

Receuil du No. 49

Accompagnement du projet: Penser à la sécurité dès le début du projet

Généralement, quand on commence à s'inquiéter de la sécurité d'une application, il est trop tard. Ce type de préoccupation apparaît généralement lorsque les développements sont achevés, et qu'on est en train d'effectuer les tests préalables à la mise en œuvre. On s'aperçoit alors que le système qu'on est en train de mettre en place, est une véritable passoire. On découvre, par exemple, que le système accepte n'importe quel type de données sans réagir ou bien qu'il produit sans sourcilier des résultats totalement ineptes. C'est parfois dû à des erreurs techniques mais, la plupart du temps, c'est la conséquence de graves défauts survenus dans la démarche de sécurité.

Il existe des situations encore plus désagréables. Ainsi, on constate, parfois, qu'après plusieurs années d'utilisation, une application a tout d'un coup de curieux comportements. L'analyse des incidents survenus montre qu'ils sont dus pour l'essentiel à une dégradation progressive du contenu des bases de données. Celle-ci est la conséquence de graves défauts des dispositifs de sécurité mis en place. Ce type de situation est, très souvent, lié au fait qu'on a pensé à la sécurité de l'application seulement après sa mise en place. Le résultat est une dégradation progressive du système due à la fragilité de sa sécurité. C'est un grave oubli, pire, c'est une erreur! En fait, il aurait été souhaitable de penser à la sécurité dès les premières étapes du projet.

En fait, la sécurité est une des composantes du projet. Il est nécessaire de la prendre en compte le plus tôt possible. C'est un facteur clé, trop souvent sous-évalué, voire négligé, car les risques liés aux projets sont généralement sous-estimés. Le management des entreprises a la responsabilité de veiller à ce que la sécurité soit correctement prise en compte. Trop souvent, on ne réagit pas, car on pense, a tort, que la sécurité est avant tout une affaire d'exploitation informatique. Cette vision a des conséquences importantes.

Il est trop tard pour y penser

Il est, bien entendu, nécessaire de prendre en compte la sécurité au moment de la mise en exploitation de l'application. La plupart des «operating system» proposent des fonctions de sécurité qui permettent d'assurer un minimum de sécurité. Il est en particulier possible de mettre en place des mesures de contrôle d'accès basés sur l'emploi de mots de passe. C'est utile, mais est-ce suffisant? L'objectif recherché est d'essayer d'éviter que n'importe qui ne fasse pas n'importe quoi dans le système informatique. Généralement, on y arrive, mais il existe des cas pendables ou certaines entreprises sont passées près du gouffre.

Tous les conférenciers spécialisés dans le domaine de la sécurité disposent

d'une étonnante collection d'histoires horribles qu'ils adorent confier à leurs auditoires ravis d'être effrayés. On a ainsi droit aux récits détaillés d'entreprises victimes d'escrocs, de joyeux plaisantins ou de techniciens imbéciles. Mais, certaines de ces histoires relèvent de l'imaginaire. Ainsi, on a de nombreuses fois décrit un grave détournement dont aurait été victime le réseau interbancaire Swift. Une défaillance dans le système de cryptage aurait permis de voler une somme considérable. Or, il n'en est rien. Une pareille affaire n'a jamais eu lieu. Mais la rumeur continue de courir.

Pour faire face à ces risques, les entreprises ont donc mis en place des systèmes de contrôle d'accès généralement efficaces. Dans les cas où on a besoin d'une sécurité renforcée, il est même possible de recourir à des dispositifs de contrôle physique comme, par exemple, des lecteurs de badges ou de cartes à puces, mais aussi des systèmes de reconnaissance de la voix, des empreintes, du visage, de la pupille... C'est un peu le concours Lépine de la sécurité. Mais il ne faut pas se faire d'illusion, tous ces dispositifs, même les plus originaux, ont des limites qu'il est important de connaître, car ils ne couvrent qu'une partie des risques.

En fait, ces différentes parades ne protègent que contre certains types de risques. L'expérience montre qu'elles concernent uniquement les risques les plus apparents pesant sur les entreprises. En fait, le principal danger n'est ni la pénétration du réseau par des «hackers» ou par des concurrents, ni la multiplication des virus. Les risques de pénétrations des systèmes d'information et le viol de secrets d'affaires

ne représentent qu'une faible partie des problèmes de sécurité. En fait, le véritable danger est lié au comportement d'un maladroit qui effectue, sans même s'en rendre compte, des opérations aberrantes, qui finissent par se traduire par des dégradations irréversibles des données, des traitements ou des informations produites. Or, face à ce type de risque, les fonctions de sécurité se trouvant dans les systèmes d'exploitation et dans les logiciels spécifiques de gestion de la sécurité, n'apportent qu'une réponse très partielle.

En fait, les risques encourus sont de différentes natures:

■ *La dégradation de données.* C'est sûrement le risque le plus significatif et probablement le plus fréquent. A la suite de manœuvres douteuses, des données importantes sont perdues et il est nécessaire de les reconstituer. Cette situation est pour le management une situation très inconfortable. La reconstitution des données peut se traduire par des dépenses importantes. C'est une perte franche et massive. Mais ce n'est pas le cas le plus grave. Il y a pire, c'est la perte insidieuse. A la suite d'une méthode de travail inadaptée, tous les jours, on dégrade un peu les informations se trouvant dans les bases de données. A chaque mise à jour, on perd quelques données et le pire c'est qu'on ne s'en rend même pas compte.

■ *Les erreurs de manipulation.* Elles sont fréquentes. C'est, par exemple, la perte des écritures comptables d'une journée au cours de la nuit suivante à la suite d'une fausse manœuvre. Le soir, une fois les écritures passées, le comptable chargé de la mise à jour des comptes se trompe de fichier et prend malencontreusement celui de la veille et efface celui du même jour. Le lende-

main les comptables découvrent avec inquiétude que les écritures de l'avant-veille sont passées deux fois dans les comptes clients et que celles de la veille ont été perdues. Mais ces erreurs peuvent aussi être dues à des fusions mal faites entre deux fichiers, à une sauvegarde des données difficiles à récupérer ou à une opération d'exploitation quotidienne mal organisée. D'une manière plus générale les erreurs de manipulation sont graves et peuvent finir par coûter très cher.

■ *Les erreurs de traitements.* Elles sont nombreuses et présentes dans toutes les applications, surtout lors qu'elles sont récentes. Ces erreurs sont infinies et l'imagination des programmeurs est, dans ce domaine, sans limite. On trouve des cas invraisemblables. Ainsi dans certaines applications, on oublie de traiter le dernier dossier, dans d'autres cas un écart est constaté mais il n'est pas signalé... Pour lutter contre ces défauts, il est nécessaire d'avoir des jeux d'essai assez complets et de les repasser périodiquement pour s'assurer que les applications ne se sont pas dégradées lors des modifications. Ceci dit, il faut savoir que, malgré les tests, de nombreuses erreurs persistent dans tous les traitements.

■ *Les erreurs aléatoires.* Ce sont les pires de toutes, car on a alors très vite le sentiment que le diable est dans l'ordinateur. Pendant des mois, voire des années, les utilisateurs effectuent quotidiennement un certain nombre d'opérations, et tout se passe bien. Puis, tout d'un coup, sans qu'on sache pourquoi, des erreurs curieuses apparaissent. Les informaticiens alertés, essaient de reproduire l'erreur, mais à ce moment elle n'apparaît plus. Fort logiquement, dans un premier temps on l'ignore et on nie l'incident. Malheureusement,

très vite, elle réapparaît. Les utilisateurs ne savent plus ce qu'il faut faire. Ils ne savent même plus qui accuser. C'est le genre de situation qui rend fou.

La multiplication des erreurs de conception ou de réalisation est un facteur d'insécurité. Elles sont d'autant plus grave qu'on ne dispose pas d'outils permettant de maîtriser facilement cette situation. C'est pour cette raison, qu'il est nécessaire de prendre en compte la sécurité dès les premières étapes du projet. Elle n'est pas seulement un ajout fait au moment de la mise en place de l'application. En fait, la sécurité est un point essentiel du projet et doit être prise en compte le plus tôt possible.

Il fallait y penser plus tôt

En fait, si on n'y pense pas dès l'étape de conception, il y a de fortes chances qu'on n'y pense jamais, ou du moins cela risque d'être trop tard, et à ce moment il risque d'être très difficile d'arriver à corriger les défauts constatés. Pour cette raison, il est nécessaire de penser à la sécurité dès le dossier d'expression des besoins ou la fiche d'investissement. Il est notamment très important que les futurs utilisateurs puissent s'exprimer sur ce sujet et proposent une ou plusieurs orientations relatives à la sécurité.

Ces orientations doivent ensuite être reprises et développées dans le cahier des charges. Il est souhaitable qu'un chapitre entier soit consacré à la sécurité. Cela fait partie des spécifications de base de l'application. Il est, en particulier, très utile de repérer assez vite les principaux risques liés à des

défauts de sécurité et de proposer des parades efficaces permettant de limiter leur impact. L'expérience montre qu'il existe trois grands types de risques liés à la conception:

■ *Les données.* C'est un risque fréquemment rencontré et souvent le plus important. C'est, nous l'avons vu, la perte d'informations ou la dégradation des données. Mais la situation la plus grave est en fait l'oubli de données. On n'a pas perdu la donnée, on l'a ignorée. Elle n'est jamais entrée dans le système d'information. Si on ne s'organise pas pour détecter rapidement ce type de situation, on risque de perdre beaucoup de temps avant de s'en apercevoir. En effet, comment repérer ce qui n'a jamais été saisi. C'est la fameuse blague de l'adjudant: «Que les absents lèvent le doigt». Généralement, personne ne lève le doigt et l'adjudant est content de son effet.

■ *Les traitements.* Les risques peuvent aussi être liés aux opérations. Les causes possibles d'erreurs sont nombreuses. Il y a d'abord les erreurs de manipulations. Elles sont fréquentes. Mais les causes les plus graves de difficultés sont les nombreux «bugs» qui truffent les programmes. Ils sont généralement liés à des erreurs d'analyse ou de conception mais il y a aussi de nombreuses erreurs de programmation.

■ *Les résultats.* Il est aussi possible que des erreurs se glissent dans les affichages d'écrans, les transactions, les états,... Trop souvent, on fait confiance a priori aux informations produites par les ordinateurs. Or, l'expérience montre que les erreurs peuvent se glisser dans tous les résultats. Parfois, ce sont de simples détails mais très souvent ce sont de graves anomalies qui peuvent avoir des conséquences importantes.

Heureusement, on n'est pas complètement désarmé contre ce type de situation. Il est possible de se protéger contre ces nombreuses erreurs. Mais pour j on doit s'y prendre suffisamment à l'avance. Il est pour cela nécessaire de faire preuve de beaucoup de métier et d'expérience.

«Le diable est dans les détails»

Proverbe allemand.

Heureusement, il existe de très nombreuses parades. Mais elles sont très souvent assez techniques. Il est en effet nécessaire de plonger dans un niveau de détail assez poussé pour trouver des solutions adaptées. En effet, cela se fait en mettant en place des contrôles complémentaires effectués par des routines de contrôles. Ceci suppose une certaine capacité à imaginer les types d'erreurs possibles et d'en déduire les parades les plus efficaces. Celles-ci sont différentes selon le type d'anomalies possibles:

■ *Les données.* Il est d'abord nécessaire de s'assurer de la qualité des mouvements saisis. Ce n'est pas toujours simple. On va notamment vérifier que toutes les informations entrées servent bien à mettre à jour les bases de données. Il est en particulier sage de s'assurer qu'elles sont effectivement utilisées pour mettre à jour la bonne version de la base de données. On doit aussi vérifier la consistance des bases de données opérationnelles, c'est-à-dire de s'assurer que les informations stockées sont cohérentes et ne comprennent pas d'anomalies.

■ *Les traitements.* On doit de même s'assurer périodiquement que les opérations se passent conformément à ce qui était prévu. On va pour cela contrôler que toutes les opérations, qui ont été traitées au cours d'un laps de temps

donné, se sont effectivement déroulées sans incidents. On va pour cela garder la trace des opérations sous forme d'un journal, de façon à pouvoir ensuite contrôler certaines pièces.

■ *Les résultats.* On doit ensuite s'assurer que les résultats obtenus sont de bonne qualité. Il est pour cela nécessaire de s'assurer de manière simple qu'on consulte la bonne version de la base de données, et que les montants affichés ou imprimés sont les bons. Dans le cas d'une application comptable, on va, bien entendu vérifier automatiquement que les mouvements de la période, ajoutés aux cumuls antérieurs donnent bien les cumuls à ce jour. Ces contrôles sont très importants, car ils permettent de détecter rapidement des anomalies d'exploitation ou des erreurs de traitement.

Comme on le voit, il est indispensable de consacrer du temps à réfléchir à la manière d'améliorer la sécurité des applications opérationnelles et tout particulièrement à optimiser la qualité des bases de données qu'elles exploitent. C'est un enjeu important. Il l'est d'autant plus que cette approche est, en fait, une démarche assez proche de celle faite quand on cherche à améliorer le niveau de la qualité. Dans les deux cas, on cherche à repérer les défauts du système et à les réduire. Finalement, l'objectif est le même: protéger l'entreprise contre les maladresses des imbéciles et des maladroits.

*Claude Salzman, Consultant,
vice-president de l'AFAI*

Nachdruck mit freundlicher Genehmigung des französischen Chapters der ISACA (AFAI).