

Livre blanc

Systemes d'Information :

La gestion des prestataires externes



WALLIX
Infrastructure and Security Solutions

Sommaire

I.	Problématique.....	3
II.	Enjeux spécifiques	3
III.	Quelles sont les solutions existantes ?.....	4
	a) Faible granularité des droits.....	5
	b) Multiplicité des solutions entrainant une administration complexe	5
	c) Reporting inadapté aux exigences réglementaires	5
	d) Divulgarion des mots de passe	6
	e) Traçabilité insuffisante	6
IV.	Spécifications d'une plate-forme d'administration « prestataires »	6
	a) Très forte granularité des droits.....	6
	b) Compatible multi-équipements	6
	c) Outils de reporting intégré.....	6
	d) Non-divulgarion des mots de passe des comptes cibles.....	7
	e) Traçabilité totale des opérations effectuées.....	7
	f) Intégration à l'existant	7
	g) Coût d'installation et d'administration réduit.....	7
	h) Génération d'alertes.....	8
V.	Wallix AdminBastion (WAB) – la plate-forme d'administration orientée prestataires.....	8
	a) Très forte granularité des droits.....	8
	b) Compatible multi-équipements	9
	c) Outils de reporting intégré.....	9
	d) Non-divulgarion des mots de passe des comptes cibles.....	10
	e) Traçabilité totale des opérations effectuées.....	10
	f) Intégration à l'existant	10
	g) Coût d'installation et d'administration réduit.....	11
	h) Génération d'alertes.....	11
VI.	Les apports d'une telle solution	11
	a) Coût d'installation et d'administration réduit.....	11
	b) Diminution des risques.....	12
	c) Conformité par rapport aux normes (« Compliance »).....	12
VII.	Conclusion	13

I. Problématique

Aujourd'hui, les entreprises doivent ouvrir leur système d'information à un nombre toujours plus important de prestataires extérieurs, d'abord pour réduire le budget informatique – ce qui se traduit par le recours à des prestataires externes pour des compétences qui ne font pas partie du cœur de métier de la DSI - ensuite pour gagner en rapidité dans le déploiement de nouvelles solutions. Parmi ces différents types de prestataires figurent par exemple :

- des éditeurs de logiciels métiers devant intervenir sur leurs applicatifs
- des infogérants assurant la gestion de tout ou partie des infrastructures et / ou des applications
- Des « outsourcers » en charge du support technique (exemple : SSII spécialisée dans le support et le tuning Oracle)
- Des consultants spécialisés dans un domaine applicatif spécifique (ex : expert CRM ou ERP)

Ces prestataires sont indispensables au bon fonctionnement du système d'information mais ils ne sont pas salariés de l'entreprise et présentent donc des risques potentiels particulièrement importants pour l'entreprise (fuite d'informations, destruction de données sensibles ...). De plus, sans traçabilité des actions, il devient difficile de connaître les causes et les responsables d'un éventuel dysfonctionnement.

Notons en complément que le personnel IT de l'entreprise doit également pouvoir se connecter à distance – que ce soit en cas d'astreinte ou simplement de déplacement, avec des problématiques de connexion identiques à celles des prestataires externes.

II. Enjeux spécifiques

Un certain nombre d'études récentes confirme les risques inhérents aux privilèges dont disposent les administrateurs IT – que ces administrateurs soient internes ou bien prestataires.

A titre d'illustration on peut notamment citer ⁽¹⁾ :

- 35% des administrateurs IT admettent utiliser leurs privilèges d'administrateurs pour obtenir des informations confidentielles ou sensibles.
- 74% des administrateurs IT se disent capable de contourner les mécanismes actuels de protection des informations confidentielles ou sensibles
- Parmi les informations sensibles auxquelles accèdent les administrateurs figurent notamment par ordre d'importance :
 - Base de données clients
 - Base de données des ressources humaines
 - Plan de fusion/acquisition

¹ Source : 2009 Trust, Security & Passwords Survey Research Brief – étude réalisée par Cyber-Ark Software auprès de 400 professionnels IT

- Informations marketing
- Plan de licenciement

En cas de licenciement, les administrateurs IT quitteraient la société avec les informations suivantes :

Type d'information	2009	2008
Base de données clients	47%	35%
Mot de passe administrateur du serveur de messagerie	47%	13%
Projets de fusion/acquisition	47%	7%
Copie des données R&D	46%	13%
Mot de passe du compte du P-DG	46%	11%
Données financières confidentielles	46%	11%
Liste des mots de passe des comptes à privilège	42%	31%

Il est à noter que la conjoncture économique actuelle accroît de façon très importante les risques de fuite d'informations.

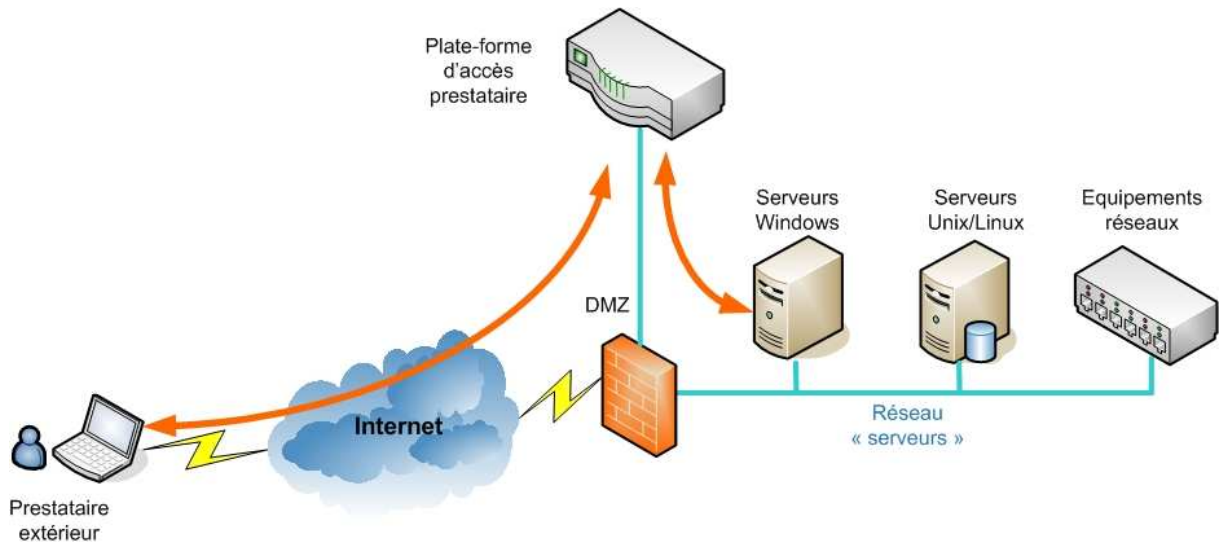
Le recours à des prestataires externes - pour administrer tout ou partie des équipements d'un Système d'Information – démultiplie ces risques en raison :

- du très rapide turn-over existant chez de nombreux prestataires – qui accroît les risques de fuite d'information suite au départ d'un administrateur IT du prestataire
- de la difficulté pour le client de s'assurer de la probité du personnel d'un prestataire – avec un risque démultiplié dans le cas d'un prestataire disposant d'équipes situées dans des pays à faible revenu compte tenu de la valeur marchande des informations accessibles

III. Quelles sont les solutions existantes ?

Différentes solutions existent déjà avec pour objectif de fournir un accès sécurisé à des prestataires externes, telles que par exemple : VPN IPSEC ou SSL, liaisons spécialisées, serveurs de rebond SSH, accès RDP, développement interne ...

Ces solutions s'installent habituellement en DMZ et sont positionnées en relais entre le prestataire extérieur et l'équipement cible.



Toutefois, ces solutions présentent différents inconvénients :

a) Faible granularité des droits

Ces solutions assurent en général un contrôle d'accès autorisant ou non une connexion vers une adresse IP cible représentant un serveur ou un équipement réseau – sans descendre au niveau du compte cible.

Il n'est donc pas possible de pouvoir par exemple autoriser uniquement une connexion sur un ou plusieurs comptes précis mais uniquement d'autoriser l'accès à un équipement sur l'ensemble de ses comptes !

b) Multiplicité des solutions entraînant une administration complexe

Pour chaque type d'équipement existe en général une solution spécifique. Par exemple, des serveurs Unix ou Linux seront accessibles en SSH via un serveur de rebond tandis que des serveurs Windows seront de leur côté accessibles via un serveur Windows TSE – et les personnes en astreinte se connecteront via une solution VPN SSL.

Chacune de ces solutions s'administre de façon spécifique, avec donc au quotidien un coût d'administration élevé en temps et en personnel et donc un risque important d'ouvrir plus que nécessaire les droits d'accès afin d'éviter d'avoir à les modifier trop souvent.

c) Reporting inadapté aux exigences réglementaires

Ces solutions permettent l'accès par des prestataires extérieurs à des systèmes critiques et doivent donc fournir les éléments de reporting permettant de vérifier la conformité de ces accès par rapport aux différentes normes (SOX, Bâle 2 ...).

Or la très grande majorité de ces solutions n'intègrent pas en général d'outils de reporting répondant à ces exigences.

d) Divulgarion des mots de passe

Ces solutions imposent que les prestataires connaissent le mot de passe du compte utilisé sur l'équipement cible, ce qui fait qu'en cas d'utilisation d'un compte système générique (ex : compte « administrateur » sur un serveur Windows ou « root » sur un serveur Unix/Linux), le mot de passe de ce compte devra être transmis au prestataire.

Cette transmission peut constituer une faille de sécurité majeure en raison du fait que les mots de passe des comptes système génériques ne sont que très peu souvent modifiés.

e) Traçabilité insuffisante

Ces solutions fournissent en général un journal des connexions mais ne permettent pas de savoir exactement ce qui a été fait lors d'une connexion. Ainsi, il n'est pas possible de savoir par exemple si un prestataire extérieur a par exemple essayé de rebondir vers un autre serveur.

IV. Spécifications d'une plate-forme d'administration « prestataires »

Compte tenu des déficiences présentées par les solutions actuelles et des retours d'expérience de nombreux clients et prospects, Wallix a établi le cahier des charges d'une plate-forme d'administration optimisée pour l'accès de prestataires extérieurs au système d'information :

a) Très forte granularité des droits

La plate-forme d'administration doit permettre une très grande granularité des droits d'accès avec la possibilité, prestataire par prestataire voire administrateur par administrateur, d'autoriser uniquement l'accès à certains comptes sur un équipement cible donné.

b) Compatible multi-équipements

Afin d'éviter la multiplication des plates-formes d'accès, une même plate-forme d'administration « prestataires » doit permettre l'accès à tout type d'équipement cible, que ce soient des serveurs Windows, des serveurs Unix/Linux, des équipements de stockage ou bien des équipements réseaux.

L'utilisation d'une plate-forme unifiée permet de limiter les coûts d'acquisition mais aussi et surtout de limiter le coût de possession en limitant le temps d'administration nécessaire.

c) Outils de reporting intégré

La plate-forme doit permettre de disposer automatiquement de rapports répondant aux principales exigences réglementaires, telles que par exemple savoir qui a accès à un compte de service critique (ex : compte « root » d'un serveur Unix/Linux ou compte « administrateur » d'un serveur Windows).

d) Non-divulgation des mots de passe des comptes cibles

La solution doit permettre de ne pas avoir à diffuser aux prestataires les mots de passe des comptes critiques.

Cette non-divulgation permet notamment de ne pas avoir à changer tous les mots des comptes cibles en cas de rupture du contrat avec un prestataire ... ou tout simplement du départ, chez le prestataire, de l'une des personnes connaissant les mots de passe !

e) Traçabilité totale des opérations effectuées

La solution doit permettre de savoir exactement ce qui a été effectué par le prestataire lors de sa connexion sur l'équipement cible – et cela quel que soit le type d'équipement.

Cette traçabilité peut d'une part pousser les prestataires externes à faire preuve d'une déontologie exemplaire dans l'exécution de leur mission (la fameuse peur du gendarme !), d'autre part permettre de définir avec certitude et objectivité quelle action et quel intervenant est à l'origine d'un incident. Ce dernier point peut être très intéressant dans le cas d'une infogérance d'une partie du SI, permettant à l'infogéreur comme au client de faciliter la gestion du contrat d'infogérance et la détermination de la responsabilité en cas d'incident (donc l'application ou non des pénalités prévues au contrat).

f) Intégration à l'existant

La solution doit s'intégrer à l'existant, notamment en termes de gestion des utilisateurs. Ainsi, si les prestataires figurent dans un annuaire d'entreprise (ex : LDAP, Active Directory, ...), il faut que la solution puisse les authentifier à partir de cet annuaire.

En complément, la solution doit pouvoir réutiliser l'existant en terme de solutions d'authentification forte orientées prestataires (ex : RSA SecurID ...).

Enfin, la solution doit disposer d'une interface programmatique (ex : API, langage de scripting, ...) permettant de l'interfacer à l'existant (ex : solution d'IAM, solution de helpdesk ...)

g) Coût d'installation et d'administration réduit

La solution doit être facile et rapide à installer mais aussi et surtout ne pas impliquer de changement majeur pour les prestataires – que ce soit en terme technique (pas d'installation de logiciel client spécifique) ou fonctionnel (pas de formation longue du personnel des prestataires).

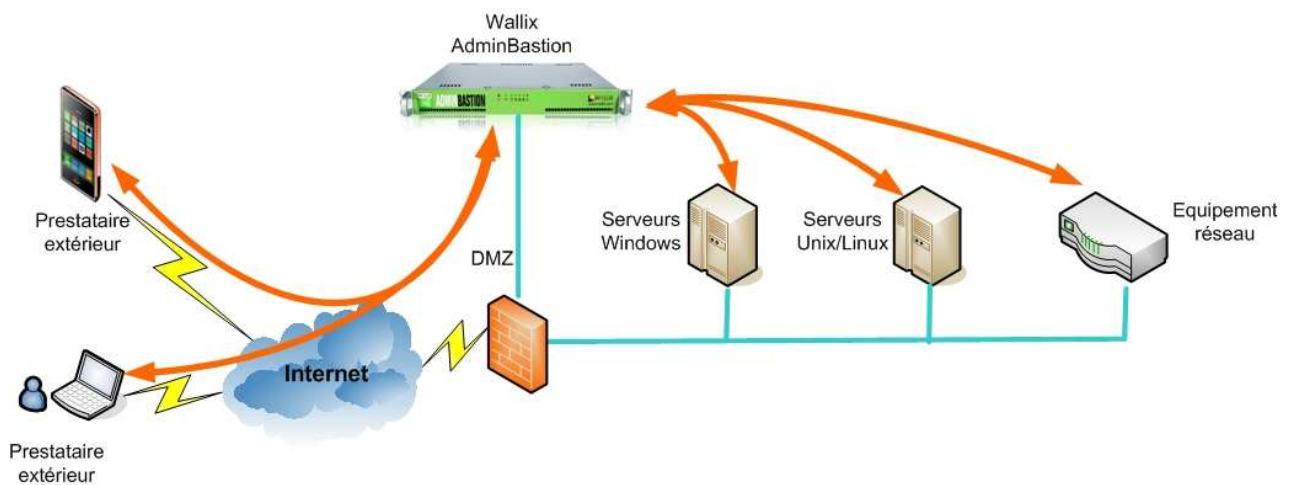
Idéalement, cette solution doit également pouvoir suivre les évolutions actuelles en termes de mobilité et donc pouvoir être utilisable via un smartphone (iPhone, Android, Windows Mobile ...) si nécessaire.

h) Génération d'alertes

Une telle solution devrait être capable d'envoyer (mail, inscription dans un fichier de logs, ...) des alertes à des responsables de la sécurité en cas de connexions – même autorisées – à des serveurs dont le bon fonctionnement est jugé critique pour la société.

V. Wallix AdminBastion (WAB) – la plate-forme d'administration orientée prestataires

Wallix AdminBastion (WAB) est une solution développée par Wallix spécifiquement pour les besoins des entreprises et des collectivités locales souhaitant mettre en place une plate-forme d'administration orientée « prestataires ».



WAB dispose des caractéristiques suivantes :

a) Très forte granularité des droits

WAB définit des droits d'accès non pas au niveau des équipements mais au niveau des comptes cibles. Ainsi, en fonction de son profil, un prestataire externe pourra se connecter à un ensemble de comptes cibles donnés.

Ainsi, sur un même serveur Windows, un prestataire X pourra par exemple être autorisé à utiliser le compte « administrateur » tandis qu'un autre prestataire Y ne sera autorisé à utiliser qu'un compte avec des privilèges bien plus réduits.

La gestion des droits des utilisateurs utilise le concept du contrôle d'accès à base de rôles (RBAC – Role-Based Access Control).

A noter, en complément des droits d'accès, WAB permet également de définir des droits « protocolaires » dans le cas d'une connexion SSH. Ainsi, pour chaque prestataire, en fonction du compte cible, il est possible d'autoriser ou d'interdire :

- l'accès au « Shell »
- l'exécution de commandes distantes
- l'« upload » ou le « download » de fichiers via SCP

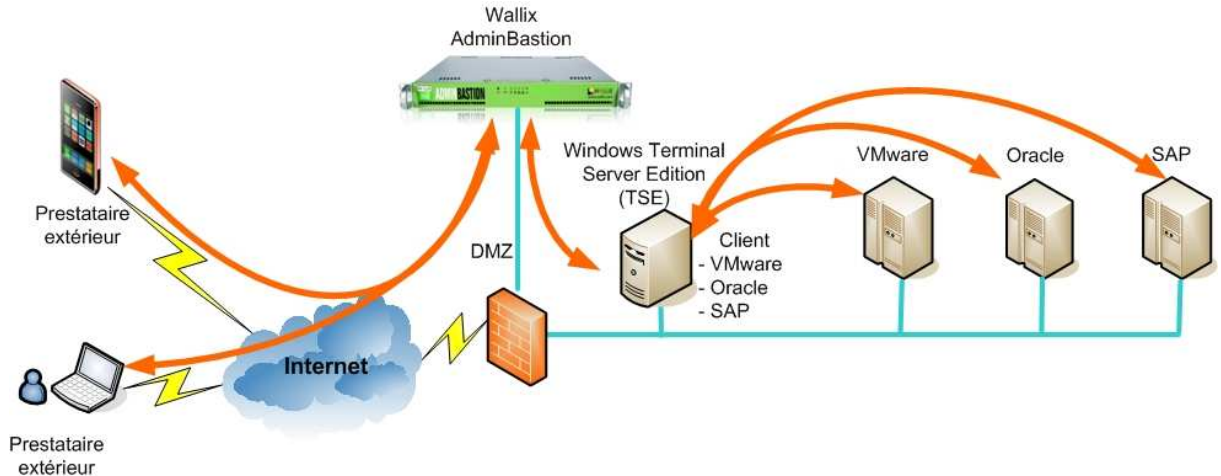
Par exemple, il est possible de ce fait de n'autoriser un prestataire en charge de la supervision de serveurs qu'à envoyer des commandes vers ces serveurs (ex : Reboot) sans possibilité de s'y connecter en « shell » ou bien de transférer des fichiers.

b) Compatible multi-équipements

WAB ne nécessite l'installation d'aucun agent sur les équipements cibles et permet donc - via le support natif des protocoles RDP, SSH, TELNET, SFTP et RLOGIN – de contrôler et d'enregistrer les connexions vers les principaux types équipement cible :

- serveurs Windows
- serveur Unix (AIX, Solaris, HP-UX ...)
- serveurs Linux
- équipements réseaux ...

En complément, WAB peut enregistrer les connexions utilisant d'autres protocoles – et notamment des protocoles métiers -via l'utilisation d'un serveur RDP (ex : Windows Terminal Server Edition) intermédiaire jouant le rôle de serveur de rebond sur lequel sont installés les logiciels clients des applications devant être enregistrées (ex : Oracle, SAP, Notes, VMware ...).



c) Outils de reporting intégré

Via l'interface d'administration du WAB, il est possible de connaître l'historique des connexions par utilisateur ou par compte cible ainsi que de savoir à tout moment « qui est connecté à quoi ».

En complément, WAB permet de disposer à tout moment de rapports sur les autorisations d'accès de chaque utilisateur, ainsi que les droits d'accès pour chaque compte cible.

WAB fournit par exemple automatiquement la liste des utilisateurs pouvant utiliser un compte précis sur un équipement (ie : qui a accès au compte générique « root » d'un serveur Linux).

d) Non-divulgateion des mots de passe des comptes cibles

WAB dispose d'un module d'authentification centralisée qui stocke dans WAB les différents mots de passe des comptes cibles. Ainsi, on peut permettre à un prestataire de se connecter à un compte à privilège sans avoir à lui transmettre le mot de passe correspondant.

En complément, dans le cas où un prestataire a accès à plusieurs comptes cibles, il n'aura toujours besoin de ne connaître **qu'un seul mot de passe** : celui de son compte WAB, évitant ainsi les risques de « fuite » de mot de passes existant avec d'autres solutions.

A noter, cette fonctionnalité est bien entendu désactivable compte par compte. Dans ce cas, le prestataire devra s'authentifier une première fois sur le WAB et une seconde fois sur l'équipement cible.

e) Traçabilité totale des opérations effectuées

WAB permet d'enregistrer le contenu des sessions, que ce soit sous la forme de fichier vidéo Flash© pour les sessions RDP/TSE (serveurs Windows) ou bien sous la forme de fichiers textes ou vidéo pour les sessions SSH, TELNET et rlogin (serveurs Linux & Unix, équipements réseaux ...).

Ces enregistrements de session peuvent ensuite être visualisés pour savoir exactement ce qui a été effectué par un prestataire sur un équipement cible. En complément, les enregistrements sous forme de fichiers textes des sessions SSH permettent d'effectuer très facilement des recherches par mot clé.

A noter : les enregistrements de session peuvent être stockés au sein du WAB ou bien être exportés vers un équipement de stockage externe.

f) Intégration à l'existant

WAB s'intègre à l'existant en terme de gestion des utilisateurs. Ainsi, si les prestataires figurent dans un annuaire d'entreprise (ex : LDAP, Active Directory ...), ils peuvent être authentifiés à partir de cet annuaire. Bien entendu, WAB permet également de les authentifier en local (le mot de passe du prestataire est alors géré par le WAB).

WAB permet également une authentification forte grâce au support de RADIUS comme protocole d'authentification externe et supporte donc des solutions telles que RSA SecurID ou bien SafeWord.

Enfin, WAB dispose d'un langage de scripting permettant à un applicatif externe (IAM, helpdesk ...) de piloter l'application.

g) Coût d'installation et d'administration réduit

WAB est commercialisé principalement sous forme d'appliance matérielle ou virtuelle, ce qui permet de mettre en place la solution dans des laps de temps très courts.

Par ailleurs, la mise en place de la solution ne nécessite l'installation d'aucun agent, que ce soit sur les équipements cibles ou bien sur les postes utilisateurs.

Le paramétrage initial du WAB, ainsi que son administration au jour le jour, s'effectue via une interface Web (https) simple d'emploi et intuitive disponible en français et en anglais. Il est également possible d'administrer le WAB via une interface « Commande en Ligne » (CLI).

En complément, WAB permet aux administrateurs de continuer à utiliser leurs outils habituels d'administration des serveurs (clients SSH tels que Putty ou WinSCP, client RDP « Bureau à distance » ...) – évitant ainsi d'avoir à former les prestataires à de nouveaux outils.

A noter : pour se connecter aux équipements cibles en passant par le WAB, les prestataires peuvent bien entendu utiliser un PC (Windows, Mac, Linux ...) mais aussi un smartphone (iPhone, Android, BlackBerry, Windows Mobile ...).

h) Génération d'alertes

WAB dispose d'un module de génération d'alertes permettant d'envoyer une alerte à une personne précisée à l'avance (ex : administrateur du WAB) en cas de connexion à un compte cible jugé critique.

Cette alerte est transmise par e-mail et est également inscrite dans le fichier de logs correspondant du WAB – ce qui permet de pouvoir aisément la traiter au sein d'un outil de supervision du marché.

Après réception de cette alerte, l'administrateur du WAB a la possibilité – si la session semble illégitime – de directement « tuer » cette session via l'écran affichant en temps réel la liste des sessions ouvertes.

VI. Les apports d'une telle solution

La mise en place d'une solution Wallix AdminBastion pour l'administration des prestataires IT externes apporte à la DSI des avantages compétitifs déterminants, qui peuvent être analysés et chiffrés en adoptant le plan suivant :

a) Coût d'installation et d'administration réduit

Par rapport à l'utilisation de plusieurs solutions juxtaposées du marché, une telle solution présente l'avantage d'un faible coût de possession (en anglais Total Cost of Ownership ou TCO).

Dans un tel projet, les éléments à prendre en compte pour comparer les différentes solutions sont :

- Durée du projet d'installation : parle-t-on d'une charge de travail qui se compte en mois hommes ou en jours ?
- Coût d'administration : combien de temps pour introduire un nouveau prestataire et les droits conférés, combien de temps pour faire évoluer le parc d'équipements à administrer
- Formation des utilisateurs : combien de temps pour former un prestataire externe à l'utilisation de la solution ? (important, notamment en période de congés avec les inévitables remplacements à organiser).

b) Diminution des risques

Par rapport à l'absence d'une telle solution, ou par rapport à une solution qui ne répond qu'à une partie des problématiques évoquées, la mise en place de Wallix AdminBastion permet à la DSI de réduire fortement les risques auxquels l'expose le recours à des prestataires externes :

- Non divulgation des mots de passe sur les machines cibles
- Granularité des droits d'accès
- Traçabilité intégrale des sessions d'administration (enregistrement de la session)
- Alertes en cas d'accès à des serveurs critiques

La comparaison de solutions entre elles peut se faire en attribuant un nombre de points à chacun des items précédents, en fonction de l'impact de chacun d'entre eux sur la sécurisation du SI de l'entreprise.

On peut aussi estimer le coût d'un sinistre dans ces domaines, et évaluer la diminution de la probabilité d'incident apportée par la solution. Par exemple, grâce à la traçabilité des sessions d'administration, et à la détermination objective de la responsabilité d'un incident, un infogéreur pourra faire une évaluation de la réduction des pénalités qu'il aurait à payer dans le cadre d'un contrat d'infogérance.

c) Conformité par rapport aux normes (« Compliance »)

Grâce essentiellement aux outils de reporting et à l'enregistrement des sessions d'administration (traçabilité), une telle solution permet aux entreprises soumises à des normes particulières (ISO 27001, SOX, Bâle II, ...) de progresser dans le respect de ces normes.

La valeur ajoutée par une telle solution est à rapprocher des recommandations faites par les auditeurs de la société, qui pourront aider à valoriser ses apports.

VII. Conclusion

Avec Wallix AdminBastion, les entreprises disposent aujourd’hui d’une solution permettant enfin un contrôle très poussé des prestataires IT externes sans s’engager dans un chantier technique et organisationnel pharaonique.

Ce contrôle s’appuie notamment sur une granularité très forte des droits d’accès ainsi que sur la possibilité de pouvoir enregistrer intégralement le contenu d’une session d’administration.

En complément, Wallix AdminBastion s’appuyant sur une gestion des droits « par rôle », son implémentation oblige à enfin formaliser les droits d’accès des administrateurs et donc à remettre à plat les politiques de contrôle d’accès (ex : qui a accès aux comptes générique ou de service) – sachant que celles-ci sont souvent informelles et donc sources de failles de sécurité critiques.

A propos de Wallix

Wallix est le leader français des logiciels de sécurité informatique à base d'Open Source.

Expert dans la sécurisation des réseaux et la gestion des infrastructures informatiques critiques, Wallix répond à des besoins émergents qui ne sont couverts que par des solutions complexes et coûteuses. Wallix privilégie les solutions sans installation d'agents spécifiques sur les équipements et qui s'intègrent aisément dans le système d'information du client.

Aujourd'hui, la société propose une offre innovante, Wallix AdminBastion - WAB, un puissant outil de traçabilité qui permet aux organisations de contrôler les connexions et d'enregistrer toutes les opérations d'exploitation effectuées sur les équipements ou l'infrastructure informatique des entreprises, en se conformant aux nouvelles normes. Les solutions Wallix sont commercialisées à travers un réseau de partenaires revendeurs et intégrateurs informatiques.

Wallix est leader des projets AdminProxy, Deskolo et OpenGPU soutenus par le FUI et la Région Ile de France. L'entreprise est lauréate de l'Oseo Innovation, du programme PM'UP, et partenaire du Pôle System@tic Paris Région. La société est soutenue par des investisseurs privés tels que les fonds Access2Net, Sopromec, Hedera et Venturis Capital.

Wallix

118 rue de Tocqueville

75017 Paris

Tel : +33 1 53 42 12 90

Web : <http://www.wallix.com>

©Wallix – décembre 2009