La sécurité des données dans les plateaux virtuels collaboratifs

Article de Guy Forax, créateur du FPDMUG et Associé de PLM Décision

1. Préambule

Aujourd'hui, concevoir, analyser et mettre sur le marché de nouveaux produits toujours plus sophistiqués, nécessite la collaboration de multiples acteurs, qu'ils soient dans l'entreprise ou chez ses partenaires. Nous avons vu dans le précédent numéro de Cad-magazine, que les plateaux virtuels collaboratifs se multipliaient pour répondre à ces nouvelles exigences de collaboration en entreprise étendue. Mais utiliser ces nouveaux environnements oblige à repenser complètement les modes de travail et particulièrement les règles de sécurité, de confidentialité, de sureté et d'accès aux informations. En effet, il faut arriver à trouver un compromis entre deux exigences contradictoires :
– partager les informations entre partenaires et les rendre accessibles le plus simplement possible,
– protéger ces informations qui constituent le Capital Intellectuel (les IPs) de chacun des partenaires.

2. Les règles d'or de la sécurité dans les environnements collaboratifs

Les retours d'expérience sur les plateaux projets mis en place par de grands donneurs d'ordre de l'automobile et de l'aéronautique et sur les premiers plateaux virtuels multi-projets mutualisés permettent de tirer quelques précieux enseignements que l'on peut considérer comme les règles d'or de la sécurité dans les environnements collaboratifs mutualisés :
– Centraliser la définition des identités.
– Contrôler les droits par une gestion rigoureuse des rôles.
– Gérer les droits sur les données en fonction des attributs, de la maturité, du projet et du découpage produit.
– Ranger l'information dans un coffre-fort à accès sélectif suivant les droits et non dans des répertoires et sous-répertoires.
– Publier les informations une seule fois pour tous les utilisateurs.
– Synchroniser les données partagées avec les données privées.
– Se méfier des accès par moteur de recherche et par navigation.
– Privilégier l'accès aux données par l'intermédiaire de Workflows.

2.1. Centraliser la définition des identités

La première chose à faire lorsqu'on autorise un utilisateur à accéder à des informations partagées est de s'assurer de son identité. Cette identité ne doit pas être générique du genre « concepteur » ou « relecteur », mais elle doit être nominative. Par ailleurs, pour éviter les usurpations ou les prêts d'identité, il est bon de compléter les mécanismes traditionnels de login/password par un contrôle plus précis, adresse IP, mais attention aux adresses dynamiques ou mieux les adresses MAC. L'inconvénient est que dans ce cas la personne désignée ne peut accéder que depuis sont poste de travail déclaré et non depuis un autre poste ou un poste mobile. On pourra essayer de concilier les deux impératifs en limitant les actions que l'utilisateur pourra effectuer depuis un poste qui n'est pas son poste nominal.

Une autre difficulté est d'éviter la prolifération de login et de password qui peut provoquer des pertes de temps importantes lorsqu'on les oublie. Une attitude qu'on rencontre souvent, pour éviter ce problème est d'utiliser partout le même identifiant ou de le coller sur son écran, ce qui va à l'encontre du niveau de sécurité qu'on cherche à obtenir !

De façon plus technique, on peut simplifier l'identification par un mécanisme de Single Sign On (SSO) ou plus compliqué en utili-

sant la fédération d'identités. Le plus simple est que les identités soient gérées de façon centralisée sur la plate-forme collaborative mutualisée elle-même, avec délivrance de certificats suivant une procédure plus ou moins complexe suivant les besoins. Pour des systèmes très sensibles, cette sécurité logique peut se compléter d'une sécurité physique de reconnaissance de clé USB, carte à puce, ou d'une caractéristique biométrique.

Une difficulté de la gestion centralisée est la charge de travail qu'elle peut induire pour les gestionnaires de l'environnement collaboratif. Il est nécessaire alors de déléguer la responsabilité de déclarer les utilisateurs à des personnes de leur entreprise par exemple, dûment habilitées pour cela.

2.2. Contrôler les droits par une gestion rigoureuse des rôles

Lorsqu'une personne se connecte à la plate-forme, après vérification de son identité, il faut alors définir ses droits à exécuter telle ou telle action sur l'information. Comme ses actions peuvent être très nombreuses, leur définition élémentaire peut là aussi être très pénalisante en termes d'administration. La méthode classique consiste à définir non pas des droits élémentaires, mais des profils de droits qu'on appelle des rôles. Les rôles sont très génériques : « administrateur », « concepteur », « valideur », « lecteur »…

Une bonne méthode consiste à définir les 10 ou 15 rôles différents que les personnes peuvent jouer et de définir ensuite pour un projet donné, quels sont les rôles retenus pour ce projet. Ces rôles auront tout intérêt à être organisés par entreprise participant au projet et en fonction des clauses contractuelles qui définissent les responsabilités des différents partenaires. Bien sur, un sous-traitant technique n'aura pas le même ensemble de rôles, qu'un partenaire qui partage les risques du projet. Une même personne pourra bien sûr jouer des rôles très différents suivant les projets dans lesquels elle sera impliquée, et pour un même projet, elle jouer aussi des rôles différents suivant les données concernées. Par exemple, elle pourra être « concepteur » d'un sous-ensemble du produit, « valideur » pour un autre sous-ensemble et encore « lecteur », pour les résultats de calcul.

2.3. Gérer les droits sur les données en fonction des attributs, de la maturité, du projet et du découpage produit

Cette question de la gestion des droits en fonction de la partie du produit qui est concernée est tout à fait spécifique du PLM. Si on ajoute à cela que les droits peuvent être différents suivant l'état de maturité de l'information (en cours ou validé), suivant la nature de l'information (assemblage ou document, modèle 3D ou spécification, modèle natif ou représentation simplifiée…) et même suivant l'attribut (on a le droit de voir le poids mais pas le nom du fournisseur…), on arrive à un besoin de gestion très fine des droits sur l'information. Ce besoin reste encore mal adressé dans la plupart des outils de PLM sur le marché aujourd'hui.

2.4. Ranger l'information dans un coffre-fort à accès sélectif suivant les droits et non dans des répertoires et sous-répertoires

Alors qu'on aurait besoin d'une gestion très fine, des accès à l'information, ce qui est proposé le plus souvent, est un mécanisme d'espaces de travail partagés, gérés comme des répertoires et des sous-répertoires, sur lesquels tel ou tel utilisateur possède des droits de type « système de fichier ». Au mieux, les droits qui s'appliquent au répertoire, peuvent être affinés par des droits individuels sur les fichiers (documents).

L'utilisation des espaces partagés est une bonne solution lorsque deux organisations ont besoin d'échanger des informations, sans chercher à savoir qui y accède réellement, et dans une logique où l'espace partagé ne sert que de boîte aux lettres pour transmettre le fichier, qui est ensuite traité par le partenaire, avant de rendre le résultat par le même mécanisme. On est alors dans une logique d'échange et pas vraiment dans une logique de mise en commun et de partage de l'information.

Pour les structures produit, le problème se complique encore, puisqu'une structure produit se prête mal à la mise en fichier, ce fichier pouvant lui-même être échangé dans un espace de travail partagé. Pour interpréter une structure produit, on doit enfin pouvoir reconstituer les nombreux liens entre cette structure et le produit complet, les liens vers les composants catalogues, vers les fichiers de définition (spécifications, modèles 3D…), sans compter les liens qui portent des options ou des variantes et les liens de configuration. On voit là que partager uns structure produit est beaucoup plus complexe qu'échanger un fichier CAO par exemple.

Echanger des structures produit et toutes les informations qui s'y rattachent ne peut se faire qu'avec des échanges de PDM à PDM. Malheureusement, il n'existe pas encore vraiment de standard d'échange de PDM à PDM qui couvre tous les besoins. A défaut, on peut s'appuyer sur ce qui s'en rapproche le plus : les protocoles d'application AP 203 et AP 214 de STEP ou l'AP 239 de PLCS par exemple.

Mais après tout, si nous venons de voir que le mécanisme d'échange de fichiers dans un espace de travail partagé permettait à deux partenaires de travailler alternativement sur un

même jeu de données, existe-t-il d'autres situations de collaboration que celle-ci.

Sans parler de réel co-design qui à ce jour nécessite impérativement de disposer du même outil « auteur » (CAO) des deux côtés, il existe des situations réelles où le partage d'information est nécessaire : par exemple lorsqu'on veut mener une co-revue à distance ou lorsqu'on veut travailler en contexte.

2.5. Publier les informations une seule fois pour tous les utilisateurs

Aujourd'hui dans ces cas de réelles collaborations, trois solutions existent :
– Travailler sur le système du donneur d'ordres,
– Collaborer sur un plateau virtuel mis à disposition par le donneur d'ordres,
– Collaborer sur un plateau virtuel neutre.

Pour le donneur d'ordres, la première solution est la plus simple. Malheureusement elle possède un inconvénient majeur : comme le partenaire travaille sur le système du donneur d'ordres, s'il y a une faille de sécurité, le partenaire peut potentiellement accéder à l'ensemble de l'information du donneur d'ordres.

Moins grave, le donneur d'ordres doit sur dimensionner son système, prévoir des locaux, des accès… En revanche, le résultat du travail réalisé par le partenaire s'intègre naturellement dans le produit du donneur d'ordres.

Pour résoudre le problème majeur de sécurité que nous venons de mettre en lumière, le donneur d'ordres peut définir, une zone de travail. Celle-ci est sous sa responsabilité, il l'alimente depuis son propre système et elle est accessible par le partenaire, sans que ce dernier ne puisse accéder au système interne du donneur d'ordres, c'est le concept de DMZ.

Il y a cette fois-ci un autre inconvénient majeur pour le donneur d'ordres : la duplication de l'information entre le système interne et la DMZ. Et qui dit duplication, dit risque d'incohérence. Il faut donc trouver un moyen d'assurer une synchronisation entre les deux systèmes.

Il existe aussi un autre inconvénient pour le donneur d'ordres, lié à la confidentialité. En effet, si ses partenaires n'ont pas le droit d'accéder aux mêmes informations, le donneur d'ordres doit mettre en forme l'information de manière spécifique à chaque partenaire, ce qui devient très lourd lorsqu'on a de nombreux partenaires. Le donneur d'ordres peut donner aussi à tous ses partenaires le même contexte de travail, qui dans ce cas-là doit être l'union (au sens ensembliste) de tous les contextes nécessaires, union qui tend vers le produit tout entier. On se retrouve rapidement dans la même situation que le cas n° 1.

Pour le partenaire, la difficulté est le besoin de maîtriser deux environnements de travail, le sien et celui du donneur d'ordres. Bien sur, le donneur d'ordres incite ses partenaires à utiliser les mêmes progiciels que lui, mais lorsque le partenaire est partenaire de plusieurs donneurs d'ordres et que ces derniers n'ont pas les mêmes progiciels, la situation devient vite ingérable pour lui.

Pour essayer de concilier tous ces points de vue et de faciliter la vie du donneur d'ordres et des partenaires, on voit apparaitre une nouvelle génération d'environnements collaboratifs : les plate-formes mutualisées neutres. Dans ce dernier cas, le donneur d'ordre délivre sur la plate-forme le sur-ensemble de l'information produit nécessaire à un groupe de partenaires et chaque partenaire du Groupe n'accède qu'à l'information qui le concerne suivant ses droits d'accès. Cet accès fin à l'information sur la plate-forme n'est possible que si cette dernière est dotée d'un PDM.

2.6. Synchroniser les données partagées avec les données privées

L'OEM peut disposer d'un moyen automatique de synchronisation du contexte avec son propre PDM, mais comme il ne délivre qu'un contexte unique au lieu d'un contexte par partenaire, il peut recalculer ce contexte lorsqu'un de ses éléments change. Le partenaire de son côté est notifié lorsque le contexte change et il va rechercher l'information. Là aussi, le nouveau contexte peut enrichir automatiquement son propre PDM, ou être traité manuellement.

2.7. Se méfier des accès par moteur de recherche et par navigation

Nous avons vu que la clé de la sécurité des données lorsqu'on utilise des environnements collaboratifs mutualisés est de pouvoir appliquer une ségrégation très fine de ces données, bien plus fine que le niveau du répertoire ou même du document.

Lorsque ces mécanismes fins s'appuient sur la structure de décomposition du produit, on peut alors empêcher des accès à des informations qui ne font pas partie de la zone de travail de l'utilisateur. Il faut alors être particulièrement attentif à ce que l'information ne puisse pas être atteinte par un chemin détourné : requête multicritère, requête plein texte, requête géométrique, requête sur des composants analogues ou d'autres cas d'emploi, etc.

2.8. Privilégier l'accès aux données par l'intermédiaire de Workflows

Pour renforcer encore la sécurité, on peut ajouter une obligation de n'accéder aux données (ou à certaines données particulièrement sensibles) qu'au travers de Workflows. La mise en œuvre de processus bien encadrés ne permettront par exemple que les requêtes qui passent par des chemins où la conformité des accès sera dûment contrôlée.

3. Conclusion

La sécurité des accès à l'information revêt une dimension particulièrement critique lorsqu'on met en œuvre des moyens collaboratifs mutualisés. En effet, les acteurs d'un même projet multipartenaires n'ont pas tous les mêmes droits et on ne peut pas se contenter de donner tous les droits à tous le monde comme on le fait parfois dans une entreprise. Mais le problème se complique encore quand on n'est pas seulement dans un plateau virtuel lié à un projet, mais lorsqu'on travaille dans un environnement collaboratif mutualisé multi-projets. Dans ce cas, les partenaires dans un projet sont parfois concurrents dans un autre.

Il faut arriver alors à trouver un compromis entre deux exigences contradictoires : partager l'information le plus simplement possible avec ses partenaires, et protéger son capital intellectuel. Pour atteindre ce compromis, une batterie de mesures doit être prise :

– Pour identifier sans ambigüité les personnes qui accèdent au système.
– Pour calculer les rôles qu'ils jouent dans tel ou tel projet, conformément aux dispositions contractuelles.
– Pour en déduire les droits dont ils disposent sur telle ou telle information, avec une granularité suffisamment fine pour que le donneurs d'ordres mettent à disposition l'information de contexte le plus simplement possible et pour que chaque partenaire n'accède qu'au sous-ensemble d'information auquel il a droit.

Les environnements collaboratifs dont la sécurité repose sur un mécanisme de répertoires ne permettent pas d'atteindre la finesse nécessaire. Seule l'utilisation d'un PDM dans l'environnement collaboratif permet de lever cet obstacle. Mais l'organisation des droits dans un PDM n'a pas été pensée initialement pour les environnements collaboratifs multi-projets, et elle peut s'avérer conceptuellement insuffisante sans une personnalisation importante…