Chapitre 6
Les spécificités de projets sécurité

1. Introduction

À chaque domaine les projets qui lui sont spécifiques avec des caractéristiques qui lui sont propres. Ainsi, un chef ou un directeur de projet spécialisé dans le domaine public et de la paie, par exemple, saura éviter ou du moins anticiper les écueils les plus courants dans son domaine mais sera démuni lors du pilotage d'un projet de déploiement de cash management international. Il ne connaît pas le domaine bancaire ainsi que les métiers associés.

Dans les paragraphes suivants, c'est ce que nous allons présenter : quelques projets en sécurité typiques et classiques, les pièges à éviter ainsi que les bonnes pratiques à mettre en œuvre.

Nous irons du projet de déploiement d'un antivirus au pilotage d'un Plan de Reprise d'Activité (PRA) en passant par la mise en œuvre de ce plan.

Remarque

Le PRA est un projet complexe qui donne lieu à un ouvrage dédié aux éditions ENI : Plan de Continuité d'Activité - Concepts et démarche pour passer du besoin à la mise en œuvre du PCA.

Nous avons sélectionné des exemples de projets essentiellement techniques. Mais, comme nous l'avons vu, la protection de l'information est transverse à l'entreprise et ne représente qu'une partie des sujets à traiter.

Par exemple, à la période où j'écris ces lignes – fin 2016 –, je suis de plus en plus sollicité pour des projets de mise en conformité relatifs à de nouvelles obligations réglementaires ou légales. Ce type de projets sécurité est purement fonctionnel ; nous y analysons l'écart entre ce qui est en place, ce qui devrait l'être et ce qu'il va falloir mettre en œuvre. Ce qui doit être mis en œuvre du point de vue de la sécurité fait ensuite l'objet de plans d'action spécifiques qui concernent toute l'entreprise.

Il faut également garder à l'esprit que l'ensemble des projets SSI doit être conforme aux différentes politiques de l'entreprise (PSSI, PTH, PTR, etc.) ou alors que ces politiques doivent être rendues conformes aux obligations des différents projets de façon à ce que l'impératif de sécurité ne pèse pas sur l'activité de l'entreprise.

2. Les bons réflexes à appliquer

2.1 Les principes directeurs

La liste ci-dessous est une somme de bons réflexes qu'il convient, suivant les besoins et la taille du projet, d'appliquer en totalité ou de façon partielle. Cela dit, dans tous les cas, vous devez vous poser la question de l'applicabilité de chacun de ces principes.

– Un projet est placé sous la responsabilité d'un chef de projet ou, selon les cas, d'un responsable métier. Ce responsable est garant de l'intégration de la sécurité lors du projet et du respect de l'application de la présente instruction.
– Le responsable du projet doit associer les équipes sécurité dès le début et à chaque étape du projet.
– Tout projet ou application doit faire l'objet d'une démarche sécurité adaptée à son niveau de sensibilité, dont les risques résiduels et le plan d'action doivent être acceptés par le responsable métier avant mise en production.
– L'externalisation de tout ou partie du projet doit être spécifiquement prise en compte lors de l'analyse de risque.

– Les jalons sécurité, ainsi que les livrables correspondants (QES, soit Questionnaire d'Évaluation de la Sensibilité, dossier de sécurité, audit de sécurité, fiche d'objectifs de sécurité...), sont à intégrer dans la gestion de projet.

2.2 Durant la "préparation de projet"

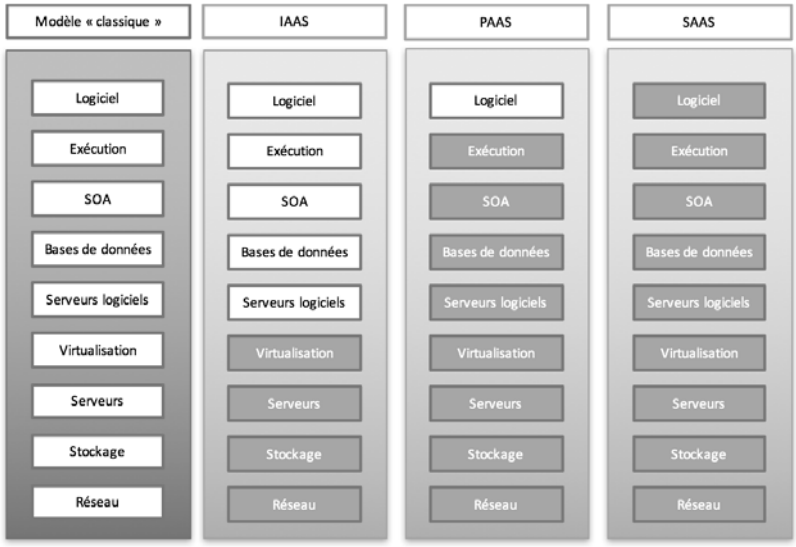
– La démarche sécurité doit être initiée dès le début du projet. Cela se concrétise par la rédaction d'un QES.
– Ce questionnaire doit être réalisé durant les phases d'étude d'opportunités et de cadrage à l'initiative du chef de projet, en collaboration avec la filière SSI concernée, validé par le responsable métier, et mis à disposition du RSSI. Un comité projet doit s'assurer du remplissage et de la validation du QES avant la fin du cadrage.
– Toute application sensible doit disposer d'un dossier de sécurité. Dans les autres cas de sensibilité remontés par le QES, le RSSI doit déterminer s'il est nécessaire de remplir un dossier de sécurité adapté pour l'application.
– En cas d'externalisation, une analyse de risque spécifique doit être conduite et les risques résiduels remontés au responsable métier pour acceptation.
– L'acceptation, par le responsable métier, des risques résiduels liés à l'externalisation doit être consignée en comité projet.

2.3 Quelques spécificités dans le cadre d'une prestation externalisée

Avec l'essor des solutions "Cloud", il me semble nécessaire de faire un point spécifique sur le sujet des prestations externalisées et les questions/obligations qu'il convient impérativement d'adresser dans le cahier des charges au fournisseur de la solution.

Une parenthèse cependant, je parle ici de solution "Cloud" – car c'est à la mode – ce qui correspond à du SaaS (*Software as a Service*). Mais avec un peu d'adaptation, ces recommandations peuvent être élargies à n'importe quel type de "...aaS".

Pour mémoire, voici les grands types de "...aaS".



Les cases en vert représentent les couches intégrées dans le " ...aaS", les cases blanches ne le sont pas. En d'autres termes, dans une architecture IaaS par exemple, les couches réseaux, stockage, serveurs virtualisation définissent un service IaaS, les couches blanches ne font pas partie de ce service.

Ainsi, il convient lors d'un projet "Cloud", du point de vue de la gestion de la sécurité, de vérifier que les points suivants sont pris en compte :

– Tout projet d'externalisation doit contenir les modèles de clauses contractuelles de protection des SI et de sécurité de l'information.
– Les mesures de sécurité et leur suivi doivent être spécifiés contractuellement avec le fournisseur de service. Les exigences formulées par le responsable métier en termes de sécurité doivent être traitées par des engagements contractuels.
– Le fournisseur de service doit s'engager sur les mesures de sécurité et sa capacité à protéger les informations qui lui sont confiées. Il doit apporter la preuve (politique, certification...) de son niveau de conformité par rapport aux normes et montrer qu'il est capable de protéger les informations qui lui sont confiées.

– Le cahier des charges de l'application doit prévoir une clause d'audit du code ou, à défaut, des certifications d'organismes indépendants reconnus.
– Le cahier des charges doit exiger une séparation (logique ou physique) entre les données spécifiques de l'entreprise et celles des autres clients.
– Le cahier des charges doit exiger la protection des accès aux données de l'entreprise pour tout accédant aux plateformes hébergeant l'application.
– Le cahier des charges doit exiger une administration des comptes et des habilitations par l'entreprise. Le fournisseur de service ne doit pas pouvoir créer des comptes et fournir des droits directement aux usagers de la solution.
– Le cahier des charges doit exiger une protection des traces réalisées par tout accédant aux plateformes hébergeant l'application. Le fournisseur de service, en particulier ne doit pas pouvoir modifier ces traces.
– Le cahier des charges doit exiger une protection des échanges d'informations entre le système d'information du fournisseur de service et le système d'information de l'entreprise. Ces échanges doivent respecter les règles émises par la société sur les flux réseau, les dispositifs de protection et de filtrage ainsi que les règles de protection de l'information (telles que définies dans les politiques thématiques).

2.4 Durant "l'élaboration de la solution"

– Si le niveau de sensibilité défini par le QES pour le projet ou l'application l'exige, une analyse de risque doit être réalisée durant la phase de conception. Des mesures de sécurité doivent être proposées pour pallier les risques. Ces éléments doivent être consignés dans le dossier de sécurité. Les mesures de sécurité doivent être adaptées aux impacts métiers et respecter les besoins de sécurité établis par le responsable métier.
– Les mesures de sécurité à mettre en place doivent être décrites dans les spécifications générales et/ou techniques.
– Les mesures de sécurité doivent en priorité être recherchées dans les solutions existantes au sein de l'entreprise. Dès qu'une solution de sécurité est disponible au sein de l'entreprise et utilisable dans le contexte du projet, elle doit être privilégiée. Le choix d'une solution alternative doit être validé par le RSSI.

- Les mesures de sécurité doivent être construites conformément aux éléments validés au sein du dossier de sécurité et aux spécifications du cahier des charges.
- Les équipes de développement ne doivent pas avoir accès à l'environnement de production. Les équipes en charge du développement et des tests ne doivent pas avoir de comptes actifs dans l'environnement de production.
- Les cahiers de tests techniques et fonctionnels doivent intégrer les mesures de sécurité. Les mesures de sécurité doivent être testées au même titre que les fonctionnalités classiques de l'application. Tout dysfonctionnement doit donner lieu à une fiche d'anomalie.
- L'application doit être testée dans un environnement conforme à l'environnement de production mais disjoint de ce dernier.
- Les fichiers de test ne doivent pas contenir d'informations sensibles. Les tests doivent être réalisés sur des données non sensibles. En particulier, les données personnelles devront être anonymisées.
- Dans l'environnement d'homologation technique, l'accès au code source doit être restreint aux seules personnes habilitées afin de réduire les risques de compromission. Les platesformes de test et de recette comportent souvent tout ou partie du code associé à l'application. Elles doivent être protégées pour éviter une modification indue de ces éléments (bombe logique...) ou la récupération d'informations.
- Dans le cas des applications sensibles, tout retrait de mesures de sécurité doit être identifié, et ses risques résiduels validés par le RSSI, acceptés par le responsable métier et périodiquement réévalués. Dans le cas d'un retrait temporaire, un planning de remise en place doit y être associé. Si les mesures de sécurité envisagées ne peuvent pas être déployées pour des raisons de planning, de complexité, de budget, etc., elles doivent être identifiées comme telles. Le retrait de fonctionnalités doit être analysé. Cette analyse doit être fournie au RSSI qui la valide.

2.5 Durant "le déploiement de la solution"

Les processus de mise en production de l'entreprise doivent être respectés.