Sécuriser un ERP
les bonnes pratiques

par Hélène Courtecuisse
fondatrice du cabinet Lisis Conseil

Sécuriser un ERP : les bonnes pratiques

par Hélène Courtecuisse

Beaucoup de DSI le savent pour l'avoir expérimenté au moins une fois dans leur carrière, les projets ERP sont longs, complexes, consommateurs de temps, et surtout vastes : ils touchent à de nombreux services de l'entreprise, impliquent de très nombreux acteurs. Avec des enjeux cruciaux en matière de sécurité.

Les projets ERP ont pour objectif, souvent, de remplacer une multitude d'autres systèmes de tailles variées, plus ou moins anciens, plus ou moins bien maîtrisés ou documentés. Le planning du projet est généralement centré sur la mise en place de l'ERP lui-même, ses fonctionnalités, son paramétrage, son adéquation avec les besoins, ses interfaces avec les applications principales. Lorsque l'on arrive vers la fin du projet, la phase de recettage et de pilote par les utilisateurs de référence (*« key users »*) fait apparaître de nouvelles tâches non planifiées, entraînant souvent des retards de livraison dans les interfaces les moins critiques ou dans les rapports d'éditions.

Bref, l'ampleur de cette tâche, la lourdeur de la coordination des équipes et les ressources limitées peuvent parfois occulter totalement, ou repousser, un aspect vital du projet : la sécurité du nouveau système.

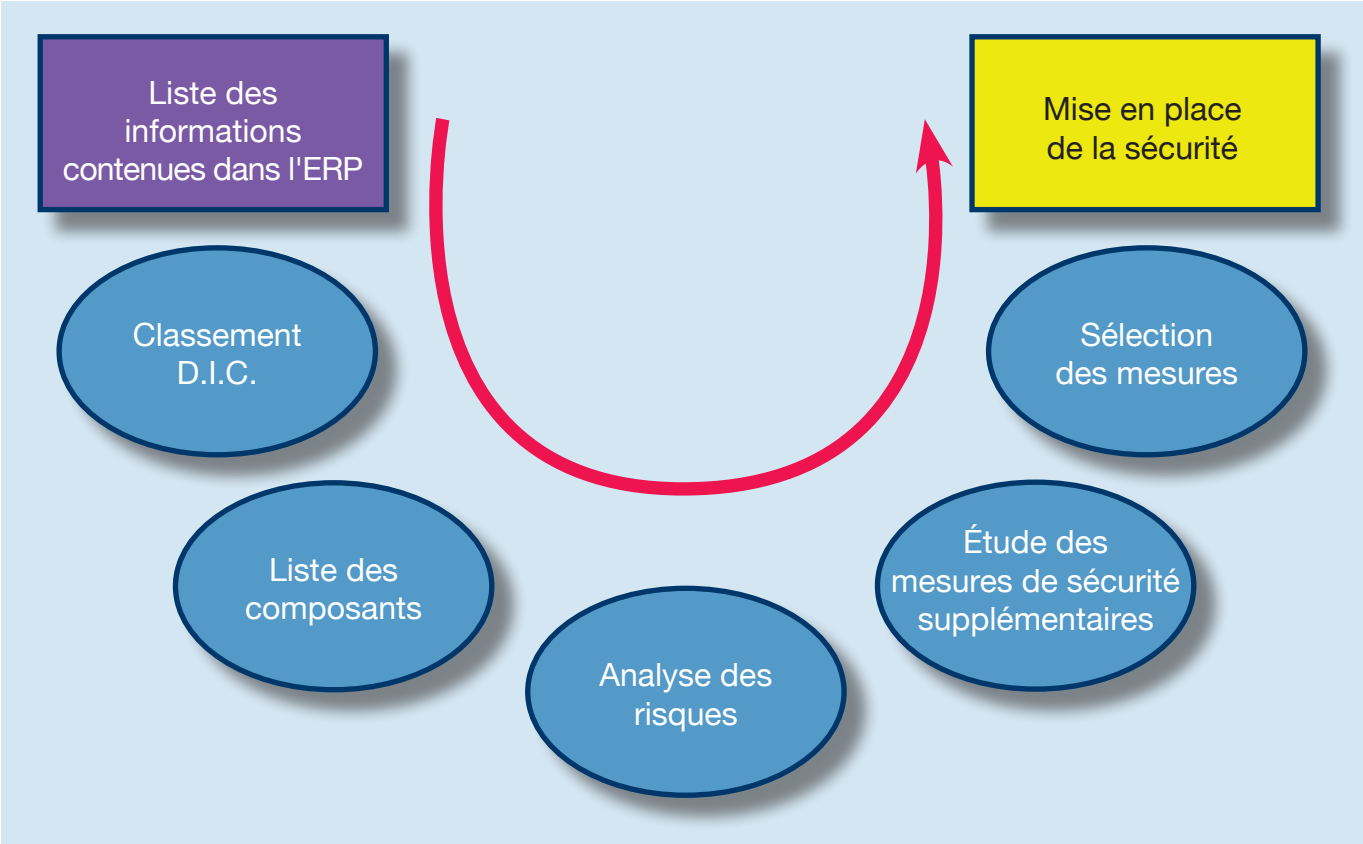
Or, cette sécurité doit pourtant être traitée dès le début du projet, dès que les premiers plannings sont établis, afin non seulement d'être en mesure de démarrer l'utilisation du nouvel ERP en conditions totalement sécurisées (échanges des données, accès, etc.), mais aussi afin de ne pas prendre en cours de projet des options techniques qui ne pourraient pas plus tard être sécurisées à la hauteur des besoins réels (choix du protocole d'échange de données avec des systèmes externes, par exemple).

Lorsque votre entreprise dispose d'un RSI (responsable de la sécurité des informations) ou d'un département sécurité, il est primordial, dès la confirmation du projet, d'aller le lui présenter et d'envisager avec lui les étapes d'analyse nécessaires. Si vous n'avez pas de RSI, il y a quelques étapes incontournables à suivre pour garantir la sécurité et assurer la pérennité de votre ERP.

- Le planning général : vous devez y inclure un sous-projet « sécurité », qui commence dès l'analyse (prototypage) de l'ERP.
- Quel niveau de sécurité devrez-vous implémenter dans et autour de votre ERP ? Commencez par établir un « classement

« Ne pas prendre en cours de projet des options techniques qui ne pourraient pas plus tard être sécurisées à la hauteur des besoins réels. »

Hélène Courtecuisse ex-directeur informatique et de la sécurité de l'information chez Novartis Santé Familiale, et fondatrice du cabinet Lisis Conseil



D.I.C » *(voir encadré)* du futur système, c'est-à-dire déterminez quel niveau de disponibilité, d'intégrité et de confidentialité il devra avoir. Pour cela, interrogez les responsables métiers : ils devront dresser la liste des informations qui seront gérées dans l'ERP (fichier des clients, produits, conditions commerciales, contrats, prix...) puis attribuer à chacune un niveau souhaité de protection selon les trois critères D.I.C. sur une échelle de 1 à 3. Vous aurez ainsi le point de départ de votre analyse de sécurité car vous aurez identifié précisément le niveau-cible à atteindre.

- Procédez ensuite à une analyse des risques détaillée du futur système. Pour cela, quatre actions doivent être engagées.
  - Établissez la liste la plus exhaustive possible des « composants » sur lesquels reposera cet ERP : le logiciel principal, les logiciels utilitaires sans lesquels il ne pourrait fonctionner (GUI, etc.), les types d'accès distants, la TMA (tierce maintenance applicative) éventuelle, les matériels, les postes utilisateurs, la (ou les) salle(s) machines impliquée(s), le LAN (réseau local), le WAN (réseau étendu)…
  - Pour chacun de ces composants, déterminez quels sont les risques, c'est-à-dire quels sont les sinistres possibles et plausibles (compte tenu de la sécurité déjà en place dans l'entreprise, de la probabilité que ce sinistre arrive réellement) qui pourraient impacter la disponibilité, l'intégrité ou la confidentialité de l'ERP.
  - Pour chaque risque identifié et retenu comme possible et plausible, analysez quelle protection supplémentaire vous pourriez mettre en place. Cette étape peut prendre du temps, vous devrez consulter de nombreux spécialistes internes et externes : services informatiques, services généraux, sociétés de maintenance de vos réseaux, etc.
  - Présentez à votre comité de pilotage les propositions, étudiez-les, puis faites un choix de solutions

- Enfin, en coordination avec tous ces intervenants, vous pourrez procéder à la planification et à la mise en place des mesures de protection identifiées.

À chaque étape, vos responsables utilisateurs doivent être sollicités. Leur implication est très importante, l'étude est basée sur leurs connaissances de leurs données et des enjeux métiers.De même, et ce n'est pas le point le plus facile à réaliser, ces mesures et étapes doivent aussi être appliquées

Le classement D.I.C.

Le classement D.I.C. consiste à prendre en compte les trois composantes de base de toute stratégie de sécurité : la disponibilité, l'intégrité et la confidentialité.

- ***La disponibilité***

La disponibilité se définit comme la capacité d'un système d'information à pouvoir être utilisé à tout moment, en fonction des performances prévues. A tort, la disponibilité est perçue comme allant de soi, mais de nombreux exemples de rupture de performances, voire de destruction plus sérieuse, existent. Or, la disponibilité est d'autant plus importante que le système d'information intègre des composantes telles que des systèmes d'information tiers (liens avec les sous-traitants, les partenaires...).

- ***L'intégrité***

« Intègre : qualité de ce qui est entier, intact, intégral, non diminué. » C'est le principe même d'un système d'information que de garantir que les données qu'il collecte, stocke, traite et restitue ne sont pas altérées. L'intégrité assure que des informations ne sont pas modifiées entre le moment où elles sont émises et celui où elles sont réceptionnées par leurs destinataires. Elle assure également que les informations ne sont modifiées que par les utilisateurs autorisés. Il faut donc qu'aucune modification volontaire ou accidentelle ne survienne.

- ***La confidentialité des données***

La confidentialité est un besoin fondamental de tout système d'information. Il s'agit de la propriété qui assure que seuls les utilisateurs habilités ont accès aux informations. La perte de confidentialité se traduit de multiples manières, la plus connue étant la pénétration de hackers dans le système d'information. Pour répondre aux besoins de confidentialité, des mécanismes de contrôle d'accès logiques et physiques, de chiffrement et d'authentification seront mis en place. Notamment pour protéger les informations stratégiques. Est stratégique toute entité (information, programme, document papier, images, e-mails...) qui, en cas de divulgation, peut entraîner des conséquences significatives pour l'entreprise, par exemple des pertes de chiffre d'affaires, d'exploitation, de clientèle, une dégradation de l'image de marque, voire des procès.

à vos sous-traitants : hébergeurs, mainteneurs… Il est donc important d'aborder ces points avec eux dès le début du projet. Si leurs mesures de sécurité actuelles ne correspondent pas à vos attentes, à vous de les aider à déterminer les mesures complémentaires qu'ils devront implémenter ainsi que le planning de mise en place. Enfin, il sera nécessaire d'aller les auditer afin de vérifier que vos niveaux de sécurité sont respectés.

Enfin, avant le démarrage de votre ERP, les plans de continuité et de reprise doivent avoir été établis : les plans métiers (PCA : plan de continuité d'activités, PRA : plan de reprise d'actvités) et les plans informatiques. Si ces plans existent déjà, il faudra les adapter à votre nouvelle architecture. Il faudra aussi vérifier que vos sous-traitants disposent de plans de continuité à jour. ◆

En savoir plus :

Hélène Courtecuisse est docteur en pharmacie, diplômée de l'IPI (Institut de pharmacie industrielle, option gestion de production). Après un début de carrière dans la gestion de l'information médicale chez Danone, puis dans l'informatique de gestion aux AGF, Hélène Courtecuisse a travaillé dix-huit ans dans les domaines de la sécurité de l'information et de l'informatique chez Novartis, un des leaders mondiaux de l'industrie pharmaceutique. Chez Novartis Pharma, elle a conduit la fusion des systèmes d'information de Ciba-Geigy et de Sandoz. Puis, elle a créé le service sécurité de l'information de Novartis France et a acquis une expérience des analyses de risques, des plans de réduction des risques et des plans de continuité des activités, à travers l'utilisation des méthodes internationales du groupe. Ensuite, directeur informatique et de la sécurité de l'information chez Novartis Santé familiale, elle a dirigé les projets informatiques (SAP, CRM…), la gouvernance des systèmes d'information sous-traités ou hébergés et la mise en œuvre des mesures de sécurité et de reprise d'activité. Elle a fondé le cabinet Lisis Conseil (www.lisis-conseil.com).

Sécuriser les composants de l'ERP : dix *best practices*

Des mesures « simples » de sécurisation peuvent être envisagées sur les composants de votre ERP :

- **Logiciel principal** : établissez la matrice des rôles utilisateurs (quelles transactions seront autorisées pour quels utilisateurs) en tenant compte, si besoin, de la loi Sarbanes-Oxley (ségrégation des tâches). Faites créer des *queries* pour contrôler régulièrement ces autorisations.

- **Réglementation** : en fonction du secteur métier de votre entreprise, certaines réglementations (par exemple : règles bancaires, agroalimentaires, pharmaceutiques) ou normes, peuvent être applicables (ISO, etc.). Si votre ERP est amené à gérer des données relatives à une distribution sur un marché étranger (Europe, États-Unis, etc.), les réglementations du pays s'appliquent aussi. Renseignez-vous sur ces réglementations et normes. Lorsque leurs exigences sont élevées, le choix de l'ERP peut en être affecté : c'est donc une étape à mener très en amont de votre projet.

- **Interfaces avec les autres systèmes internes (décisionnel, EDI, etc.) ou externes (prestataire de paie, de logistique et distribution…)** : leur niveau de sécurité doit être aussi haut que celui de l'ERP. N'oubliez pas que la sécurité résultant de votre ERP sera celle du « maillon le plus faible » du système complet. Pensez aux communications et transferts de données, ayez le « réflexe VPN », édictez des règles strictes de gestion des authentifications.

- **Systèmes décisionnel et *datawarehouse*** : protégez-les aussi strictement que votre ERP lui-même. Les données contenues doivent être disponibles (la direction générale préfère accéder aux tableaux de bord dans le système décisionnel plutôt que dans l'ERP), intègres (justesse des données et des agrégats, donc contrôle des interfaces et des règles d'alimentation), et leur confidentialité doit être maintenue (sécurisation des accès, y compris des exportations de données vers des tableurs sur les postes clients…).

- **Réseau local** : assurez un débit suffisant pour garantir les accès simultanés de tous vos utilisateurs ; mettez en place une redondance appropriée du réseau pour éviter les blocages en cas de panne.

- **Accès distants** : paramétrez les postes clients pour garantir l'accès distant (certains ERP nécessitent un paramétrage spécifique), et assurez-vous que les droits sont les mêmes et que l'impression fonctionnera….

- **Serveur** : vérifiez que les mots de passe des administrateurs sont de bonne qualité, et que leur changement régulier est organisé.

- **Sauvegarde** : vérifiez que les sauvegardes sont effectuées et stockées comme l'analyse des risques l'a déterminé (générations de sauvegarde, transfert dans un site distant, journalisation et processus de reprise…).

- **Sécurité physique** : vérifiez la sécurité physique de la salle machines.

- **Gestion des conflits** : attention aux conflits éventuels entre la sécurité de votre réseau (système de gestion de clé - PKI : *Public Key Infrastructure*-, système de gestion de mot de passe unique -SSO : *Single Sign On*-, règles de gestion des authentifications), règles de gestion des authentifications) et celles de l'ERP que vous avez retenu : certains ERP ne sont tout simplement pas compatibles ni paramétrables ! Dans ce cas, à moins de disposer d'un bon budget pour faire modifier l'ERP par son éditeur, il faudra accepter de fonctionner avec les règles de votre ERP.

LISIS CONSEIL
8 bis avenue Lily
78170 La Celle Saint CLoud
France