DOSSIER

Sécuriser ses données : Pourquoi ? Comment ?

En 2005, les entreprises françaises ont dépensé 1,11 milliards d'euros pour renforcer la sécurité de leurs réseaux informatiques ! Si les grandes entreprises industrielles et, bien entendu, les secteurs marchands ou financiers sont aux avant-postes de la lutte, les PME se préoccupent désormais du problème. Cette prise de conscience semble cependant tarder à se traduire par des plans d'action. Pourtant les risques sont majeurs, et les solutions relativement simples comme nous le verrons dans les pages qui suivent.

A l'échelle de l'entreprise

Dans le contexte actuel, peu d'entreprises peuvent se permettre de subir un arrêt de fonctionnement de leur système d'information ou une perte de leurs données critiques, sans risquer de mettre en péril leurs activités. Face à ce constat, il est indispensable aujourd'hui pour les industriels de mettre en place une politique de sauvegarde globale pour assurer la disponibilité de leur outil de travail. Ils doivent donc non seulement sécuriser leurs données critiques pour que l'information soit disponible en toutes circonstances, mais également préparer leurs systèmes d'information en mettant en place une infrastructure sécurisée et adaptée à leurs besoins.

Nous n'aurons pas la prétention ici de faire un état des lieux exhaustif des techniques de sécurisation informatique, le sujet est trop vaste et intéresse surtout les services informatiques des entreprises. En revanche, nous essaierons d'une part de présenter les bases de la sécurisation de données, et d'autre part de signaler les méthodes les plus en phase avec les besoins des bureaux d'études.

Le piratage, mais également l'inattention ou le contournement de certaines règles de prudence peuvent être la cause de la perte de données stratégiques pour l'entreprise.

Sécuriser ses données, c'est se protéger de trois risques : les pertes d'informations, les virus, les accès non autorisés à ses données. Ces risques peuvent survenir à la fois en interne à travers le réseau propre de l'entreprise, et en externe à travers les échanges de données et les accès Internet par exemple. Autant de cas de figure à considérer pour éviter de désagréables surprises.

Vos données à l'abri des trous de mémoire

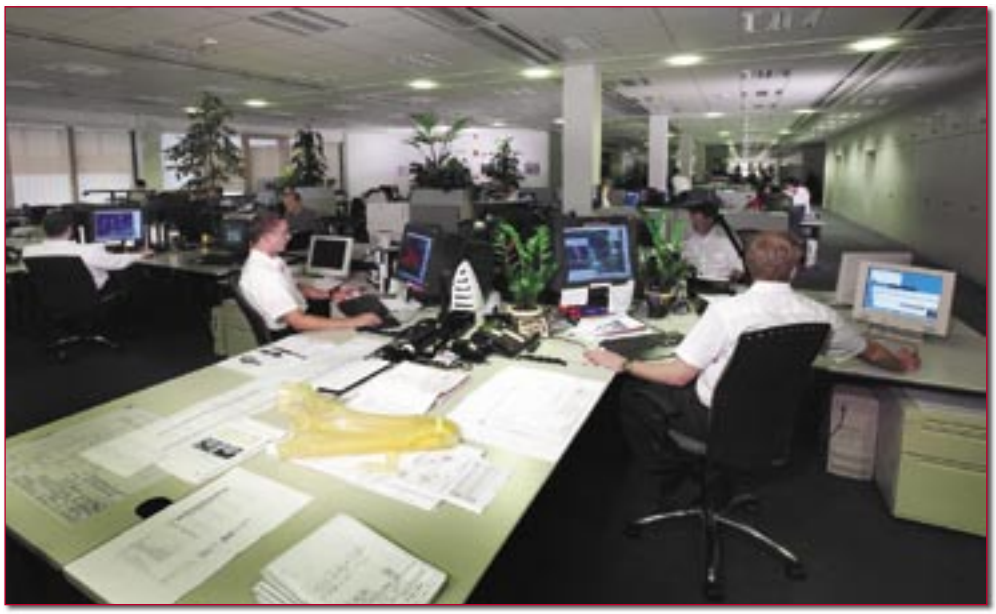
Vos précieuses données sont à la merci d'une panne de votre ordinateur, aussi dramatique qu'impromptue ou d'un virus fatal. Pour que ce scénario ne devienne pas réalité, commencez dès aujourd'hui à sauvegarder. Une opération menée en un rien de temps, une précaution qui deviendra vite un réflexe et qui, un jour, vous sauvera la mise.

Dans un environnement professionnel, deux systèmes de sauvegarde cohabitent et se complètent : la sauvegarde individuelle sur un poste de travail et la sauvegarde collective, celle

des données partagées en réseau de l'ensemble de l'entreprise.

Bien évidemment la sauvegarde personnelle n'est possible que si l'administration informatique de votre entreprise vous l'autorise.

Mais attention aux formats multiples, CD+/-R/RW, DVD+/-R/RW et à l'aspect définitif de la gravure, sauf pour les formats réinscriptibles (RW), qui n'est pas adapté à la sauvegarde incrémentielle.



Les entreprises industrielles et les PME prennent conscience depuis peu de la nécessité de protéger leur savoir-faire contenu dans leurs plans.

Dans ce cas, il n'y a pas (ou plus) 36 solutions techniques. Oubliez les systèmes à bande type Jazz ou Zip, devenus obsolètes, optez plutôt pour les disques durs externes qui constituent aujourd'hui les solutions les plus avantageuses sur tous les plans ou presque : prix, rapidité, capacité, simplicité de mise en œuvre. Sachez par exemple qu'un petit disque dur amovible en USB 2.0 de 250 Go coûte 150 € HT... Et qu'il existe des modèles de capacité légèrement inférieure que vous pouvez mettre dans votre poche le soir après avoir sauvegardé votre activité quotidienne. Les graveurs de cédéroms ou de DVD peuvent être employés eux comme dispositifs d'archivage.

La sauvegarde collective, celle des ressources partagées, intervient lorsque plusieurs salariés partagent la même banque de données. Choix stratégique de la direction informatique de l'entreprise, la mise en place de tels systèmes reste une affaire de spécialistes que nous n'aborderons pas dans ce dossier. On peut simplement dire que les très grosses entreprises comme les constructeurs automobiles misent aujourd'hui sur le SAN (Storage Area Network), un réseau de stockage indépendant du réseau principal du groupe. Tandis que les PME/TPE se dirigent, elles, vers le NAS (Network Area System), des unités de stockage en réseau, soit un serveur dédié uniquement à cette tâche.

Un pare-feu pour quoi faire ?

Avec l'intensification des échanges électroniques, il devient vital de bien protéger le système informatique de l'entreprise et de dissuader toute attaque interne ou externe. Comme l'explique Xavier Daspre, ingénieur sécurité chez Afina – Idepro, un distributeur à valeur ajoutée spécialisé dans le domaine de la sécurité, *« les dangers prennent deux formes : les virus et l'intrusion dans les systèmes. Cependant, il est inutile de céder à la panique, des solutions simples de protection existent. Elles permettent d'agir principalement à deux niveaux : l'authentification et le contrôle d'accès. L'authentification est assurée par les mots de passe, alors que le contrôle d'accès s'appuie sur deux technologies : les antivirus et les firewalls ou pare-feu. Investissement minimal, l'antivirus est un programme informatique qui réside en règle générale dans la mémoire de l'ordinateur. Les plus fréquents se réfèrent à une table de définitions virales pour identifier les virus. Leurs missions ? Analyser en permanence le contenu du disque dur, les clés USB, CD-Rom, documents ouverts ainsi que les fichiers téléchargés à partir d'Internet. Restent les tentatives d'intrusion et de prise de contrôle d'un ordinateur depuis l'extérieur du réseau pour en pirater le contenu.*

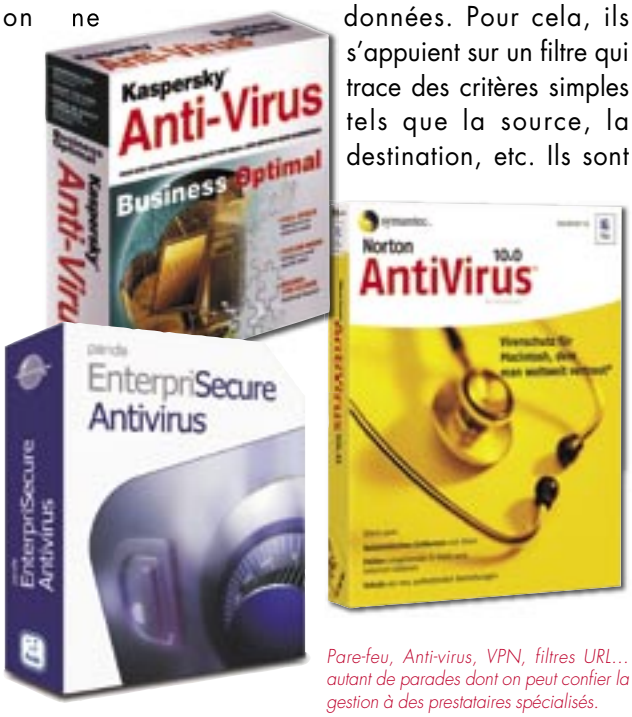
Les pare-feu, tel celui intégré à Windows XP, constituent une première mesure de protection simple et relativement efficace.

C'est là qu'entrent en jeu les « firewalls ». Éléments actifs du réseau, ils s'appuient sur des technologies logicielles pour analyser le

trafic réseau afin d'autoriser ou d'interdire les accès. » Voici une rapide explication de leur fonctionnement pour que vous puissiez briller quelques minutes (pas beaucoup plus) dans un dîner d'informaticiens…

Souvent déployés à l'occasion d'une connexion à Internet, les « firewalls » sont installés, puis configurés en fonction des services fournis à l'entreprise par son fournisseur d'accès. Le plus souvent, la PME n'en entendra pas parler, le pare-feu étant installé chez son fournisseur. Mais lorsque les connexions se multiplient, l'entreprise a tout intérêt à mettre en place un accès permanent à Internet. Il faut alors envisager de protéger son réseau. L'installation d'un pare-feu sur un serveur dédié s'impose. Simple à mettre en œuvre en théorie, sa configuration peut être réalisée en interne grâce aux assistants de paramétrage. Reste que l'on ne peut s'improviser du jour au lendemain responsable sécurité de son accès Internet. Mieux vaut s'en remettre à un professionnel. À ce niveau, deux approches possibles : soit faire appel à son revendeur, soit utiliser les services de son fournisseur d'accès qui peut fournir, sur demande, un routeur sécurisé en location et définir avec vous une politique de sécurité personnalisée (nombre d'utilisateurs, droits d'accès, type d'activité de la société…). Du plus simple au plus sophistiqué, il existe trois grandes catégories de *firewalls* : les filtres de paquets, les passerelles applicatives, baptisées aussi « *proxies* » et les outils intervenant à différents niveaux de la communication. En dehors des termes techniques un peu barbares, il faut savoir que la première catégorie constitue la première génération de pare-feu. Leur mission : interdire ou autoriser les échanges de données. Pour cela, ils s'appuient sur un filtre qui trace des critères simples tels que la source, la destination, etc. Ils sont rapides et peu coûteux et sont en général livrés avec un routeur. Malheureusement, ils présentent un défaut majeur : ils sont faciles à berner et compliquent les tâches de maintenance pour assurer une protection efficace. Plusieurs éditeurs ont donc développé des passerelles dites applicatives. Clairement, le *firewall* est le passage obligé entre l'utilisateur et le réseau Internet. Chaque fois que l'utilisateur désire se connecter au réseau, il passe par le pare-feu qui lui accorde ou pas l'accès et contrôle les échanges de données. La troisième catégorie, ou *firewalls* multicouches, est quasi similaire aux passerelles applicatives. Alors que le « *proxy* » se substitue à l'application, les *firewalls* multicouches comparent chaque paquet de données pour vérifier sa conformité par rapport à une structure de paquet connue. Un tel fonctionnement nécessite des paramétrages complexes et peut ralentir les réponses. Le choix consiste donc à trouver le bon équilibre entre une sécurité optimisée et des temps de réponse rapides.

Les entreprises soucieuses de leur sécurité n'ont pas toujours les ressources internes pour soutenir leurs ambitions sur ce sujet. Mais la parade existe : la sécurité managée. Afina, distributeur de solutions de sécurité, d'infrastructures et de services informatiques associés propose une solu-



Pare-feu, Anti-virus, VPN, filtres URL… autant de parades dont on peut confier la gestion à des prestataires spécialisés.

À faire

- Mettez en place des outils de premier niveau de sécurité avec des antivirus, complétez-les avec un ou plusieurs firewalls.
- Faites appel à des outils qui ont été certifiés et validés par le marché.
- Utilisez des technologies suffisamment évolutives et souples, car cela revient très cher de développer des outils de sécurité.
- Préférez des outils standard à des outils propriétaires.

À éviter

- Ne pensez pas que la sécurité est absolue avec la mise en place d'un firewall. Le processus de sécurité ne doit jamais s'arrêter, car il faut sans cesse continuer à faire les mises à jour des pare-feu, des antivirus, etc.
- N'installez pas des technologies complexes pour vous retrouver avec une véritable usine à gaz en matière de sécurité. Une approche qui s'avère rapidement difficile à contrôler.

tion de ce type adaptée aux PME. Il s'agit pour l'entreprise de sous-traiter totalement cet aspect informatique à un spécialiste, qui installe, administre et gère les technologies susceptibles de garantir la sécurité de vos données. Firewall, VPN, antivirus, anti-hacking, filtres URL, suivi du trafic, sauvegarde des données... tout peut être géré à distance de manière transparente.

Faire face aux menaces internes

Marc Agullo, responsable technique de la société Query Informatique, un spécialiste de la sécurité et de l'intégration des systèmes informatiques : *« la sécurité informatique dans le monde industriel et notamment vis-à-vis des problèmes internes est naissante mais prend de l'ampleur. A l'heure où les enjeux de la compétition se situent dorénavant dans l'innovation et le time to market, les risques de perte ou de vol de données stratégiques doivent être étudiés de prêt. L'intrusion sur le réseau de l'entreprise depuis l'extérieur est une menace connue et traitée depuis longtemps par les directions informatiques à l'aide de solutions classiques de type firewall, filtrage de contenu, anti-virus, DMZ (zone démilitarisée d'échange de données), etc. Mais depuis peu, la menace principale est interne à l'entreprise. »* En effet, quoi de plus facile que de brancher sur le port USB de sa

Clés USB, PDA, lecteur MP3, APN... autant de portes d'entrée pour les virus et de portes de sortie pour vos données critiques.

machine l'un des supports amovibles très répandus aujourd'hui comme les clés USB, lecteurs MP3, appareils photos numériques, PDA, disques durs... sans compter la généralisation sur les postes de travail des graveurs de cédérom. *« Les frontières entre les données personnelles et les données de l'entreprise sont de plus en plus floues. Et la malveillance n'est pas le risque principal ! Il y a aussi la négligence et le manque d'application de règles efficaces d'utilisation des outils informatiques de l'entreprise »*. Qui n'a pas un jour montré à ses collègues ses photos de vacance réalisées avec son dernier APN ? Branché une clé USB pour transférer un fichier récupéré chez un client ? Gravé la compile idéale des Stones qu'écoute le stagiaire à longueur de journée ? *« Et les directions informatiques qui se sont risquées à une analyse hasardeuse de quelques PC de l'entreprise ont eu des surprises en découvrant les Go de données musicales et photographiques stockées ! En France, il est difficile de trouver des informations chiffrées sur le piratage de données ou les infections des réseaux d'entreprises. Du côté anglo-saxon, le problème est moins occulté et des études montrent que plus de 70 % des incidents de sécurité sont d'origine interne. Deux autres chiffres font réfléchir : 94 % des entreprises anglaises ont subi des incidents de sécurité en 2004 et 72 % des employés n'ont aucun problème d'éthique pour emporter des données dans un nouvel emploi ! »* observe Marc Agullo.

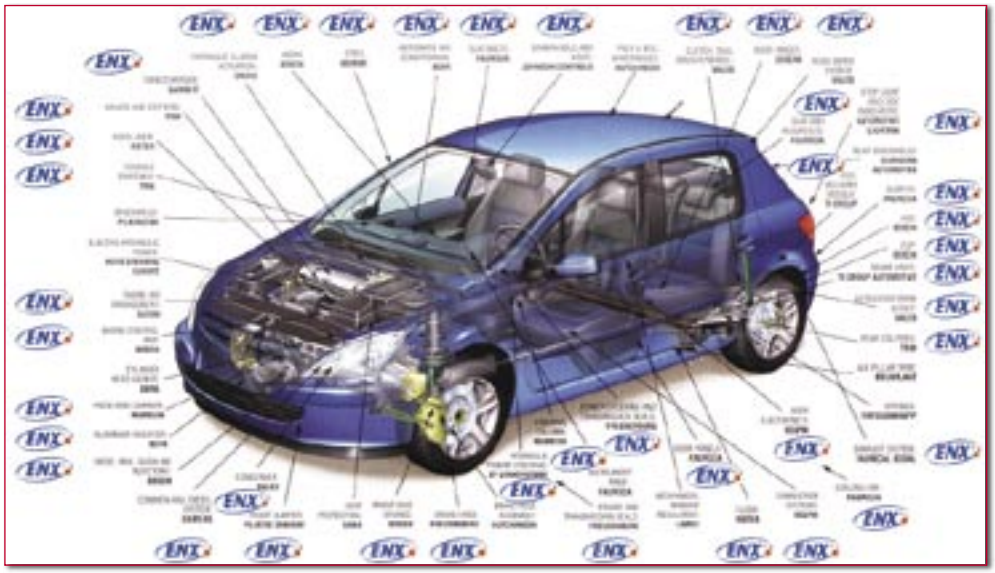
De nombreuses entreprises proposent donc des systèmes complémentaires aux firewalls et application de gestion de droits d'accès

> ***« Les frontières entre les données personnelles et les données de l'entreprise sont de plus en plus floues. Et la malveillance n'est pas le risque principal ! »***

au réseau de l'entreprise, pour bloquer tous supports de copie illicites. Le logiciel DeviceWall de Centenial Software commercialisé par Query Intégration par exemple gère l'accès aux classes de médias amovibles choisies selon les besoins légitimes des utilisateurs. Cette application permet donc de paramétrer finement les privilèges de sécurité de chaque utilisateur sur une machine en réseau ou en autonome. Elle peut bloquer toute tentative d'utilisation d'une large variété de supports : disques et clés USB, cartes *Compact Flash*, appareil photo numérique, lecteurs MP3, PDA, Smartphones, lecteurs ZIP... et ceci sur tous les ports de connexion, y compris Bluetooth et Wi-fi ! Il est également en mesure de fournir des autorisations temporaires avec une traçabilité des opérations effectuées.

La période des transferts...

L'échange de données avec un partenaire extérieur à l'entreprise ou à son réseau constitue l'un des principaux risques de piratage. Les procédés les plus couramment utilisés dans l'industrie sont le FTP et les liaisons VPN. Le premier est un protocole de transfert répandu mais sans véritable protection puisque les mots de passe circulent en clair sur le réseau. A combiner donc avec des outils de cryptage disponibles sur le marché genre Pkzip, PentoZip, etc. Le VPN (*virtual private network*) est, lui, une liaison privée physique ou plus souvent logique avec un système de cryptage des données. C'est donc un moyen particulièrement sûr, fondé sur



Environ 800 entreprises européennes utilisent le réseau privé d'échange de données ENX mis en place par le secteur automobile. (Doc. Galia)

un système de clés privées et publiques permettant aux seuls destinataires de lire les données.

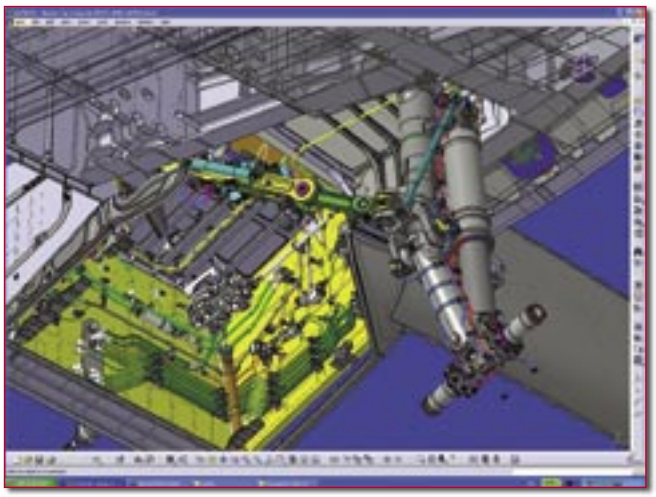
L'efficacité et la sécurité des communications sont critiques pour les constructeurs de l'industrie automobile, ainsi que pour les fournisseurs et les revendeurs. Les fournisseurs qui travaillent avec une multitude de constructeurs, qui eux-mêmes exigent l'utilisation de leur solution de communication spécifique, n'ont pas le choix. Ils doivent cependant refléter le système d'échange de données de chaque constructeur dans leur société et donc mettre en œuvre et gérer différentes solutions simultanément. Il en est de même pour les communications avec les sous-traitants des fournisseurs. Ceci crée une multitude de moyens de communication, avec différents protocoles, différentes interfaces utilisateur et systèmes de transfert, et pour finir, des coûts importants pour un dédale de solutions de connexion individuelles, isolées et inflexibles. D'où la création d'un accès unique pour l'ensemble de l'industrie.

« ENX (European Network eXchange) est une plate-forme d'échange de données privilégiée par l'industrie automobile européenne et mise en œuvre depuis juillet 2002. Le nom représente l'organisation aussi bien que le produit lui-même. ENX a été créée par un groupement de 20 constructeurs, de fournisseurs et d'associations de l'automobile. Il s'agit d'une infrastructure de communication unifiée qui combine les avantages d'un Internet professionnel, ouvert et flexible, avec la sécurité et la performance d'un réseau local d'entreprise » explique Nadine Buisson-Chavot chef de projet EDI et ENX chez Galia.

C'est Galia, l'un des membres fondateurs qui a en charge son évolution et sa diffusion dans l'industrie. Sa mission : élaborer des standards d'échange, promouvoir ces technologies et assister ses adhérents dans leur mise en œuvre. En Europe, l'organisme est représentée par l'association Odette et fait partie d'un consortium international d'organismes similaires (VDA, AIAG, Jama...).

Environ 800 partenaires européens utilisent ce réseau virtuel privé (VPN) totalement « étanche » vis-à-vis d'Internet, et ceci principalement pour de l'échange de fichiers CAO. Largement adopté par les constructeurs automobiles européens, mais également par Ford et Toyota, ce système intéresse aussi le secteur aéronautique qui utilise une technologie semblable mais propriétaire et donc coûteuse. Notons également que la DGA a choisi cette solution pour travailler avec ses partenaires et que certains instituts financiers ont suivi la même voie. Une offre spécifique dont les tarifs démarrent à 150 euros/mois a été lancée pour favoriser l'accès des PME à cette infrastructure d'échange.

Sur le plan de la sécurité, ce réseau de communication européen s'appuie sur quatre opérateurs certifiés par l'association (dont France Télécom), les protocoles sécurisés IPsec, OFTP, FTP, des données cryptées via le protocole 3DES, enfin une certification des signatures électroniques par une autorité tiers. Cet outil supporte tous les types d'applications présentes dans l'industrie automobile : EDI, plateaux virtuels, CAO, messagerie, transfert de fichiers, etc. *« Finalement ce système*



Les solutions de CAO comme Catia V5 intègrent des outils permettant de « vider » un modèle natif de sa structure et donc des intentions de conception.

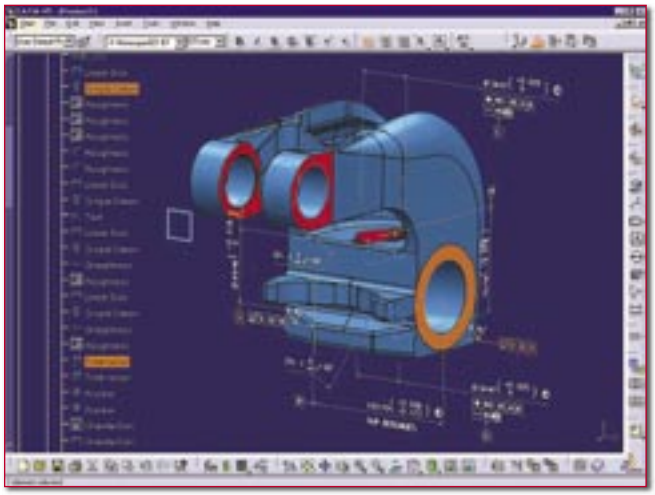
VPN se fonde sur trois couches fondamentales pour garantir la sécurité et la fiabilité des échanges. La première c'est le « tuyau » : ENX, la seconde c'est le protocole d'échange : OFTP est le plus fréquent, enfin le processus ENG DAT V3 est une enveloppe numérique formalisant l'échange et son processus entre les partenaires (demande d'échange, accusé réception de la demande, processus de validation, etc.). Ce troisième niveau est en cours de déploiement dans l'industrie » ajoute Nadine Buisson-Chavot.
Alexandre Loire, Chef de Projet Galia rajoute : *« Notre organisation travaille également sur la notion de préservation de la propriété intellectuelle et notamment autour du logiciel Catia V5. Ce dernier dispose par exemple d'une fonctionnalité permettant de « vider » un modèle natif de sa structure et donc des intentions de conception. De la même manière, des travaux sont en cours sur les formats d'échange de données CAO et sur leur qualification par rapport aux formats spécifiques à la simple visualisation des modèles. Car, malgré son avancement en la matière, même l'industrie automobile utilise quasi systématiquement les formats natifs de CAO ! Si les constructeurs automobiles et leurs équipementiers de rang 1 sont conscients du problème et nous interrogent sur le sujet, les PME n'en sont pas encore là. La plupart transmettent directement par messagerie Internet leurs modèles CAO sans trop se soucier du format, pourvu que celui-ci soit lisible par leurs partenaires ou donneurs d'ordres. D'ailleurs, peu d'entre elles dévoilent totalement leurs pratiques d'échange, tant les processus sont encore peu formalisés et fiables... ».*

> ***« La plupart transmettent directement par messagerie Internet leurs modèles CAO sans trop se soucier du format, pourvu que celui-ci soit lisible. »***

Que faire à l'échelle du BE, du projeteur ?

Sécuriser ses données CAO, c'est aussi conserver ses droits sur la propriété intellectuelle.

La tâche se complique avec l'avènement et la démocratisation galopante des technologies numériques, d'Internet et du travail collaboratif. Le numérique est désormais un outil majoritairement adopté par les entreprises, qu'il s'agisse de traiter la géométrie, la simulation, le calcul, la visualisation réaliste ou encore l'aspect tolérancement. Sans hésitation, il remplace avantageusement le support papier grâce, entre autres, à sa capacité à véhiculer une grande quantité d'information. Mais, cette caractéristique positive peut parfois se retourner contre son utilisateur. Un fichier CAO est en effet susceptible de contenir plus d'informations que ce qui est strictement nécessaire à sa destination. D'où un risque supplémentaire (par rapport au support imprimé) lors du partage ou du stockage de ce fichier, de voir ses intentions de conception, ses innovations ou son savoir-faire atterrir sur un poste de travail non autorisé...



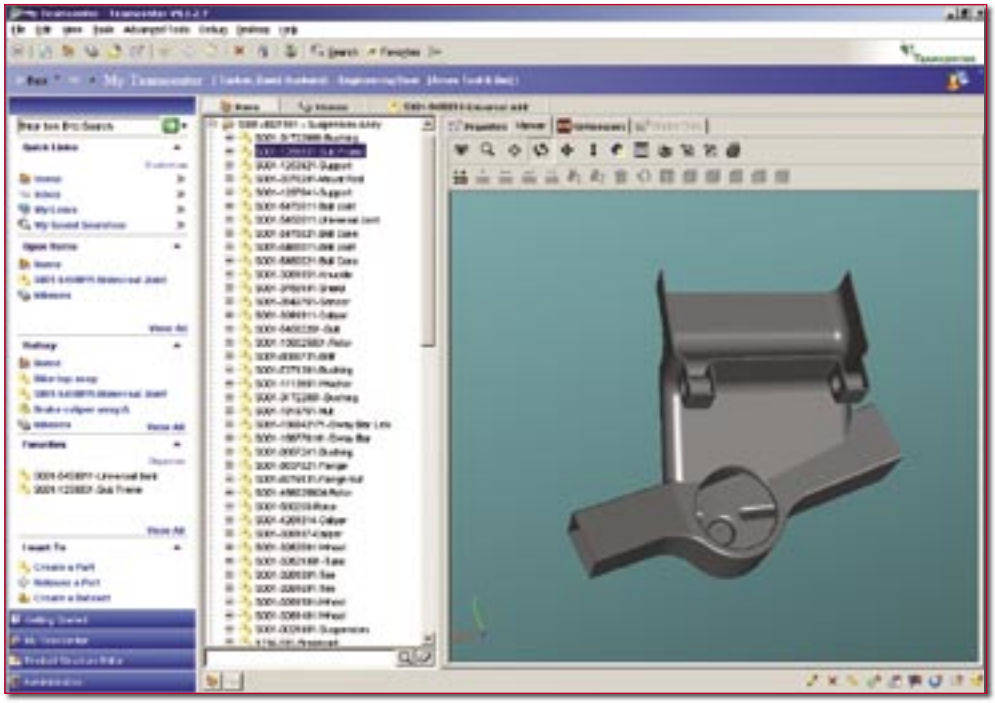
Transmettre à son partenaire le juste nécessaire à l'accomplissement de sa tâche. (Doc. Dassault Systèmes)

Quelles que soient les organisations des entreprises industrielles en terme de réseaux, de logiciels, de protocoles d'échanges, de partenaires extérieurs... il est possible de donner une démarche commune pour optimiser la sécurité de ses données sur son poste de travail. Celle-ci repose sur trois fondamentaux relativement faciles à mettre en œuvre : la sécurisation de son réseau informatique, limiter ce que l'on partage et adopter des clauses contractuelles légales en matière de sécurité et de confidentialité. Nous ne rentrerons pas ici dans le détail des méthodes à adopter, nous voulons juste rappeler quelques règles de bon sens souvent négligées par les entreprises.

Sécuriser son réseau local

Outre les outils et procédures que les directions informatiques imposent à leurs salariés (bien souvent sous la pression de leurs clients...), certaines précautions basiques peuvent être prises et éviter bien des problèmes. Première démarche élémentaire de précaution : sécuriser vos procédures d'entrée et de sortie pour ne permettre un accès réseau qu'aux seuls membres autorisés. Ensuite, assurez-vous que tous vos dossiers contenant vos fichiers critiques sont placés sur des répertoires visibles seulement des personnels autorisés. Combien de

> ***« A partir du moment où il est possible de visualiser un dossier sur le réseau, il est facile de le copier et de le transférer par mail ! »***



Attention au bon paramétrage des outils de gestion de données techniques ou de GED, notamment à la présence de « back doors »… (Doc. UGS Team Center)

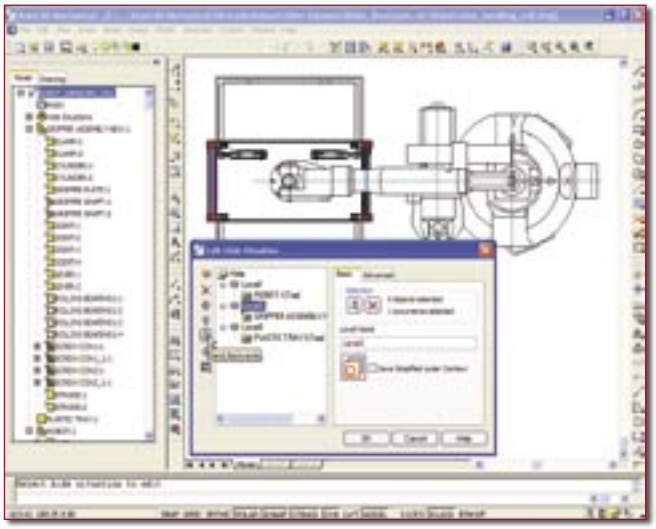
projeteurs stockent en effet leurs données sur des volumes publics pouvant être parcourus par tout le monde ? Même si l'on spécifie quels membres de l'équipe peut éditer les dossiers, la sécurité sur ce qu'ils contiennent est quasi nulle. A partir du moment où il est possible de visualiser un dossier sur le réseau, il est facile de le copier et de le transférer par mail !

De la même manière, si vous employez des serveurs FTP pour partager des données en interne ou avec vos partenaires extérieurs, prenez la précaution d'utiliser les mêmes commandes réseau pour tous les dossiers partagés. En effet, trop de PME élaborent et mettent en place des pratiques parfaitement sécurisées vis-à-vis de leur réseau central, mais laissent un flou artistique en la matière quant à leurs serveurs FTP ! Très facilement accessibles, ces portes sont employées pour échanger tout et n'importe quoi avec l'extérieur. Pour un contrôle rigoureux, il est nécessaire d'interdire systématiquement les ouvertures de sessions anonymes. Le plus simple reste un accès par mot de passe pour toutes les personnes qui se connectent au serveur, et l'obligation de changer régulièrement ce mot de passe. Dans le cas où votre entreprise travaille avec un outil de GED ou de gestion de données techniques, il peut également être sain de s'assurer qu'il n'est pas possible de copier des dossiers en dehors du système. Attention à la présence fréquente de *« back doors »* dans les logiciels du commerce, qui sont souvent paramétrées « ouvertes » par défaut… A quoi sert un logiciel de travail collaboratif dernier cri, si son paramétrage n'est pas soigneusement vérifié !

Il faut insister encore sur l'importance des mesures à prendre pour éviter que les dossiers sensibles soient visibles par des personnes non autorisées sur la totalité de votre infrastructure informatique. D'une part parce que les copies illégales sont trop faciles, d'où une perte de confidentialité de vos données, mais d'autre part parce que vous risquez de perdre aussi le contrôle des révisions des plans. Adieu donc la traçabilité tant martelée par votre responsable qualité ! Même si ces mesures de sécurité imposent quelques contraintes pour le personnel, elles sont indispensables pour vous protéger de vos concurrents, d'un salarié indélicat ou inattentif, ou simplement pour respecter les contrats de confidentialité que vous avez passés avec vos clients. Si l'équipe dirigeante laisse un peu trop de liberté au personnel sur ce sujet, il sera difficile de faire machine arrière.

Limiter les informations partagées

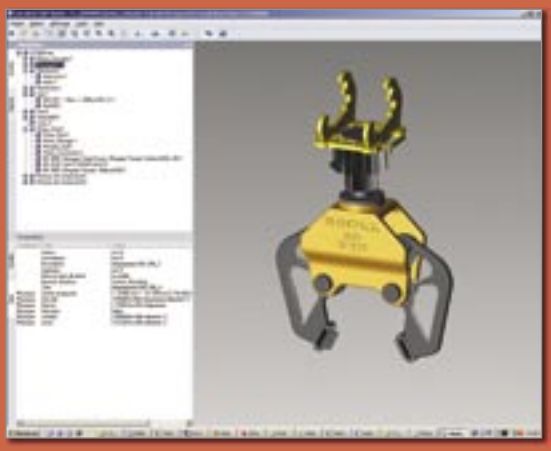
Après avoir optimisé la sécurité du « contenant », c'est-à-dire vos réseaux informatiques, on peut également diminuer le risque de fuite en limitant le « contenu », c'est-à-dire la quantité d'informations partagées. Lors des échanges avec les clients et fournisseurs, il convient



Autodesk propose le format DWF et un viewer gratuit pour le partage sécurisé des données 2 et 3D.

Microsoft prend en charge le format DWF d'Autodesk

Microsoft prend désormais en charge le format de données DWF pour permettre aux utilisateurs des logiciels de ce dernier d'intégrer facilement des informations de conception aux applications Microsoft Office, Great Plains et Axapta de Microsoft Business Solutions, maintenant Microsoft Dynamics. Pour sa part, Autodesk prévoit la prise en charge du format XAML (Extensible Application Markup Language) de Microsoft par DWF pour début 2007. Cela permettra aux utilisateurs de Windows Présentation Foundation de partager plus facilement un contenu de conception 3D complexe avec des utilisateurs non-CAO. Il sera notamment possible de rechercher et récupérer avec MSN Search des informations basées sur le format DWF pour trouver plus facilement des spécifications de conception et des informations critiques postées sur l'Internet.



Dès à présent, avec l'application DWF Writer, les concepteurs peuvent se servir de la fonction d'édition en un seul clic de Microsoft Office pour éditer des données de visualisation 2D et 3D. Ils peuvent également partager des dessins, des cartes et des modèles dans des applications Microsoft Office en glissant/déposant simplement le fichier DWF dans la fenêtre d'application et pré-visualiser, rechercher, imprimer et envoyer par e-mail des fichiers DWF directement dans Windows Explorer. ◘

d'adopter les procédures et les formats de fichiers les plus adaptés. Il s'agit de transmettre le juste nécessaire d'informations dont a besoin le destinataire. Si ce dernier n'exige pas un format natif, il peut être souhaitable d'adopter un format intermédiaire performant comme le PDF d'Adobe, le DWF d'Autodesk ou encore le eDrawings de SolidWorks. Ces formats supportent les informations géométriques, mais pas les vraies données de conception. En outre, les visualiseurs correspondants sont gratuits. Les versions « pro » supportant toutes les fonctions offertes par ces formats sont quant à eux payants. Le PDF d'Acrobat présente de nombreux avantages, surtout dans sa version 7. C'est d'abord le plus répandu, c'est sans doute le plus simple d'emploi et certainement le plus universel.

Autodesk de son côté pousse son format DWF qui est disponible dans tous ses logiciels de CAO (un plug-in permet de créer un DWF à partir de tout autre logiciel CAO du marché) pour le partage sécurisé de plans 2 et 3D. Il offre l'avantage d'être conçu spécifiquement pour transférer des données CAO et se caractérise notamment par son taux de compression élevé. Le viewer gratuit peut être utilisé sans compétences préalables en CAO pour visualiser et imprimer des croquis, plans et modèles 2D et 3D au format DWF et accéder à certaines données complexes de conception sans l'application d'origine. La version payante DWF Composer offre des fonctionnalités supplémentaires paramétrables liées aux processus de révisions numériques : gestion des calques, navigation dans les calques, zooms, impression, prise de cotes exactes, annotation, arborescence des annotations, accès aux données de conception, réintégration des annotations et autres modifications dans AutoCAD, etc.

Comme Autodesk, SolidWorks a lancé un format d'échange sécurisé des données similaire aux fonctionnalités du format DWF. Trois outils sont disponibles dont eDrawings Viewer et eDrawing Publisher qui sont gratuits. Le premier ouvre non seulement les fichiers eDrawings, mais aussi les fichiers de CAO SolidWorks natifs ainsi que les fichiers DXF et DWG d'AutoCAD. Il permet également de naviguer dans un modèle volumique ou un dessin 2D, de zoomer, d'animer des pièces ou des assemblages de modèles, de passer du modèle volumique à sa représentation plane, etc. eDrawings Publisher est l'outil de création de formats eDrawings directement à partir des logiciels SolidWorks, mais aussi AutoCAD, Inventor, Pro/E, Catia V5 et Unigraphics/NX ! Enfin, la version Professionnal payante permet en plus de gérer les révisions : marquage, prise de mesure, protection du document par mot de passe, coupe, déplacement, éclatement de pièces, etc.

Correctement employés, ces différents formats de fichiers permettent à vos partenaires de visualiser les informations dont ils ont besoin, sans divulguer des données de conception précieuses. Evitez tant que

possible de transmettre vos fichiers natifs. N'hésitez pas non plus à gagner un cran de sécurité supplémentaire grâce aux utilitaires de compression qui permettent en plus de diminuer la taille de documents, d'encoder simplement le mot de passe. Seul le destinataire à l'aide de sa clé pourra ouvrir l'archive compressée…

« Blinder » vos contrats

Si les contrats légaux passés avec vos clients n'ont jamais empêché une personne mal intentionnée de copier vos documents, leur validité peut cependant assurer votre couverture juridique en cas de piratage. Il convient donc d'y prêter attention, d'autant plus que la rigueur de leur rédaction et des garanties qu'ils apportent confirme à vos clients le sérieux que vous portez à leur demande de confidentialité. En contrepartie, cela exige de votre part une « obligation de moyens », c'est-à-dire des dispositions (matériels, logiciels, procédures…) que vous devez prendre pour tenir les engagements signés. De manière générale, les contrats classiques comprennent les dispositions suivantes concernant le transfert de données par voie numérique :

– confidentialité : le destinataire ne copiera ou ne distribuera pas les informations que vous lui envoyez,

– mot de passe : le destinataire maintiendra tous les mots de passe bloqués et suivra toutes les procédures de sécurité requises pour accéder à vos serveurs FTP et GED,

– destruction : le destinataire s'engage à détruire les informations après leur délais d'utilisation,

– copyrights : le destinataire ne réutilisera aucun élément de votre conception numérique dans un autre projet sans votre consentement écrit.

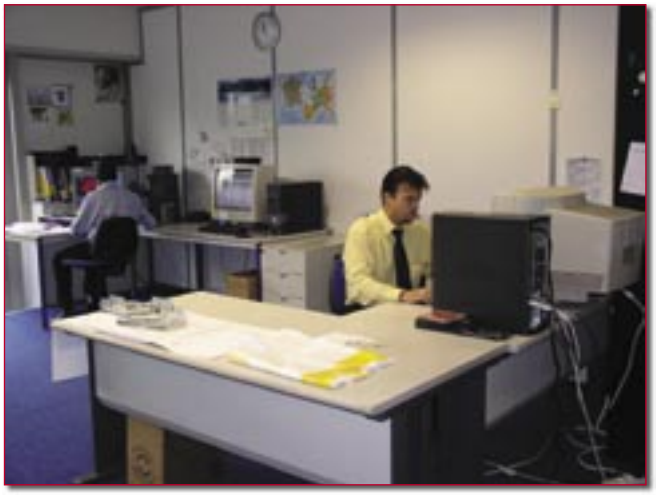
Il est également bien-venu de spécifier contractuellement quels types de fichier peuvent être échangés et quelles procédures doivent être employées pour accéder aux différents serveurs de l'entreprise, ceci afin d'optimiser la portée légale du contrat.

La visionneuse eDrawings de SolidWorks permet de consulter les fichiers créés dans AutoCAD (DWG et DXF) et les pièces, assemblages et mises en plan réalisés dans SolidWorks.

Bien sûr, il n'existe pas de parade 100 % efficace contre la perte ou le vol d'information, et les fichiers issus de la conception ne sont pas les seules données critiques de votre entreprise. Reste, qu'au même titre que vos données comptables, elles constituent un capital fondamental de l'entreprise et qu'en la matière il vaut mieux prévenir que guérir…

Deux témoignages représentatifs

Entreprise familiale créée il y a près de 25 ans, SNOP appartient aujourd'hui au groupe FSD et emploie quelques 2250 salariés. Cette entreprise de découpage-emboutissage travaille exclusivement pour l'automobile. Secteur pour lequel elle produit des pièces de structure, des supports moteurs ou encore des éléments de sécurité, puis les assemble. Sami Beugnon, responsable fonctionnel du système d'information : « *La politique de l'entreprise est prioritairement le partage de l'information, ce qui peut parfois être antinomique avec les exigences de la sécurité. Cependant, notre démarche qualité porte également attention à cet aspect et notamment à la confidentialité des informations qui circulent sur notre réseau. Il s'agit donc de trouver le juste milieu entre protection et ouverture afin de ne pas brider la productivité des salariés sous une paranoïa protectionniste. La direction informatique a donc déployé une structure informatique propre à garantir un niveau de sécurité optimal. D'une manière générale, les accès réseau sont gérés par des mots de passe utilisateur, combinés à la reconnaissance de la machine par le système. S'il s'agit d'une personne extérieure à l'entreprise qui souhaite brancher son portable, il est nécessaire de créer un accès temporaire. Pour échanger de l'information avec nos donneurs d'ordres automobile, nous utilisons un réseau VPN et les protocoles normalisés*



Les fournisseurs de l'industrie automobile comme la société SNOP bénéficient de la sécurité apportée par le réseau professionnel ENX.

Pister ses documents

Annonce importante d'Adobe concernant la sécurité de l'échange de données, l'éditeur vient de racheter la technologie de gestion des droits numériques FileLine de la société américaine Navisware. Il s'agit d'une entreprise faisant le lien entre la conception numérique et le décisionnel. Avec cette acquisition, Adobe LiveCycle Policy Server bénéficiera de nouvelles fonctionnalités permettant une protection permanente de documents stratégiques aux formats PDF, Microsoft Office et CAO, indépendamment de leur mode de stockage ou de diffusion. Ces fonctionnalités permettent d'appliquer aux documents des règles de contrôle sur leurs modalités et dates d'utilisation ainsi que sur l'identité de leurs utilisateurs. À noter qu'un journal d'audit aisément consultable révèle aux cadres comme aux auditeurs l'identité de tous ceux qui ont accédé à un document et indique, le cas échéant, ses utilisations à mauvais escient ou divulgations. Cette même technologie garantira la gestion des versions d'un document si son propriétaire décide d'une révocation immédiate ou d'une expiration à une date donnée. Adobe annonce une disponibilité de ces outils pour l'automne 2006. ◘

dans ce secteur. La démarche d'échange de données est déterminée avec chacun d'entre eux, qui généralement nous imposent ses pratiques. Ainsi, nous utilisons des lignes Numéris pour transmettre nos données CAO à travers un serveur spécifique. Les formats de fichiers échangés sont liés à la demande du client, cela peut être du natif Catia V4, du V5 ou du Unigraphics NX. »

Bureau d'ingénierie, Matis Technologies a un panel de clients plus diversifié puisqu'il réalise des études pour les constructeurs automobiles, mais également pour l'aéronautique et le spatial. Mais, comme le souligne Stéphane Bourdeau, directeur informatique : *« Bien évidemment les notions de sécurité et de confidentialité sont une problématique sensible pour nos clients, qui œuvrent dans des secteurs extrêmement concurrentiels. Pour pouvoir travailler avec eux, vous devez d'une part garantir un niveau de sécurité interne minimal, et d'autre part adopter les procédures et techniques d'échange de données qu'ils utilisent. Ce sont les standards définis par l'organisme Galia par exemple qui établissent nos méthodologies de transfert de données avec les partenaires automobiles. Toutes nos données circulent donc à travers des réseaux sécurisés de types Numéris et ENX, elles sont compressées et cryptées à l'aide d'un système de clés. Et en interne, nous avons une charte qualité qui prévoit les procédures habituelles d'identification et d'autorisation pour accéder au réseau d'entreprise. Nous avons également limité les postes de travail où l'on peut graver des cédéroms ou connecter des supports amovibles de stockage. Une infrastructure à base de disques Raid 5 assure une sauvegarde complète des données toutes les semaines et incrémentale chaque jour. Par ailleurs, nos ingénieurs travaillant régulièrement sur les plateaux de développement de nos clients, nous avons mis en place une procédure systématique de reformatage complet lors du retour des machines. Certaines entreprises comme Snecma exigent un formatage en entrée et en sortie de projet. Et il n'y encore pas très longtemps, nous devions purement et simplement détruire les disques durs après utilisation chez le client… ».*

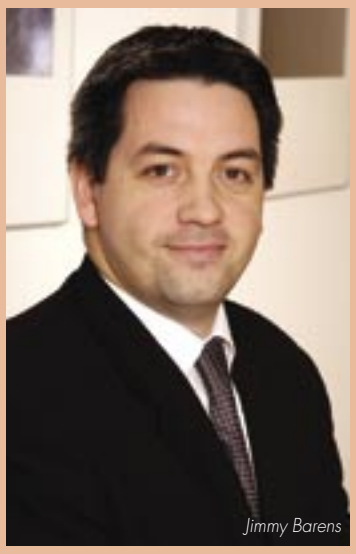
Le cas Adobe

L'éditeur multiplie les annonces et montre une implication forte dans le domaine de l'échange de données géométriques. Depuis la dernière version d'Acrobat Professionnel, la V7, il était déjà possible d'intégrer un modèle 3D au sein d'un document PDF. Avec Acrobat 3D, Adobe va plus loin et souhaite étendre l'utilisation de la 3D à toute l'entreprise avec un PDF composite, sécurisé et interactif. Et avec plus de 1,25 milliard d'exemplaires du logiciel gratuit Acrobat Reader diffusés à ce jour, l'éditeur part sur des bases plus que sérieuses en la matière… *« Il s'agit de décloisonner l'usage de la 3D du bureau d'études et de permettre sa communication sécurisée à toute personne de l'entreprise étendue pouvant en avoir besoin. Quelle que soit votre plate-forme, vous pourrez désormais visualiser un assemblage complexe à l'aide de notre viewer gratuit, mais également explorer, mesurer ou*

Acrobat 3D est la nouvelle solution d'Adobe pour intégrer de la 3D interactive dans un document PDF tout en satisfaisant aux exigences de sécurité.

Interview Jimmy Barens, Directeur avant-vente d'Adobe France

« Adobe ne propose pas de technologie de sécurisation des infrastructures informatiques dans lesquelles transitent les données numériques. En revanche, nous apportons une sécurité forte sur le document lui-même à travers le format PDF et les fonctionnalités d'échange entre partenaires qui lui sont liées.


Jimmy Barens

Nous adoptons ainsi les standards du marché en matière de chiffrement du PDF lors de son envoie. Un exemple de scénario : je suis l'auteur d'un document PDF intégrant un modèle CAO 3D dont je souhaite protéger la conception. Acrobat me permet dans ce cas de décimer les polygones du modèle, d'enlever des textures pouvant indiquer la nature des matériaux, d'interdire la prise de cote ou encore d'enlever la structure interne de l'assemblage. Le contenu du PDF est toujours « en clair », mais il ne comporte plus d'informations stratégiques. Je peux ensuite décider de le crypter avant de le transmettre à mon partenaire. Pour cela, Acrobat scanne les technologies de chiffrement que j'utilise habituellement sur mon poste de travail et les rend disponibles directement dans son interface d'utilisation.

Notons au passage qu'Acrobat offre par défaut un outil de cryptage de type RSA. Evoquons également la signature électronique, qui n'apporte pas une sécurité directe, mais valide pour l'expéditeur la réception du document par la bonne personne. Enfin, nous travaillons activement avec l'organisme Galia pour faire reconnaître les possibilités de notre format PDF et avons initié un groupe de travail sur le sujet. » ▫

encore annoter ce modèle 3D issu d'un logiciel de CAO et intégrer à un fichier PDF », explique Jimmy Barens, Directeur avant-vente d'Adobe France.

Acrobat 3D étend donc les fonctionnalités déjà présentes dans Acrobat 7.0 avec notamment trois possibilités complémentaires :
– création d'un PDF intégrant un modèle 3D à partir de son application CAO favorite ou à partir de fichiers natifs quelconques,
– insertion de modèles CAO 3D dans un document Office (Word, Excel, Powerpoint) et conversion du fichier résultant en PDF,
– création de documents PDF intégrant un modèle 3D enrichi (animations, éclaté, modification de l'éclairage, des textures…) et offrant à son destinataire une forte interaction : prise de cotes, coupes, annotations, affichage/masquage des calques, de parties ou de pièces… Notons qu'il est possible de récupérer les annotations et révisions uniquement dans AutoCAD et Word 2006. En outre, le logiciel intègre un outil supplémentaire baptisé 3D ToolKit qui permet de réaliser des animations d'assemblage/désassemblage de modèles 3D de haute qualité.

Ces nouvelles capacités du format PDF en font désormais un sérieux concurrent aux formats d'échange propriétaire d'Autodesk, de Dassault Systèmes ou de SolidWorks. Acrobat 3D ouvre ainsi la porte à de nouveaux usages des modèles 3D CAO, intégrés à un document de type bureautique et interactifs : présentations de projets, réalisation de documentations marketing, d'outils de formation, de notices de montage ou de maintenance, mais également de révision de projet, grâce aux outils d'annotation, de révocation de document, de signature numérique, etc. Autant dire que l'éditeur ne limite pas le marché potentiel à l'industrie ! A quand la notice de montage animée de votre dernier meuble de rangement, une notice explicite pour vidanger votre voiture, ou une présentation réaliste et attractive de vos achats par correspondance ? Acrobat 3D est commercialisé au prix de 1200 € et disponible en 4 langues dont le français.

Sur le plan de la sécurité, le format PDF bénéficie d'une ouverture par mot de passe, du certificat de signature électronique et de la technologie d'Adobe « Policy Server ». Cette dernière permet au créateur du document de préciser sa durée de vie, ainsi que les personnes autorisées à l'ouvrir. Enfin, le logiciel assure une décimation des faces du modèle 3D ce qui permet d'une part de diminuer le poids du fichier dans lequel il s'intègre, mais surtout de ne pas délivrer le modèle complet et les intentions de conception qui s'y rattache. ▫