Julien VEHENT

Avril 2007

Intranet pour la sécurité des systèmes d'information

Master
Management de la sécurité des systèmes industriels et des systèmes d'information

---

Sommaire

Cycle de vie d'un Intranet

« Quels sont les principaux points à surveiller au cours de la vie d'un Intranet, en termes de gestion des ressources humaines y accédant et y publiant ? »

En partant du prédicat qu'un Intranet est avant tout un outil de travail collaboratif permettant de centraliser de la documentation (*désolé pour cette lapalissade*), nous pouvons isoler plusieurs axes majeurs de surveillance pour la partie des ressources humaines :

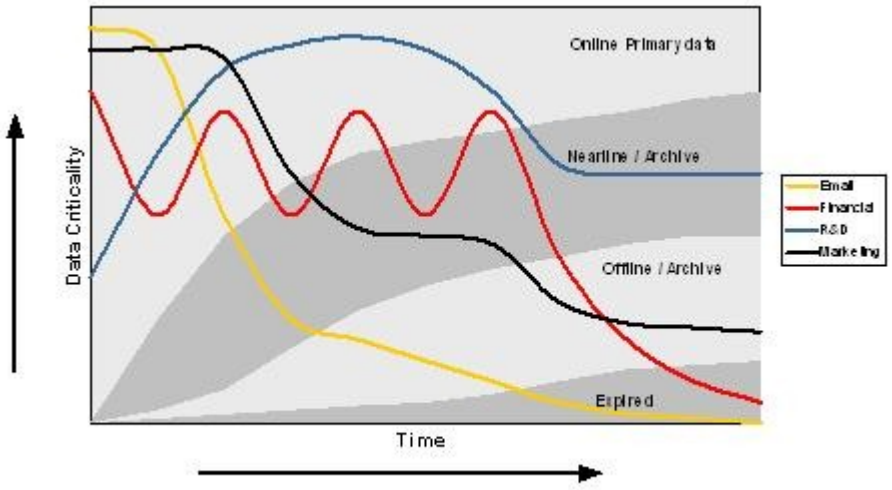
Sécurité des informations stockées

La gestion des habilitations est une tâche active qui doit être auditée à fréquence régulière. La fréquence des audits est liée aux évolutions de structure mais un minimum d'une fois par an est généralement admis comme une bonne valeur.
De même, la classification de l'information est une donnée en mouvement constant. Une documentation confidentielle peut parfaitement perdre ce niveau de confidentialité avec le temps. Afin de ne pas gaspiller des moyens matériels et humains, il est essentiel d'auditer également ces aspects.

Cycle de vie de l'information

La gestion du cycle de vie d'une information est une tâche difficile peu utilisée en entreprise en raison de son coût de mise en place. Dans le cadre d'un Intranet, dont l'objectif est de gérer de l'information, cette donnée doit être prise en compte afin d'éviter de stocker des giga-octets de logorrhée obsolètes et inutiles.

Il existe plusieurs outils d'analyse du cycle de vie que je ne détaillerais pas ici, le graphique ci-dessous donne une idée de ce que l'on peut faire (avec beaucoup de temps et d'acharnement).



Popularité et déviation

Il est presque évident aujourd'hui de déployer un outil statistique d'exploitation des logs lorsque l'on met en place une application web. L'intranet n'échappe pas à cette règle et il peut être utile de connaître les statistiques de consultation des différentes pages, en particulier lorsque la consultation est faible. Cela va aider à l'amélioration de la structure et/ou du contenu, par exemple en effectuant une formation basée sur des résultats précis pour tenter de les améliorer (les résultats...).

A l'inverse, il est également possible que l'Intranet soit victime de sa popularité et soit, de fait, sujet au spam, troll et autre digressions indésirables. C'est un aspect bien connu des administrateurs de forums et qui est généralement résolu par la nomination de modérateurs responsables et justes (s'il en est...).

Favoriser les éléments moteurs

Comme dans toute association de personnes, on va retrouver 3 types de participants à un Intranet : les éléments moteurs, les neutres et les râleurs. Si l'on ne peut rien faire pour les derniers (hormis quelques méthodes moyen-ageuses hélas interdites, au grand damn des militants du MEDEF), il est possible de favoriser les premiers en leurs donnant un pouvoir de décision sur le devenir de l'Intranet, en organisant des réunions de brain-storming, etc...

Ces éléments moteurs tournent, certains sont motivés pendant un temps et finissent par se lasser alors que d'autres vont être tentés par l'expérience un peu plus tard. Il est important de gérer ces personnes car ce sont elles qui font vivre l'Intranet.

Sécurité des mots de passe

« Un projet d'Intranet de management de la sécurité se lance. Quel outil de cryptage choisissez-vous pour coder les mots de passe du Single Sign On ? »

La bonne pratique en matière de stockage des mots de passes est de ne jamais stocker le mot de passe en lui-même mais plutôt son empreinte non réversible.
De nombreuses fonctions existent pour calculer l'empreinte d'un mot de passe. Citons les deux plus connues : MD5 et SHA-1.
Les propriétés de base des fonctions de hachage sont simples : une chaîne binaire en entrée, peu importe ce qu'elle représente mais admettons que ce soit 8 caractères ASCII, produira une chaîne binaire en sortie complètement différente, de taille fixe (128 bits pour MD5, 160 pour SHA-1) et dont la seule connaissance ne donne aucune information sur la chaîne utilisée en entrée.
Ajoutons à cela que la modification d'un seul bit dans la chaîne d'entrée implique que l'empreinte de sortie sera au moins à 50% différente de l'empreinte initiale et nous obtenons une méthode de stockage sûre est – relativement - simple.
A cela, nous pouvons coupler plusieurs techniques d'identification. Un standard du web est la norme RFC 2617 qui décrit une méthode sûre d'identification utilisant les fonctions de hachage : www-authenticate.

Lors de la transmission de mots de passe sur le réseau autrement que par une méthode comme www-authenticate, il existe plusieurs outils cryptographiques très utiles :

- La cryptographie asymétrique, avec RSA comme fer de lance, nous permet d'utiliser deux nombres, spécifiquement générés, comme clés de cryptage et décryptage pour échanger des informations entre deux hôtes sans qu'un troisième qui écoute ne puisse déchiffrer le message (sous réserve d'utilisation de clé suffisamment « fortes », comprendre grande en terme de taille).
- La cryptographie symétrique, dont le standard international est AES, utilise une seule clé pour crypter et décrypter les messages. Cette clé doit donc être partagée entre les hôtes préalablement. La cryptographie symétrique à l'avantage d'être beaucoup plus rapide d'exécution que sa consoeur asymétrique, ce qui lui confère un avantage certain lors de chiffrement de flux importants (mais n'est pas très important dans le cas d'un simple mot de passe).
- Kerberos est un protocole qui utilise l'ensemble de ces technologies pour fournir un système puissant d'authentification. Kerberos permet de délivrer des tickets à des utilisateurs sur un réseau, tickets qui sont ensuite utilisés pour accéder à des services aussi divers que variés.

Sinon, Last but not Least, la technique du rené est également très éprouvée et bien pratique bien que souffrant de quelques lacunes sécuritaires. Très utilisées dans les PME, la technique du rené est très simple : vous prenez le nom d'un utilisateur, admettons que ce soit « rené », et vous rajoutez le numéro du département à la fin, admettons que l'on soit en Indre-et-Loire (région bien connue pour son vin et sa qualité de vie mais ceci n'a aucun rapport avec le sujet qui nous intéresse) donc 37 et vous obtenez le mot de passe « rené37 ».
Étendue à l'ensemble de l'entreprise, vous avez ainsi la possibilité de vous passer complètement de politique de mot de passe, ce qui est tout de même très pratique car les mots de passes c'est quand même un peu casse pied....
Par contre, il convient de décliner toute forme de responsabilité quand à l'utilisation de la méthode du rené.

Réalisation technique

« La réalisation démarre, vous devez choisir un outil technologique principal :

- Déterminez les 5 critères de choix les plus importants

- Pour les 3 outils suivants : Microsoft SharePoint, Spip, OpenGroupware et deux autres outils que vous déterminerez, effectuez une notation sur 10 selon ces 5 critères, suivi d'un choix argumenté. »

Critères d'évaluation

Un Intranet peut être facilement comparé à un marché de la connaissance en cela que chacun y apporte et y prend ce qui l'intéresse, le partage étant une monnaie d'échange. Chacun doit pouvoir proposer et disposer de l'information facilement et rapidement, ce qui nous permet déjà d'établir un certain nombre de critères.

L'information est présente en grand nombre dans un Intranet, il faut disposer d'un outil de management de cette connaissance comme, par exemple, une méthode d'évaluation des articles.

Les aspects techniques sont également importants afin de s'assurer que cette connaissance sera accessible dans le temps. Il est indispensable de mettre en adéquation les aspects techniques avec les compétences de l'entreprise et ses besoins.

De fait, la notation suivante me paraît appropriée :

1. **Niveau de collaboration**

   Les outils d'Intranet peuvent être divisé en 3 catégories dépendant de leurs niveaux de collaboration : les outils de communication (1 à 4), les outils de conférences (5 à 7) et les outils de coordination (8 à 10).

2. **Ergonomie**

   Le temps de prise en main d'un outil pour l'utilisateur quotidien est un déterminant de la réussite d'un projet Intranet.

3. **Technologie web**

   Les techniques de diffusion de contenu sur le web évoluent rapidement. La pérennité d'une solution dépend en grande partie du choix des technologie utilisées.

4. **Sécurité**

   La protection du contenu et des utilisateurs est évaluée dans cette partie.

5. **Scalabilité**

   C'est la capacité d'un outil à monter en charge, que ce soit en termes de quantité de contenu qu'en termes d'accueil des utilisateurs.

Evaluation des solutions

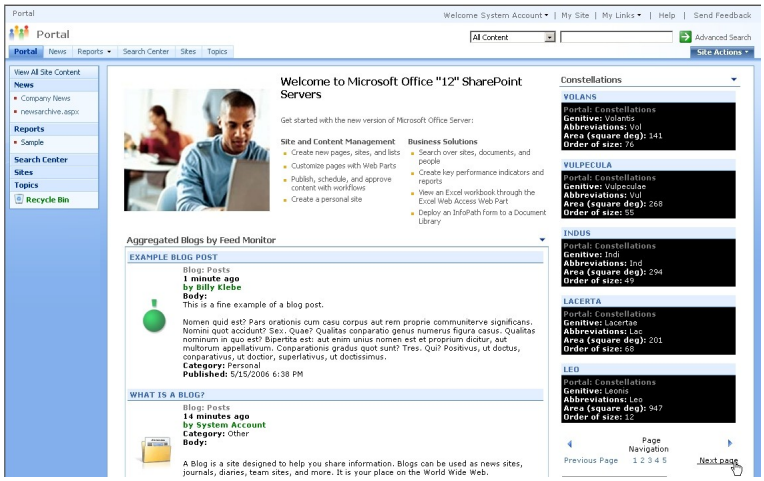
Les 5 solutions logicielles suivantes sont évaluées : Microsoft Office SharePoint Server 2007, Spip, OpenGroupware, Xwiki et Joomla.

Microsoft Office SharePoint Server 2007

C'est un composant optionnel du système Windows Server destiné à agréger et organiser l'information d'une organisation en un point central, ce qui est typiquement ce que l'on demande à un Intranet.

Le front-end de l'application utilise le langage ASP.NET via IIS (Internet Information Services, le serveur web de Microsoft) et stocke les données dans une base de données SQL Server. Ce qui fait en même temps la force et le point faible de cette solution.

La force car Microsoft possède une forte expérience en intégration de solutions, en particulier autour de son système Active Directory. La solution SharePoint n'échappe pas à la règle et fournit un système intégré efficace et relativement robuste (pour une organisation de taille moyenne).



Mais c'est également une faiblesse car Microsoft est tristement célèbre pour ses problèmes de migrations de versions, de stockage de données en formats fermés et de failles systèmes non corrigées.

Spip

Spip, Système de publication participatif (*ou partagé, pas moyen de savoir à quoi correspond ce fichu « p »*), est un logiciel libre créé pour permettre la publication et la gestion de contenu sur un site web. Il permet à un groupe de rédacteur de mettre en ligne très simplement des articles et aux administrateurs de gérer le stockage et la mise en page de ces articles tout aussi simplement.

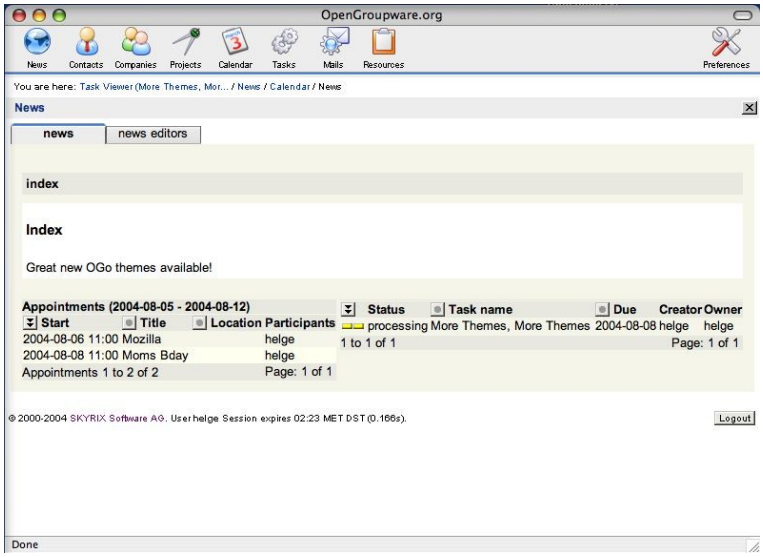
La technologie utilisée est entièrement libre : PHP, pour le langage de programmation, et MySQL pour le stockage des données. Cela apporte un intérêt tout particulier en terme de pérennité de l'infrastructure et de sécurité des logiciels (*un code libre est audité et donc - par définition - plus sûr*), mais pose aussi le problème de la scalabilité de la base de données MySQL. Cette dernière à, en effet, une fâcheuse tendance à ne pas bien tenir de fortes charges.

L'ergonomie du système d'administration de SPIP est des plus épuré, possédant uniquement les fonctions essentielles pour la publication de contenu. On ne peux pas ici évaluer l'ergonomie du front-end car elle dépend du travail du webmaster et de son amour pour le CSS.

OpenGroupware

OpenGroupware n'est pas, à proprement parler, un logiciel de diffusion de contenu comme le sont les deux précédents. Il est plutôt destiné au travail collaboratif, ce qui est un cran au dessus. Mais, comme le dit le vieil adage, qui peut le plus peut le moins, et OpenGroupware n'échappe pas à la règle.

Ce logiciel est écris en Objective-C (*langage compilé plus rapide que le PHP qui est interprété*) et utilise PostGreSQL, comme base de données, et Apache, comme serveur web. PostGreSQL est plus fiable que MySQL en termes de scalabilité et propose également des fonctionnalités d'administration qui font de lui le concurrent libre d'Oracle et SQL Server.



Le code de OpenGroupware est GPL/LGPL et confère donc les avantages cités pour SPIP.

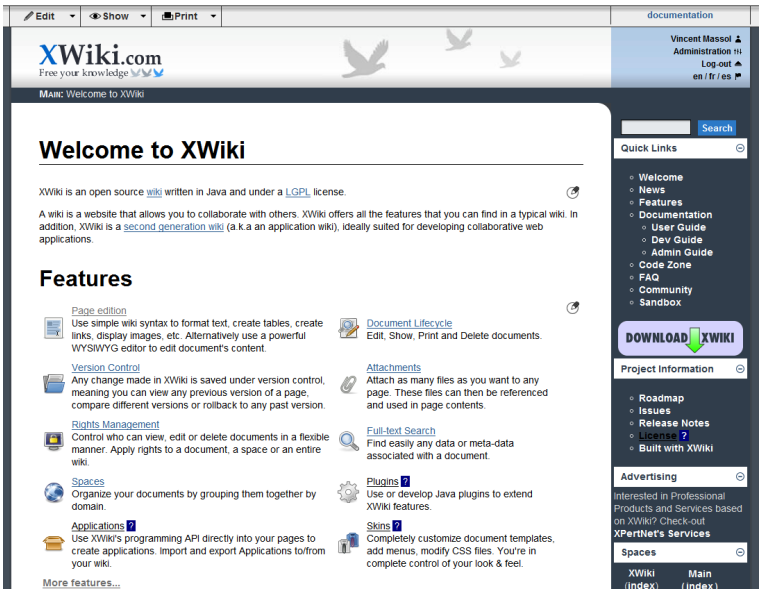
L'avantage d'un logiciel de groupware sur ceux de diffusion de contenu est que le site devient un passage obligé de tous les utilisateurs, l'information étant alors lu par un plus grand nombre d'utilisateurs.

L'inconvénient est en parallèle direct avec ce fait, car l'ergonomie et la lisibilité souffrent de cet « étalage » de fonctionnalités.

Un deuxième inconvénient est l'utilisation du langage Objective-C, qui, bien que libre, est peu connu des développeurs.

Xwiki

Xwiki est un logiciel qui permet, comme son nom l'indique, de mettre en place un Wiki sur un serveur web. Ce logiciel est écrit en Java et diffusé sous licence LGPL. Il doit donc être utilisé avec Tomcat et Apache pour la partie web, et MySQL ou PostGreSQL pour le stockage des données.

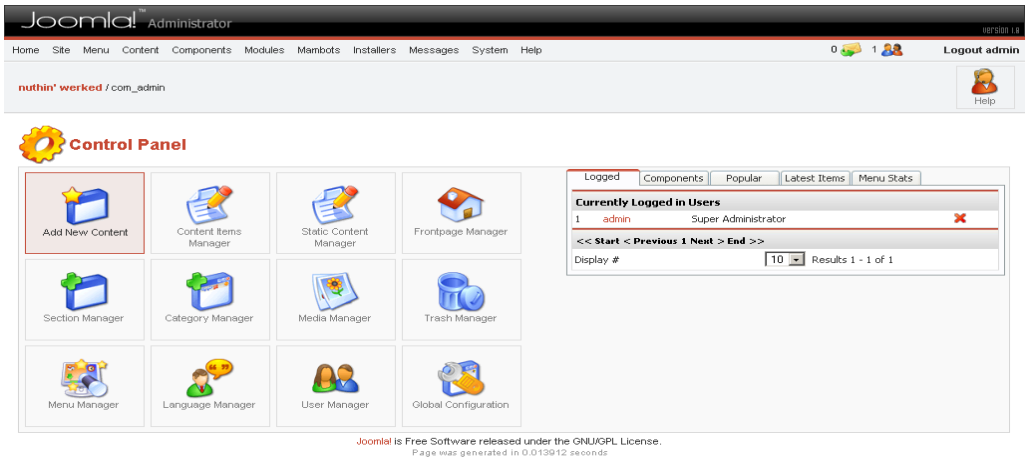


Xwiki est un outil puissant de gestion de contenu. Il gère le versionning des documents, dispose d'une gestion des droits très précise et de nombreuses fonctionnalités d'administration. Son interface est simple et, en dépit de l'utilisation d'une syntaxe d'édition spécifique, assez intuitive.

Le défaut de Xwiki réside dans l'utilisation du langage Java. Ce dernier est puissant mais lent et complexe, rendant difficile la modification du système ou l'administration du serveur.

Joomla

Joomla est un logiciel libre de publication de contenu écrit en PHP et stockant ses données dans une base MySQL. Il est similaire à SPIP en de nombreux points mais se distingue par l'étonnante ergonomie de son interface d'administration. Cette dernière permet une gestion très précise du contenu et des utilisateurs et propose également un certain nombre de statistiques.



Outre les faiblesses inhérentes à l'utilisation de MySQL, Joomla souffre d'un nombre important de failles de sécurité qui, bien que corrigée pour la plupart, laissent planer un doute sur la propreté du code.

De plus, l'interface WYSIWYG de rédaction des articles souffrent de quelques dysfonctionnement mineurs, plus irritants qu'autre chose mais pouvant décourager rapidement un rédacteur néophyte.

Notations *(sur 10)*

	Niveau de collabo-ration	Ergonomie	Technologie web	Sécurité	Scalabilité	**NOTE** (sur 10)
Microsoft Office SharePoint Server 2007	5	7	3	4	4	**4,6**
Spip	4	5	8	6	5	**5,6**
Open Groupware	8	3	5	7	8	**6,2**
Xwiki	4	5	4	7	4	**4,8**
Joomla	4	6	6	5	7	**5,8**

Conclusion

Évidemment, ce tableau ne prend en compte qu'un nombre limité d'aspects techniques et ne considère absolument pas le facteur le plus important : le contexte.

Mais nous pouvons toutefois conclure que OpenGroupware est un excellent outil pour qui en as le besoin, mais sera certainement trop lourd pour la plupart des organisations.

En revanche, Spip et Joomla sortent leurs épingles du jeu pour la gestion de rédacteurs et d'articles.

Xwiki sera certainement un très bon outil de gestion de documentations, mais il faudra lui opposer MediaWiki (*l'outil de Wikipedia*) et Dokuwiki (*un outil léger qui stocke les documents dans des fichiers textes*).

SharePoint sera, en dernier choix, un outil certainement très performant pour qui possède une infrastructure 100% Microsoft (*sisi, yen a plein !*). Pour les autres, il ne sera pas recommandé (*le premier qui dit « ça pu cay pas libre » a perdu !*)