Définir les données pour mieux protéger les documents

En l'absence de classification documentaire, il est impossible de savoir ce qu'il faut protéger.

Sommaire

Ce deuxième article technique d'une série de trois analyse la manière dont les services informatiques peuvent donner aux collaborateurs nomades les moyens d'exploiter efficacement des documents sans renoncer pour autant à leurs propres impératifs.

Partie I - Un exercice d'équilibriste : concilier les conflits d'intérêts entre services informatiques et utilisateurs dans un monde mobile

Partie II - Définir les données pour mieux protéger les documents

Partie III - Gérer la mobilité d'entreprise par un modèle informatique hybride

Dans le précédent article technique, « Un exercice d'équilibriste : concilier les conflits d'intérêts entre services informatiques et utilisateurs dans un monde mobile », nous avons abordé les attentes documentaires des employés extrêmement mobiles. Les environnements mobiles et cloud comportent des risques susceptibles d'engager la responsabilité de l'entreprise ou de nuire à sa sécurité. Parallèlement à l'essor des outils de partage et de synchronisation de fichiers, les équipements personnels ont envahi nombre de lieux de travail, les employés s'en servant pour transmettre et stocker des documents professionnels sensibles. Et aujourd'hui, ces collaborateurs ne se contentent pas d'accéder en toute sécurité à du contenu professionnel sur leurs équipements mobiles : ils manipulent également de nouveaux contenus créés dessus.

Mais l'univers mobile rend également ce personnel infiniment plus productif et n'est donc pas près de disparaître. Le présent article technique tente de répondre à la question suivante : comment le service informatique peut-il régir et protéger le contenu dans des environnements spécifiques et semi-structurés de cet ordre ?

Les documents confidentiels dans un monde mobile

La mobilité d'entreprise étant avalisée par les entreprises elles-mêmes, la protection des documents électroniques contenant des informations confidentielles est une tâche délicate dont les conséquences peuvent s'avérer fâcheuses. Un incident de sécurité est onéreux, non seulement sur le plan financier, mais aussi pour la perte de confiance qu'il peut engendrer côté clients. Dans une récente étude réalisée par PWC, 28,6 % des personnes interrogées indiquent que leur entreprise a subi des pertes financières suite à un incident de sécurité.

Or, pour ce qui est des documents, nombre de solutions de sécurisation se contentent de protéger leur contenu électronique sur leur lieu de stockage ou durant leur transfert uniquement. Elles n'assurent, de surcroît, aucune protection sur l'intégralité du cycle de vie du document électronique.

Si, dans les environnements mobiles et cloud, l'accès aux informations de l'entreprise n'est certes pas une source de préoccupation pour tous les employés, nombre de sociétés comptent, dans leurs équipes, certains éléments « atypiques » :

- Ils travaillent avec plusieurs équipements et veulent pouvoir synchroniser leurs fichiers de l'un à l'autre
- Ils se servent de différentes applications (en plus de la messagerie électronique ou du calendrier) pour effectuer leur travail sur mobiles
- Ils sont fréquemment en déplacement
- Ils participent à des programmes BYOD, le cas échéant

Ces collaborateurs sont quelque peu « en décalage » par rapport à un modèle informatique qui part du principe qu'ils sont tous derrière le pare-feu de l'entreprise, sur le même réseau local (LAN), en train d'utiliser le même type d'équipement. Vous avez besoin d'un modèle en phase avec la réalité, c'est-à-dire adapté aux collaborateurs nomades, mais qui protège également les fichiers à l'extérieur du pare-feu.

Maîtriser le contenu

La classification des données est un aspect souvent négligé, et pourtant fondamental, de la protection et du contrôle documentaires. En l'absence de classification documentaire, il est impossible de savoir quels documents nécessitent une protection.

Le tableau suivant fournit un exemple de schéma de classification de données pour les informations électroniques stockées et transmises. Les catégories sont volontairement simples pour être plus facilement exploitables et améliorer la conformité.

Classification des données	Définition	Exemples
Public	Informations librement accessibles, sans que cela ait de conséquences pour l'entreprise.	Informations publiées sur le site web en libre-accès, publicités, communiqués de presse
Interne	Informations à la disposition du personnel permanent et des intérimaires, mais non destinées à être diffusées publiquement.	Données de l'annuaire interne du personnel, certaines actualités de l'entreprise
Confidentiel	Informations à la disposition d'un groupe restreint d'employés et de sous-traitants, selon le principe du « besoin de savoir », en fonction du rôle de ces collaborateurs.	Circulaires, plans, documents stratégiques, contrats, données clients
Privé	Informations extrêmement précieuses. L'accès non autorisé à ces données est susceptible d'occasionner des risques substantiels sur les plans commercial et réglementaire. Les informations de cette catégorie sont mises à la disposition d'un groupe restreint d'employés et, éventuellement, d'autres personnels spécialisés.	Données du personnel, rapports financiers internes, données clients confidentielles, informations sur les fusions et acquisitions, accords de confidentialité, business plans, informations privilégiées, informations réglementaires

S'il est indéniable que vous devez vous montrer sélectif sur le type de données autorisées à résider sur mobiles ou transférées dans le cloud, il est difficile de savoir par où commencer. La classification des informations électroniques constitue un cadre permettant d'agencer les données en fonction de leur degré de vulnérabilité et de monopoliser les ressources sur le contenu le plus vulnérable.

Une fois le contenu classé en catégories, il s'agit de définir les niveaux de protection exigés pour chacune d'elles. Décidez, par exemple, du type de documents pouvant être raisonnablement stockés dans un cloud public. Les données jugées trop précieuses pour y résider ne devraient pas être aisément accessibles sur mobiles. Le stockage dans le cloud n'est en effet pas le seul facteur à prendre en compte. Comme nous l'avons mentionné dans le précédent article technique, les collaborateurs veulent souvent avoir la possibilité de consulter des documents hors ligne, sur un équipement mobile. Or, si ce dernier est dérobé, les documents qui s'y trouvent le sont aussi.

De surcroît, en pilotant des programmes de gouvernance pour les collaborateurs les plus susceptibles d'exploiter des solutions documentaires sur mobiles, vous pouvez également optimiser la protection documentaire de votre entreprise.

Explorer les fonctions de contrôle intégrées aux documents

Il est difficile de protéger les documents dès lors qu'ils sont partagés hors de l'entreprise ou du système de gestion documentaire. Pourtant, les outils logiciels de protection documentaire limitent les risques : tout document transmis bénéficie du niveau de sécurité choisi. Voici quelques exemples :

Cryptage. À chaque fois que vous créez et partagez un document numérique contenant votre propriété intellectuelle, des informations confidentielles ou d'autres contenus sensibles, vous devez le protéger afin d'empêcher toute utilisation abusive ou inappropriée. Les autorisations définissent les opérations permises sur un document protégé. Des autorisations par mot de passe, par exemple, permettent de déterminer si le destinataire d'un document est autorisé à ouvrir ce dernier, à l'imprimer ou à le modifier, que ce soit en reproduisant son contenu, en le complétant, en y insérant des commentaires, en ajoutant ou supprimant des pages, ou en y apposant une signature numérique.

Biffure. Cette fonction donne accès à un ensemble d'outils qui vous permettent de sélectionner du texte ou des illustrations confidentiels (noms de clients, numéros de compte et adresses) dans votre document PDF et de les supprimer définitivement de ce fichier. Elle permet également de rechercher certaines informations sur la base de modèles courants et de les biffer (numéros de téléphone et de carte bancaire, adresses e-mail). Les informations supprimées sont remplacées par des cadres noirs indiquant très exactement leur emplacement initial. Un peu comme si vous utilisiez un épais marqueur pour noircir du contenu sur une page imprimée, à ceci près que cette technique est plus sûre car les informations confidentielles sont entièrement supprimées du fichier, et pas simplement masquées.

La fonction de biffure est cruciale pour les administrations, entreprises et établissements de tous types et de toutes tailles. Elle limite le risque d'inclure accidentellement des informations confidentielles dans des documents rendus publics et les conséquences juridiques qui pourraient s'ensuivre.

Assainissement. Fonction du même ordre que la biffure, l'assainissement cible les informations masquées à l'intérieur d'un document, qu'il s'agisse de texte, métadonnées, annotations, pièces jointes, calques ou signets. Pour répondre aux exigences de conformité et protéger la confidentialité et la propriété intellectuelle, vous devez être certain que les informations masquées sont supprimées des documents avant leur diffusion.

Certificats ou signatures numériques. Nombre de transactions, notamment celles à caractère financier, juridique ou autre, exigent des garanties autour de la signature de documents. À cette fin, nombre d'entreprises ont choisi de mettre en place leur propre infrastructure de signatures à base de certificats en faisant appel à des autorités de certification tierces pour valider indépendamment l'identité des participants. Ainsi, les laboratoires pharmaceutiques utilisent des signatures conformes au standard SAFE (Signatures & Authentication For Everyone) du consortium SAFE-BioPharma, et les entreprises de l'Union européenne doivent observer les normes PAdES (PDF Advanced Electronic Signatures) de l'ETSI.

Après avoir défini un identifiant numérique reposant sur un certificat, vous pouvez l'utiliser pour signer des fichiers. Les signatures à base de certificats — ou signatures numériques — peuvent être utilisées avec des processus métier qui imposent de valider l'identité du signataire ou l'authenticité du document, d'horodater le document par le biais d'un serveur de tampons temporels, de le certifier en y insérant la signature visible ou masquée de son auteur, ou d'y intégrer les données du certificat pour attester de sa validité à long terme. Vous pouvez créer votre propre identifiant numérique à base de certificat, même si les processus métier exigeant une confiance élevée déploient généralement ceux délivrés par des autorités de certification tierces.

Voyez si ces fonctionnalités peuvent s'appliquer à certains documents de votre schéma de classification des données.

Conclusion

L'accès à des fichiers, leur consultation et leur annotation sur tout type d'équipement est révolutionnaire. Cette faculté dispense les employés d'être asservis à une situation géographique donnée ou à un ensemble restreint d'équipements. Mais, en même temps, cette technologie exige d'accélérer la mise en place de programmes optimisés de protection des données dans l'entreprise.

La classification des données permet d'identifier plus facilement celles qui sont les plus importantes à protéger et donc de prendre les décisions favorisant une approche plus cohérente et structurée en matière de protection des documents. L'analyse des techniques possibles de protection des documents eux-mêmes contribue, elle aussi, à limiter les risques d'incidents de sécurité.

Aujourd'hui, toutes les composantes technologiques nécessaires pour répondre aux besoins documentaires des collaborateurs nomades existent ; toute la difficulté consiste à les réunir de manière cohérente. Raison pour laquelle les employés « bricolent » des solutions inadaptées à une sécurité de niveau entreprise.

Toujours est-il qu'il y a aujourd'hui sur le marché un manque d'applications adaptées à la réalité actuelle : un mélange d'environnements sur site et hors site. Dans notre troisième article technique, « Gérer la mobilité d'entreprise par un modèle informatique hybride », nous exposerons notre vision : des applications mobiles et solutions SaaS qui s'intègrent avec les applications sur postes de travail en place, tout en étant compactes et prêtes pour les environnements cloud et sur site hybrides.

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com, www.adobe.com/fr

7/13