



Gestion des Identités

Une Politique pour le Système d'Information



Table des matières

Légende	5
1. Introduction	7
1.1. Où positionner le curseur de la sécurité ?	9
1.2. La fiche d'identité.	12
1.3. Rationaliser.	14
1.4. Innover.	16
2. La fiche d'identité	19
2.1. La fiche au centre des fonctions de sécurité.	20
2.2. Que contient-elle ?	24
2.3. Une notion logique.	48
2.4. Conclusion.	50
3. Rationaliser	53
3.1. Au commencement... tout était simple !	54
3.2. L'annuaire d'entreprise ou la genèse de la gestion des identités.	56
3.3. L'Identifiant Unique Personnel.	63
3.4. Aux frontières du virtuel ou comment faire face à la réalité.	72
3.5. La synchronisation. Gardez le contact avec vos identités.	77
3.6. Le provisioning ou le retour de l'humain.	86
3.7. Le SSO par délégation. Ne retenez rien, on s'occupe de tout !	96
3.8. Le SSO par domaine de confiance.	103
3.9. Les limites du tout sécuritaire. Des solutions adaptées.	110
3.10. L'analyse des logs.	137
3.11. Travailler ensemble. Un premier pas vers l'innovation.	142
3.12. Le CCI Sécurité : enfin des solutions !	151
3.13. La « Big Picture ». Prenez de la hauteur sur la gestion des identités.	155
4. Innover	159
4.1. L'entreprise étendue.	161
4.2. La confiance implicite d'entreprise.	165
4.3. La confiance explicite d'individu.	174
4.4. Des solutions simples pour innover ?	194
5. Conclusion	197
Index	201
Crédits	209
A propos d'OCTO Technology	213
Bibliographie OCTO Technology	214

1. Introduction

Explorer le sujet de la gestion des identités, c'est d'abord s'interroger sur les relations des personnes, en chair et en os, au Système d'Information.

D'une part, les personnes peuvent être des **objets de gestion** pour certaines applications : par exemple une application de Ressources Humaines gère les salariés de l'entreprise. Mais la notion d'individu est omniprésente dans le Système d'Information sous la forme des **utilisateurs** des ressources informatiques de l'entreprise : cette même application de RH utilise les données de la personne pour authentifier, autoriser un accès partiel ou total, tracer les actions des utilisateurs, envoyer des messages scellés voire confidentiels...

Comment fournir aux **utilisateurs** l'accès aux ressources du SI qui leur est nécessaire pour accomplir leur travail dans l'entreprise ?

Cette problématique existe depuis les débuts de l'informatique : rien de bien neuf donc ! Alors, pourquoi en 2007 le sujet est-il toujours sous les feux de l'actualité, tandis que d'autres sujets qui avaient passionné la communauté informatique sont aujourd'hui tombés dans la commodité (réseaux, firewall, anti-virus...) ? Tout simplement parce que l'on a changé d'échelle dans la complexité. Quasiment toutes les personnes de l'entreprise sont maintenant concernées par l'outil informatique (ce qui n'était pas vrai il y a 10 ans), et de nouvelles populations utilisatrices apparaissent (partenaires, clients...). Parallèlement, les applications de plus en plus nombreuses et hétérogènes, couvrent un spectre de fonctionnalités de plus en plus large.

1.1. Où positionner le curseur de la sécurité ?

Plusieurs générations d'informaticiens ont déjà répondu à cette question de l'accès des utilisateurs, le plus souvent vaguement posée par un : « bon, je ne veux pas que tout le monde puisse toucher à tout, on est bien d'accord ». Malheureusement, dans la plupart des Systèmes d'Information de Gestion (SIG), **la réponse à une exigence vague – c'est-à-dire sans test de recette précis – est toujours une solution complexe, de type « ceinture et bretelles »**. Cette solution à l'accès « sécurisé » des utilisateurs s'est donc conformée à **un trait caractéristique et récurrent, la maxime *Tout ce qui n'est pas expressément autorisé est interdit***. C'est-à-dire un postulat selon lequel tout est « sensible », tout doit être contrôlé *a priori* : si tu n'as pas les droits, tu n'y accèdes pas.

Or cette forme de solution, plaquée et replaquée dans le temps et l'espace du SIG, s'avère excessivement coûteuse à construire, maintenir et administrer. Les coûts directs de la sécurité sont connus : salaire du Responsable de la Sécurité des Systèmes d'Information (RSSI) et des administrateurs, logiciels anti-virus, matériels firewalls, etc. Mais le vrai comptable analytique de la DSI y additionnerait **les coûts induits indirectement par le développement des solutions de sécurité dans les applications**, c'est-à-dire la charge supplémentaire de construction, de maintenance, de tests et d'administration, **notamment due à la gestion des habilitations**. Sans pour l'instant analyser le risque d'utiliser des applications quasiment vierges de fonctions d'habilitation, nous pouvons affirmer au travers de nos observations empiriques que ces applications sans « contrôle d'accès » coûteraient environ 20% à 40% moins cher à la DSI.

Alors pourquoi en est-on arrivé là ? Aurait-on pu répondre différemment à la question initiale ? Par exemple en imaginant **la solution la plus simple qui puisse garantir le confinement de tel ou tel risque** : quel est le risque de n'être pas conforme à cette réglementation sur la protection des données privées ? Quel est le risque que tel acteur de l'entreprise consulte cette donnée qui ne le concerne pourtant pas ? Qu'il la modifie sans que je puisse le savoir ? Qu'il la modifie en sachant qu'on le saura ?

Une telle **analyse du risque** nous amène dans de très nombreux cas à pouvoir aligner la sécurité de l'entreprise sur **un paradigme renversé du précédent : *Tout ce qui n'est pas expressément interdit est autorisé (mais filmé)***.

Etrange ? Inapplicable ? Allons mon bon, vous n'y pensez pas ! Et pourtant, si l'on y réfléchit à deux fois, cette politique s'avère adaptée à la plupart

des environnements, y compris ceux gérant de la donnée personnelle confidentielle : banques, opérateurs télécom, et même administrations. Elle est par ailleurs compatible avec les exigences des principaux régulateurs (HIPAA¹, Sarbanes-Oxley..). Enfin, il faut souligner que ce paradigme agit dans le sens du décloisonnement des structures, tendance lourde de nos organisations : l'apparition des centres d'appel ou du canal Internet a, par exemple, explosé les barrières de sécurité qui cloisonnaient jusque là les outils de gestion par agence ou par région, excluant l'idée d'une vision nationale, ou d'un accès aux outils de vente ET aux outils de gestion.

La menace responsabilisante « utilisez, vous êtes filmés », couplée à des interdictions ciblées permet de se prémunir de la majorité des risques de sécurité du SI. En particulier, ce modèle est le seul qui permette de répondre à la question « vous êtes sûr que ces gens-là ne peuvent pas voir cette information-là j'espère ? ». A l'inverse, en mode *Tout ce qui n'est pas expressément autorisé est interdit*, après avoir posé des milliers d'habilitations du type « tel groupe tel droit, telle personne tel droit ... », impossible de répondre sereinement à cette question... Etes-vous bien sûr qu'au milieu de vos attributions de droits ne traîne pas un privilège incorrect ?

Le paradigme *Tout ce qui n'est pas expressément interdit est autorisé (mais filmé)* s'inspire de la réalité de nos entreprises. Lisez le règlement intérieur, qu'exprime-t-il ? La liste exhaustive de ce qui est autorisé ou plutôt la jurisprudence des interdictions posées progressivement au fil des dépassements de limites implicites ? Dès que des actes sur le SI relèvent d'une interdiction implicite, l'entreprise sait qu'il faudrait désormais la matérialiser par écrit pour que d'autres ne fassent pas la même erreur².

Au départ, les traces sont simplement stockées, l'idée est de faire peur. Puis au fil des histoires d'abus (on en a toujours, même avec le système apparemment le plus blindé³ !!), on va capitaliser dans l'analyseur de traces les formes que laissent ces abus. Par exemple détecter des modifications non groupées sur la donnée *salaire*, i.e. un individu qui augmente un salaire à 20h, alors que la DRH gère plutôt de telles mises à jour par bloc de salariés en heures ouvrées... Ce phénomène de **capitalisation progressive des interdictions s'oppose donc à la définition massive de droits a priori.**

Au final, **comme le système d'habilitation qui capitalise progressivement les interdictions, le système d'audit capitalise, lui, les formes que prennent les abus dans les traces.**

¹ Health Insurance Portability and Accountability Act

² Je vous laisse deviner pourquoi les horaires font partie de la plupart des règlements intérieurs

³ Droit ouvert abusivement ou par erreur, abus du système avec ses propres droits ...

Une politique de sécurité doit donc se caler sur un risque avéré, c'est-à-dire sur une histoire de fraude qui pourrait avoir lieu avec une probabilité non nulle. Le risque 0 n'existe pas. Il restera toujours des histoires contre lesquelles le SI ne pourra se prémunir, par exemple celle de l'administrateur qui fraude en utilisant ses privilèges d'accès par les couches basses, comme la modification directe d'une table de données sans passer par l'application.

Ce constat milite pour une nécessaire homogénéité de la politique : inutile de dresser de coûteuses barricades d'habilitations dans les applications s'il existe des chemins de traverse dans les couches inférieures de l'architecture. On est toujours attaqué sur son côté le plus faible.

Positionner le curseur de la sécurité, c'est donc répondre à un risque identifié, c'est-à-dire envisager les *histoires d'abus*, et investir de manière homogène dans les différentes couches de l'architecture pour s'en prémunir. Paradoxalement, la stratégie « tout blinder » s'inscrit souvent à rebours de cette démarche, en générant beaucoup de complexité superflue. **Or la sécurité d'un système, c'est avant tout sa simplicité.**

1.2. La fiche d'identité

Quelle que soit la position du curseur de la sécurité dans votre Système d'Information, **la personne et ses attributs en sont la pierre angulaire.**

Au cours de la vie d'une personne dans une entreprise, beaucoup d'événements (arrivée, mutation, déménagement, promotion, départ...) vont influencer les attributs qui lui sont liés, à la fois en tant qu'**objet de gestion** et en tant qu'**utilisateur**.

Nous utiliserons le terme « **fiche d'identité** » pour décrire l'ensemble des attributs d'un individu : **données intrinsèques à la personne** (état civil, photo...), **données liées à son métier** (rôle, savoir-faire, statut, niveau d'accréditation...), **données de localisation** (adresse, pays, site, bureau...), **données de contact** (mail, téléphone, pager...), **données d'organisation** (département, rattachement hiérarchique, secrétariat...), et enfin **informations dédiées à la sécurité** (mots de passe, certificat...).

La fiche d'identité est une notion logique, les données qui la constituent sont toujours réparties sur différents référentiels dans différentes applications : les référentiels de sécurité, mais aussi les gestionnaires de ressources humaines, les outils de la direction de la communication, des moyens généraux, etc. Pourtant cette vue logique, et à jour, est nécessaire pour rendre les **cinq grands services de sécurité liés à la personne : authentifier, habilitier, imputer & auditer, signer et crypter.**

Mais c'est encore le service *habilitier* qui exploite la plupart de ces données. La créativité des informaticiens dans l'espace de *Tout ce qui n'est pas expressément autorisé est interdit* conduit naturellement à des restrictions par entité organisationnelle ou géographique, par rôle métier, par niveau d'accréditation et tant d'autres. Les quatre autres fonctions que sont l'authentification, la trace, la signature et le chiffrement, n'exploitent finalement qu'un identifiant (matricule, pseudo...) et des codes secrets (mot de passe, clé de chiffrement privée).

Un **référentiel de sécurité d'entreprise** permettant de garantir quatre services de sécurité parmi cinq peut donc être simplement **composé de deux données** : un identifiant et des codes secrets. L'identifiant stable de la personne peut ensuite être utilisé comme **clé de jointure** pour déduire d'autres informations sur la personne, informations qui peuvent être gérées dans d'autres référentiels.

Mais alors, **pourquoi nos annuaires d'entreprise ressemblent-ils plus à un CRM des employés qu'à une table à deux colonnes ?**

En plus du problème de curseur de la sécurité sur les habilitations, qui a conduit à propager dans le SI tout un tas de données supplémentaires, la complexité des systèmes d'annuaire relève en fait de problèmes de *vivre ensemble*. Lorsque le *qui gère quoi*, le *qui fait quoi* n'ont pas été discutés, lorsqu'il est difficile de réaliser un projet entre deux Directions de l'entreprise, l'architecture du SI reflète ces dysfonctionnements de l'organisation avec des systèmes balkanisés et redondants.

Ainsi les différentes données de la fiche d'identité se retrouvent gérées dans plusieurs référentiels en recouvrement les uns par rapport aux autres. Qui est maître sur quelle donnée, sur quel périmètre, pendant combien de temps ? Comme il est probable que chaque Direction⁴ possède durablement son propre SI dans lesquels vivent des personnes, à la fois comme utilisateurs et comme objets de gestion, et ce à différents niveaux dans les grandes structures, **la mise en cohérence d'une fiche d'identité relève plus d'un problème de gouvernance à inventer que de technologies**. Celles-ci sont prêtes : en particulier les outils de synchronisation des données et les outils permettant de créer des processus transverses de mise à jour de la fiche (*provisioning*). Mais vous, êtes-vous prêts ?

⁴ Ressources humaines, communication, sécurité informatique, moyens généraux...

1.3. Rationaliser

Dans les grandes entreprises, les programmes responsables de fournir les cinq services de sécurité (*authentifier, habilitier, imputer & auditer, signer et crypter*) existent sous la forme d'une immense fractale dans laquelle sont reproduites les mêmes formes de données et de traitements. Chaque Direction a créé son silo d'applications embarquant avec lui ses fonctions de sécurité. Le travail de rationalisation de la DSI consiste à resserrer les liens de cette fractale, voire à supprimer certaines branches pour les mutualiser, syndrome nostalgique d'un temps du mainframe où tout était plus simple : un annuaire, un traitement de sécurité (RACF, Top Secret)...

Cette nécessaire **rationalisation de la sécurité est tirée par des arguments de risques, de contraintes réglementaires et bien entendu de coûts**. Le plus souvent dans cet ordre.

Ce qui était traité au cas par cas dans chaque silo applicatif doit maintenant être **pensé au niveau global du SI, avec pour objectif de générer une diminution des risques, de proposer de nouveaux services et de coûter moins cher**. Comme nous le précisons dans Une Politique pour le Système d'Information (2006⁵), pour créer de l'actif dans le SI, c'est-à-dire du « personnel numérique » utile pour le métier, nous pouvons nous attacher majoritairement à **diminuer le passif**, c'est-à-dire à diminuer les dettes techniques⁶ que nous ont cédées les générations passées. Nous employons trois moyens dans ce sens : la **simplification** - par la fusion de systèmes dans des systèmes plus massifs, la **généralisation** - par le partage de formes de programmes et de données (de *patterns*), et le **maintien de la maintenabilité** par la couverture de tests de ces programmes.

A ce jour, les maigres **tentatives autour de l'annuaire d'entreprise se sont révélées des réponses insuffisantes** face à la globalité du problème. Victimes de manque de qualité de la donnée, et surtout de manque **d'attractivité** des solutions de sécurité pour les applications, les résultats attendus en termes de diminution de l'insécurité, de nouvelles fonctionnalités et de diminution des coûts n'ont pas été au rendez-vous dans la plupart des cas.

Les solutions que nous vous proposons de découvrir tenteront d'explorer ces trois axes : **centraliser des fonctions de sécurité simples et robustes, aux formes attractives pour les nouvelles applications comme pour l'existant, et couvertes de tests**, garantissant à tous les clients une maintenabilité exemplaire.

⁵ Disponible dans les librairies spécialisées en informatique (Amazon, Fnac, Le Monde en Tique etc.)

⁶ Terme désignant les phénomènes de non qualité conduisant à reporter des problèmes de productivité dans le futur : code et données redondants, code stratifié/en verrues, code inutile ...

Ces solutions permettront de resserrer les liens de la fractale pour *Construire* une identité fiable sur laquelle greffer des services de sécurité d'une part, et inciter les applications du SI à les *Utiliser* en proposant des formes, voire des composants de sécurité sur étagères, d'autre part.

1.4. Innover

Si la **rationalisation** est un mouvement majeur et permanent de l'entreprise, l'**innovation** en est un second. Ces trente dernières années ont vu croître le nombre de relations électroniques entre entreprises. Des premiers EDI⁷ entre participants d'une chaîne de production étendue, aux extranets inter-entreprises de service d'aujourd'hui, les informaticiens ont régulièrement dû solutionner le problème de l'interconnexion sécurisée de SI. Et là **miracle, ce sont plutôt les solutions les plus simples qui l'ont emporté**. Ces solutions s'appuient sur une forme commune que l'on pourrait qualifier de *confiance implicite d'entreprise*. C'est-à-dire qu'un lien EDI ne nécessite que l'identité des deux entreprises en tant que *personne morale*, et non celle de chaque *personne physique* employée. On établit ainsi un canal sécurisé où les messages sont considérés comme implicitement conforme à la volonté de la personne morale, quelle que soit la personne physique à la source. De même, le poste de travail du conseiller bancaire qui accède en extranet à un site dédié du partenaire assureur de la banque : le canal Web est sécurisé entre la banque et l'assureur (via un VPN par exemple), tandis que les personnes physiques utilisatrices sont implicitement reconnues comme habilitées et responsables. Des informations comme l'identifiant utilisateur peuvent circuler sur ce lien et revenir en boucle de données dans les états que l'assureur produit vers la banque (un tel a vendu une assurance à tel client ..), et ainsi permettre une traçabilité forte.

Dans les relations inter-entreprises, c'est donc souvent le modèle *Tout ce qui n'est pas expressément interdit est autorisé (mais filmé)* qui a été appliqué.

Pourtant, de **nouveaux standards technologiques plus complexes** que ces solutions pointent leur museau, en particulier les modèles **Web Service Security** et **Liberty Alliance**. Les gens étant plutôt satisfaits de leurs solutions existantes, quelle est la limite qu'ils permettraient de franchir ? Quelle douleur viendraient-ils soulager ?

Ces standards sont plus complexes que l'existant en ce sens qu'ils s'alignent sur un paradigme *confiance explicite d'individu* : d'annuaires à N entreprises, on passe à des bases de N *milliers* d'utilisateurs... Chacun avec sa spécificité, leur utilisation sera donc forcément plus coûteuse, si l'on y inclut la mise en place, la gestion courante et la maintenance.

Côté Web Service, l'inclusion de fonctions de sécurité dans cette couche du protocole vient doubler celles des couches inférieures, en particulier HTTP,

⁷ Echanges de Données Informatisés : premiers systèmes de commande/livraison électroniques inter-entreprises

le protocole du Web⁸. Pourquoi refaire ce qui est déjà bien fait en dessous ? Pour s'abstraire des couches d'en dessous ! Les Web Services visent le **mythe du protocole unifié**, valable pour un petit appel synchrone en HTTP, comme pour l'échange asynchrone de messages, comme pour le transport de grosses masses de données à heure fixe ... **Dans la rubrique des *Standards dont vous pouvez vous passer avant 2010-2015*, vous trouverez donc WS-Security.**

Entre entreprises et administrations, il existe quelques cas métier où **Liberty Alliance** peut présenter un intérêt, en particulier **s'il existe de réelles relations multi-latérales entre nombreux acteurs**, ce qui est très rare, le bilatéralisme restant la règle (notre assureur et notre banque par exemple).

Encore et toujours, dans ces choix complexes, **intéressons-nous aux vraies limites ressenties de nos systèmes, celles qui créent une douleur, avant de céder à d'hypothétiques grands soirs de l'interopérabilité...**

Pierre Pezziardi
Février 2007

⁸ Vous vous êtes déjà authentifié sur un site, vous avez déjà été interdit d'accès à un site, vous avez déjà crypté votre échange en SSL n'est-ce pas ?

3. Rationaliser

3.13. La « Big Picture ». Prenez de la hauteur sur la gestion des identités

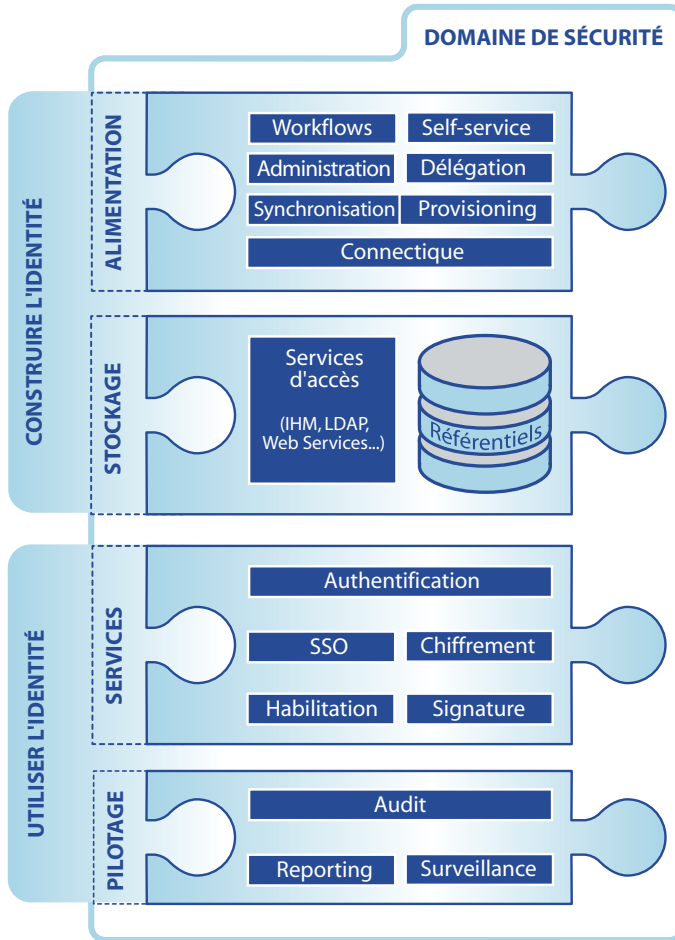
Des *patterns*, des *patterns* et encore des *patterns* ! Le SI en regorge et les architectes en demandent pour les orienter sur les routes sinueuses de la rationalisation. La gestion des identités ne fait pas défaut à la règle : que serait devenue la sécurité chez Pif et Jo Sport sans ces fameux *patterns* ? Très probablement quelque chose de générique, ressemblant à un discours convenu et surtout sécuritaire, alimentant la bourse des éditeurs et le ressentiment des utilisateurs. Car il ne faut pas les oublier ces utilisateurs ! Ils sont, dans le domaine de la gestion des identités, une pièce maîtresse de l'échiquier, tout à la fois utilisateurs de services de sécurité (authentification, signature, etc.) et fournisseurs de données pour les créateurs et les gérants de leur fiche d'identité.

L'identity management, ce n'est ni plus ni moins que cela : construire l'identité pour pouvoir ensuite l'utiliser.

Fonctionnellement, la « Big Picture » de la gestion des identités dans un SI ressemble donc à ça : la superposition de deux socles de référence, « construire » et « utiliser », eux-mêmes subdivisés en deux briques d'assemblage :

- Construire la fiche d'identité c'est d'abord être capable d'en **stocker les données**. Historiquement le stockage a d'ailleurs été la première brique fonctionnelle fournie par les SI au sein de référentiels techniques aussi variés que des bases de données, des annuaires ou des PABX !
- Construire la fiche d'identité c'est ensuite **assurer le cycle de vie** de ses données : de sa création à sa suppression pure et simple, les modifications apportées à la fiche d'identité sont à l'image des changements vécus par l'utilisateur dans l'entreprise : arrivée, mutations, promotions hiérarchiques, etc. Les conséquences de ces événements, comme par exemple l'appartenance à de nouveaux rôles métier, se retrouvent matérialisés dans une fiche d'identité dont la cohérence est assurée par de nombreux services : synchronisation, *provisioning*, *self-service*, etc. ;
- Utiliser l'identité, c'est faire appel à tous **les services assurant la sécurité des utilisateurs**, des applications et des données du SI : authentification unique, confirmation ou infirmation des accès par habilitations, chiffrement des échanges, etc. Tous ces services utilisent des données contenues dans la fiche d'identité préalablement élaborée par le socle « Construire » ;

- Mais utiliser l'identité c'est aussi être capable de **déceler les histoires d'abus dans les traces des applications**. S'il ne s'agit pas de « cliquer » les utilisateurs du SI, le pilotage permet de mettre en œuvre une politique de sécurité efficace, adaptée aux risques réels et reposant le plus souvent sur une relation de confiance maîtrisée avec les individus.



Au sein de toutes ces briques co-existent des *patterns* (et aussi bien entendu quelques *anti-patterns* !). Leur formalisation et la prise de conscience de leur existence permettent aux architectes de mener une analyse efficace et cohérente, permettant de concevoir des architectures de sécurité adaptées aux risques réellement encourus. Mais si une approche par *patterns* permet de rationaliser la sécurité du SI, elle doit également lui permettre l'innovation, c'est-à-dire l'ouverture à d'autres Systèmes d'Information. Dans cette optique, chaque pièce du puzzle de la « Big Picture » est emboîtable dans un domaine

de sécurité tierce : « Comment gérer des utilisateurs externes à un SI dont les impératifs métier nécessitent pourtant qu'ils s'y connectent ? », « Doit-on vraiment les gérer ou laisser cette tâche à la charge du partenaire ? ». A toutes ces questions, il existe des réponses, ou plutôt des *patterns*, d'innovation cette fois-ci, dans la droite lignée de leurs cousins de la rationalisation. Mais ça, c'est un autre chapitre qui commence !

La Gestion des Identités est devenue un enjeu dans votre entreprise ?
Vous trouverez dans cet ouvrage des clés pour débattre et dégager les solutions les plus adaptées à votre contexte.

UN COMBAT DE TITANS : MÉFIANCE OU CONFIANCE ?

C'est souvent dans les habilitations que s'exprime avec le plus de force l'opposition entre deux approches de la politique de sécurité.

L'approche sécuritaire : « Tout ce qui n'est pas expressément autorisé est interdit ». Le principe est de tout interdire par défaut et d'autoriser certaines actions au fur et à mesure de l'apparition des besoins. Dans cette approche, seules les fonctionnalités indispensables au travail d'une personne lui sont autorisées.

L'approche pilotée par les risques : « Tout ce qui n'est pas expressément interdit est autorisé, mais filmé ». Le principe est de tout autoriser par défaut, sauf un petit nombre de fonctionnalités critiques identifiées via une analyse de risque. En revanche, toute action de la personne est tracée.

DU SUSPENSE

...Automne 2001. A l'approche des fêtes de fin d'année des hordes de nouveaux clients déferlent dans les magasins du groupe. Jo Voyages et Jo Fitness ont profité d'un large effet positif de bouche à oreilles et les deux produits tournent à plein régime. Le succès est d'ailleurs tel que Jo Sport a dû embaucher des saisonniers pour faire face à la demande....

DES QUESTIONS EXISTENTIELLES

...Mais alors, pourquoi nos annuaires d'entreprise ressemblent-ils plus à un CRM des employés qu'à une table à deux colonnes ?

DE L'HUMOUR ... NOIR

Pris en sandwich dans cette organisation, l'utilisateur reste quant à lui seul avec ses questions et ses sautes d'humeur chaque fois qu'apparaît une fenêtre pop-up sur laquelle on peut lire « Access Denied ».

ET TOUJOURS DU POLITIQUEMENT INCORRECT

Les éditeurs font leurs choux gras des prétendues lacunes sécuritaires des Web Services. Pourtant, on peut s'interroger sur le besoin réel d'une sécurité nominative des Web Services : en dehors de cas scolaires loin des réalités du SI, on ne voit pas vraiment les limites des solutions couches basses (authentification HTTP, HTTPS, etc.) que les mécanismes complexes de WS-Security permettraient de franchir.

Cet ouvrage s'adresse aux dirigeants du Système d'Information, aux RSSI, aux architectes, aux chefs de projet et maîtrise d'ouvrage impliqués dans la sécurisation de leurs applications ou de leur SI.



39€ TTC

OCTO Technology, Cabinet d'Architectes en Systèmes d'Information
50, avenue des Champs-Élysées - 75008 Paris
www.octo.com

ISBN : 978-2-9525895-1-2