et prévoir une clause autorisant l'audit du prestataire dans le cadre du contrôle permanent. Ce point est d'autant plus crucial lorsque l'activité est classée « essentielle » au sens CRBF : la responsabilité de ces activités « essentielles » ne peut être transférée à un tiers.

Dans le cadre d'une activité externalisée, il faut limiter au strict minimum l'accès par le prestataire aux données confidentielles de l'entreprise. Ceci passe par des contrôles d'accès ou l'anonymisation de données dans le cadre de développements (bases de données de test...).

Enfin, si l'externalisation concerne les développements, il convient de mettre sur pied des processus de contrôle de qualité et de sécurité du code afin d'éviter un effet tunnel et de mauvaises surprises lors de la livraison. Si tous ces enjeux sont pris en compte dans le cadre d'une démarche de gestion des risques, l'ouverture du SI bancaire pourra se déployer avec le niveau de sécurité adéquat. ■