

EDITO	
AGENDA	
ACTUALITES	P2
VEILLE	P3
➤ Sécurité des logiciels (3/3) : Moyens palliatifs	
L'ESSENTIEL	P5
➤ Focus sur le SMSI (2/2)	
ZOOM	P7
➤ Le nomadisme	

EDITORIAL

Les vacances sont bel et bien finies et les choses sérieuses reprennent pour chacun, les professionnels de la sécurité comme les pirates. En effet, on constate une recrudescence progressive du nombre de virus détectés par messagerie, tout comme du nombre de spam.

Le plus gros danger est que les utilisateurs d'Internet ne sont pas aussi sensibilisés qu'on pourrait le croire ; à titre d'exemple, le phishing a causé plus de 110 000 euros de perte dans une banque Irlandaise le mois dernier. D'un côté des grands organismes s'entendent pour contrer ce fléau, d'un autre les éditeurs des futurs nouveaux navigateurs promettent de signaler ce type de menaces. Cela sera-t-il suffisant pour endiguer le phénomène ? Des mises à jour de plus en plus régulières s'imposeront vraisemblablement.

Un second article sur les aspects organisationnels de la sécurité trouve naturellement sa place dans cette édition, qui présente cette fois la norme ISO 27001 dans le détail des aspects de mise en place et du processus de certification. Le dernier article de la trilogie sur la sécurité des logiciels s'intéresse quand à lui aux moyens palliatifs à mettre en œuvre pour prévenir l'exploitation des failles de sécurité.

Nous faisons également un zoom sur les solutions de mobilité et nomadisme qui apportent beaucoup d'agilité à l'entreprise, mais qui doivent à tout prix être examinées sous l'angle sécuritaire car ce sont des vecteurs privilégiés d'intrusion.



AGENDA - Sélection rentrée 2006

⇒ **Salon de la SECURITE INFORMATIQUE - Paris la Défense, du 22 novembre au 23 novembre 2006**

Ce salon permettra aux DSI/RSSI d'avoir une vision sur l'état actuel du marché de la sécurité ainsi que ses enjeux. Les thèmes principaux concerneront les intrusions, le phishing et la cryptologie.

Plus d'infos : <http://www.infosecurity.com.fr>

⇒ **STORAGE EXPO - CNIT Paris la Défense, du 22 novembre au 23 novembre 2006**

Storage Expo est l'événement clé pour ceux qui ont en charge de gérer l'environnement de stockage, l'archivage, la reprise et continuité d'activité de leur entreprise. SAN, NAS, SRM et virtualisation seront abordés.

Plus d'infos : <http://www.storage-expo.fr>

⇒ **La 6e édition des Assises de la Sécurité et des Systèmes - Monaco - du 11 au 14 octobre 2006**

Phishing, robots, chevaux de Troie, virus, rootkits, espionnage économique : 2005 a subi une explosion sans précédent de la cybercriminalité. La sécurité informatique est, plus que jamais, un enjeu vital pour faire face aux menaces et vulnérabilités qui pèsent sur les systèmes d'information.

Plus d'infos : <http://www.lesassisesdelasecurite.com>

Directeur de la publication :
Edouard Jeanson

Agence ESEC
Sogeti Infrastructures Services
6-8 rue Duret
75016 Paris - France
Tél : 33 (0)1 58 44 55 66

Société par Actions Simplifiées
au capital de 15 999 790 €
RCS Paris 479 942 583

Edition du 25 septembre 2006

ACTUALITES

Microsoft compatible ou pas

Compte tenu des récents déboires de Microsoft avec certains organismes gouvernementaux, une équipe est maintenant chargée de s'assurer de la compatibilité des logiciels, tels que les maintenant célèbres Firefox (navigateur) et Thunderbird (client de messagerie). Un échange donnant-donnant, chacun participant au développement du navigateur de l'autre ; une façon également d'éviter les abus.

Pour les éditeurs d'antivirus le problème est autre. En effet, jusqu'à maintenant les antivirus interviennent directement au niveau du noyau pour avoir un accès rapide aux pièces à scanner. Or, une des fonctionnalités principales de Windows Vista est justement d'exercer un contrôle très fin des accès au noyau. Certains éditeurs commencent d'ailleurs à grincer des dents, surtout quand on sait qu'une partie de Windows

One Care, le service antivirus, spyware, analyse de base de registre est déjà disponible gratuitement en France.

Attention cependant, la version gratuite scanne à la demande et non en permanence ; la version complète payante sortira l'année prochaine.

Pour en savoir plus :
<http://www.microsoft.com>



Les téléphones mobiles écoutés

Un débat est né en Angleterre à propos d'un logiciel qui, une fois installé sur un téléphone portable permet de l'activer à distance pour écouter les bruits alentours. Bien évidemment, le plus dur consiste à installer le logiciel sur le téléphone que l'on souhaite surveiller mais dans certaines circonstances, l'installation peut être très simple à réaliser...

Cette application qui se « cache » et empêche sa désinstallation est heureusement déjà considérée par certains éditeurs d'antivirus comme un virus... L'éditeur lui se défend : comme l'installation est volontaire, son application ne peut être considérée comme un virus ou un Cheval de Troie...

Pendant que se déroulent ces débats, n'oubliez pas de verrouiller vos périphériques Bluetooth et infrarouge...

Pour en savoir plus :
http://www.theregister.co.uk/2006/09/08/flexispy_illegal



La voix sur IP passe plus mal

De plus en plus de données passent maintenant par Internet, des partages de fichiers (surtout la vidéo) aux offres de stockage en ligne. Globalement, les quantités de flux croissent plus vite que les tuyaux qui servent à les faire transiter et ceci commence à avoir un effet négatif sur la qualité des flux, et notamment sur les flux sensibles à la disponibilité de bande passante : les données voix.

Une récente étude américaine a montré que globalement la qualité de la voix sur IP baisse de manière régulière sur toute la durée de l'étude (Décembre 2004 à mai 2006). L'arrivée sur le marché de solutions telles que la fibre optique pour le particulier (FTTH : Fibre To The Home) risquerait paradoxalement de faire encore plus baisser cette qualité.

Un outil est disponible sur le site pour tester votre qualité de service voix sur IP.

Pour en savoir plus :
http://www.brixnet.com/news_and_events%5CpressRelease.aspx?news_item_id=858



VEILLE TECHNOLOGIQUE

⇒ Sécurité des logiciels (3/3) : les moyens palliatifs

L'ESEC vous propose une série de trois articles consacrés à la sécurisation des logiciels. Cette troisième partie présentera les moyens palliatifs destinés à prévenir ou au moins limiter les impacts des failles sur les logiciels.

📁 Introduction

Dans les deux précédents articles, nous vous avons présenté la sécurisation d'une application en amont, c'est à dire dès sa phase de conception et tout au long de son développement, par la formation et la sensibilisation des développeurs aux failles de sécurité classiques et à l'audit de l'application (code source ou binaire).

Nous allons dans cet article parler des moyens palliatifs. Nous présenterons pour cela quelques moyens existant sous Linux permettant de prévenir l'exploitation de failles de sécurité ou d'en limiter les impacts. Nous nous intéresserons au principe de fonctionnement de ces systèmes, ceux-ci étant transposables, et d'ailleurs souvent implémentés, à d'autres systèmes d'exploitation.

📁 SSP

Nous allons étudier un peu plus en détail un mécanisme de protection des applications contre les « buffer overflow » et autres attaques utilisant une corruption de la pile. La protection évoquée ici est celle développée par Hiroaki Etoh pour IBM, pour le compilateur GNU gcc (fournie comme un correctif pour gcc). Une ré-implémentation de cette protection est maintenant incluse dans gcc 4.1. Le principe est le même pour Stackguard et d'autres protections.

Le but de l'extension SSP est d'ajouter du code lors de la compilation d'un programme (en C ou en C++), afin de s'assurer que l'adresse de retour ne sera pas écrasée. La figure suivante présente simplement une pile avec deux tableaux (buffer1 et

buffer2) et l'adresse de retour (sfp). On imagine bien qu'en cas de débordement de buffers, les données écrites vont écraser la valeur de sfp.

```
<Haut de la mémoire>
-----
Buffer 1
-----
Buffer 2
-----
Sfp
-----
<Fin de la mémoire>
```

Mais lorsque la protection est activée, un marqueur est ajouté avant le pointeur de retour, entre les buffers et le pointeur de retour. Ainsi, tout dépassement de ces buffers visant à réécrire l'adresse de retour modifiera ce marqueur. Avant d'effectuer le retour, la valeur du marqueur est vérifiée. Si celle-ci est incorrecte, l'exécution du programme est stoppée. Pour éviter de pouvoir prévoir la valeur du marqueur, une valeur aléatoire est utilisée.

La protection SSP est un moyen de prévenir efficacement les différentes attaques réécrivant l'adresse de retour des fonctions sur la pile de façon linéaire, notamment les attaques de type « buffer overflow » ou « return-to-libc ». Les pertes en termes de performances à l'exécution sont par ailleurs négligeables (de l'ordre de quelques pourcents).

Ceci permet donc d'utiliser ce type de protection pour les programmes critiques d'un système d'exploitation.

L'inconvénient principal de cette méthode est qu'elle nécessite de recompiler les programmes que l'on veut protéger ; ceci est possible pour les programmes open source, si la fonctionnalité n'est pas incluse dans le binaire de l'application.

📁 PAX

Nous ne détaillerons pas le fonctionnement de Pax, cela dépasserait le cadre de cet article. Grossièrement, les protections offertes par PaX peuvent être scindées en deux catégories :

- protections de l'espace exécutable (executable space protections),
- disposition aléatoire de l'espace d'adresse (address space layout randomization).

📁 Executable space protections

Le principe est de ne marquer comme exécutables que les zones mémoires qui le requièrent, c'est à dire le code et non les zones de données. Prenons l'exemple d'une attaque par « buffer overflow » sur la pile : le fait que la pile soit accessible en écriture (ce qui ne peut être évité pour la pile) permet d'injecter du code et de réécrire l'adresse de retour ; cependant, si cette zone n'est pas accessible en exécution, l'exécution du code injecté sera refusée et le programme se terminera sans autres conséquences. On évitera à tout moment d'avoir des zones accessibles en écriture et en exécution, afin d'empêcher l'injection puis l'exécution du code.

📁 Address Space layout randomization

Cette technique consiste simplement à placer les différents éléments d'un processus (pile, tas, librairie partagée, etc.) de manière aléatoire en mémoire. La répartition en mémoire est aléatoire et sera différente à chaque nouvelle exécution.

Ceci rendra l'exécution de code déjà existant très improbable, que le code ait été injecté comme dans l'attaque par injection de shellcode (classiquement « buffer overflow ») ou non, comme dans le cas d'une attaque ret2libc. L'adresse mémoire sera fort probablement incorrecte, et le programme sera tué.

L'utilisation conjointe des pages non-exécutables et de la disposition aléatoire des différents éléments des processus permet de réduire les exploits possibles. Il faut ajouter à cela que tout processus tué par PaX (tentative d'exécution dans une zone où cela est interdit, erreur d'adresse mémoire) est journalisé afin de pouvoir tracer les problèmes.

Grsecurity

Grsecurity est un patch pour le kernel linux, qui en plus d'inclure les fonctionnalités de PaX, offre un certain nombre de nouvelles. Il est développé et maintenu par Brad Spengler et Michael Dalton.

La stratégie générale de Grsecurity est « detection, prevention, and containment » :

- detection : Elle consiste naturellement à essayer de détecter toute opération anormale, et à rassembler des informations a son sujet.

- prevention : La prévention consiste à mettre en œuvre les fonctionnalités empêchant l'exploitation de certaines failles.

- containment (endiguement) : Il consiste à éviter que l'exploitation d'une faille localisée ne mette en péril tout le système, par exemple en ne faisant pas automatiquement confiance aux autres tâches, en enfermant les processus sensibles dans certaines zones, etc.

Nous ne listerons pas toutes les possibilités offertes par Grsecurity. Il est notamment possible de prévenir les 'race conditions' dans le répertoire /tmp, de restreindre les processus que les utilisateurs peuvent voir, de rendre les ports sources TCP aléatoires, de restreindre les utilisateurs autorisés à ouvrir des sockets sur le net, etc.

Par ailleurs, une possibilité intéressante est le « Trusted Path Execution » : le principe de cette option est d'éviter que n'importe quel morceau de code ne puisse être exécuté (volontairement ou non), sans être sûr qu'il n'est pas néfaste. Pour permettre cela, les utilisateurs n'ont la permission d'exécuter les fichiers que dans les répertoires que root possède et dans lesquels il est seul à pouvoir écrire. Cela permet d'éviter qu'un utilisateur exécute par mégarde un programme malicieux qu'il a reçu par email par exemple.

Enfin, des fonctionnalités d'audit additionnelles sont apportées par Grsecurity : les signaux, changements d'heure, les erreurs de fork(), et l'adresse IP depuis laquelle est exécutée l'application peuvent être journalisés.

Conclusion

Les techniques de protection présentées ci-dessus, surtout lorsqu'elles sont combinées ensemble, offrent une protection très efficace contre la majorité des attaques classiques. Ainsi les attaques automatisées telles que celle des bots ou de « scripts kiddies » seront bloquées, et le niveau technique nécessaire pour réussir une attaque sera plus élevé. Cependant, aucune protection n'est infaillible, et il est vain d'essayer de sécuriser une application, dont la sécurité n'a jamais été prise en compte, uniquement par ce genre de moyens. La sécurisation d'une application doit prendre en compte l'ensemble des étapes décrites dans cette série d'article :

- conception sécurisée de l'application,
- formation des développeurs et sensibilisation aux problématiques de sécurité,
- audit de l'application,
- mise en place de moyens de protection.

Dans le cas d'une application déjà existante, il faudra commencer par l'auditer afin de déterminer les faiblesses dans le code et la conception, avant de passer par une étape de re-développement. Enfin, une fois cette phase terminée, la sécurisation du serveur (durcissement) grâce à ces méthodes finalisera la sécurisation de l'application.

Ce processus a naturellement un impact financier sur le coût du développement. Mais celui-ci est à comparer aux coûts engendrés par l'indisponibilité d'une application business, ou aux problèmes techniques et juridiques consécutifs à un piratage...

L'ESSENTIEL

➔ Focus sur la norme ISO 27001 (2/2)

La première partie de cet article dédié à la norme ISO 27001 a consisté en une présentation générale du standard et son utilité pour les entreprises dans un cadre opérationnel et économique. La seconde partie décrit le processus que doit suivre toute organisation désireuse d'implémenter un Système de Management de la Sécurité de l'Information (SMSI) suivant cette norme et d'obtenir une certification de conformité par un organisme accrédité.

Mise en place du SMSI

Cette mise en place s'appuie sur la norme ISO 27001 mais aussi ISO 17799, cette dernière étant un recueil des meilleures pratiques en matière de sécurité de l'information. Conformément au modèle P-D-C-A décrit dans le précédent article, elle comprend quatre phases principales.

La planification

De manière générale, cette phase est centrée sur l'analyse des risques pesant sur l'organisme et la définition des mesures à prendre pour les gérer, tout en obtenant un appui fort de la part de la Direction. En fonction de l'importance de l'entreprise et du périmètre du SMSI, cette phase peut représenter une somme de travail importante ; elle doit se concrétiser par l'élaboration des documents suivants :

- Le périmètre du SMSI. Ce document doit définir les limites du SMSI en termes de caractéristiques business, de l'organisation, de localisations géographiques, de biens, de technologies.
- Le document de Politique de Sécurité du SMSI. Ce document doit démontrer l'engagement de la Direction et définir l'approche de l'organisation pour gérer la sécurité de l'information en son sein. Il doit notamment contenir les éléments suivants :
 - Une définition de la sécurité de l'information et les objectifs généraux recherchés,
 - Une déclaration d'intention de la Direction soutenant les objectifs et principes de sécurité de l'information, en conformité avec la stratégie de l'organisme,
 - Une démarche de définition des objectifs de sécurité et des mesures à mettre en œuvre, intégrant l'appréciation et le management du risque,
 - Une brève explication des politiques, principes, normes et exigences en matière de conformité qui présentent une importance particulière pour l'organisme, notamment les éléments suivants :

La conformité avec les exigences légales, réglementaires et contractuelles ; les exigences en termes de sensibilisation en matière de sécurité ; la gestion de la continuité de l'activité ; les conséquences des violations de la sécurité de l'information.

- Une définition des responsabilités générales et spécifiques dans le domaine de gestion de la sécurité de l'information,
 - Des références à la documentation susceptible d'appuyer la Politique et devant être respectée, par exemple des procédures de sécurité plus détaillées devant être suivies par les personnels.
- Les procédures et les contrôles supportant le SMSI. Ceux-ci doivent permettre de détecter les erreurs dans les résultats de processus, d'identifier les failles de sécurité et les incidents. Ils doivent décrire la manière de revoir régulièrement l'efficacité du SMSI en prenant en compte les résultats des audits, les incidents, les retours d'expérience des différentes parties intéressées. Enfin, ils doivent comprendre une révision de l'évaluation des risques et des niveaux de risque acceptables en tenant de l'évolution de l'entreprise, des technologies, des objectifs et des menaces.
 - La description de la méthode d'évaluation des risques. Cette méthode doit être appropriée au SMSI, adresser la sécurité des informations liées au business ainsi que les exigences légales et réglementaires. Elle doit intégrer les critères d'acceptation des risques et identifier les niveaux acceptables de risque. Elle peut être soit normalisée (Ebios, Méhari, ...) soit propre à l'entreprise ou l'organisation.
 - Le rapport d'évaluation des risques. Ce document doit comprendre l'identification, l'analyse et l'évaluation des risques ainsi que l'identification des options pour les traiter.
 - Le plan de traitement des risques. Pour chaque risque identifié dans le rapport d'évaluation, le plan de traitement décrit les actions à mettre en

œuvre : appliquer les mesures de contrôle appropriées pour réduire le risque, accepter le risque, annuler le risque, transférer le risque (assurance, tierce-partie). Les mesures de contrôle sont à sélectionner dans l'annexe A de la norme ; elles sont décrites de manière explicite dans la norme ISO 17799, paragraphes 5 à 15.

- La Déclaration d'Applicabilité du SMSI et des mesures de sécurité à mettre en œuvre, de la part de la Direction. Cette déclaration doit inclure les mesures de sécurité (de l'annexe A) sélectionnées. Elle doit aussi présenter un résumé des décisions concernant le traitement des risques et justifier les mesures de sécurité (de l'annexe A) non retenues.

La mise en œuvre

C'est en quelque sorte la phase opérationnelle de la mise en place du SMSI. Elle se concrétise par les éléments suivants :

- L'implémentation des mesures sélectionnées dans le Plan de traitement des risques et figurant dans l'annexe A de la norme, qui opèrent sur l'ensemble des 11 domaines :
 - Politique de sécurité,
 - Organisation de la sécurité de l'information,
 - Gestion des biens,
 - Sécurité liée aux ressources humaines,
 - Sécurité physique et environnementale,
 - Gestion opérationnelle et gestion de la communication,
 - Contrôles d'accès,
 - Acquisition, développement et maintenance des systèmes d'information,
 - Gestion des incidents liés à la sécurité de l'information,
 - Gestion de la continuité de l'activité,
 - Conformité.
- L'élaboration des procédures pour assurer la planification, la mise en œuvre et les contrôles des processus de sécurité sélectionnés.
- L'élaboration des procédures pour détecter les incidents et y répondre.

• La sélection et la réalisation des enregistrements de sécurité, qui vont prouver la conformité du SMSI aux exigences et les contrôles déclarés (traces, journalisation, ...).

• L'élaboration des programmes de sensibilisation et de formation à la sécurité de l'information.

La surveillance et le contrôle

Il s'agit ici de surveiller et contrôler le bon fonctionnement du SMSI en :

- Exécutant les procédures définies précédemment,
- Menant des revues de surveillance régulières,
- Révisant les niveaux des risques résiduels,
- Conduisant des audits internes,
- Menant des revues de management.

La maintenance et l'amélioration

Conséquence directe des actions de surveillance et de contrôle, cette phase consiste à :

- Mettre en œuvre les actions correctives et préventives identifiées,
- Implémenter les améliorations potentielles détectées,
- Vérifier l'efficacité des mesures prises et des actions menées,
- Communiquer les résultats aux personnels responsables.

Suivant le modèle suivi par la norme ISO 27001, cette dernière phase de remise à niveau du SMSI doit régulièrement être suivie de la phase initiale de planification, afin de respecter le processus P-D-C-A.

Certification du SMSI

Une fois la mise en place du SMSI effectuée, en respectant le modèle P-D-C-A, l'entreprise peut passer à l'étape de certification. Très souvent, celle-ci est précédée d'une étape intermédiaire de validation, effectuée en interne ou par un prestataire extérieur spécialisé. Son but est de vérifier que le SMSI réalisé respecte bien la norme et ne comporte pas d'erreurs ou d'oublis réhibitoires pour obtenir la certification. Cet audit de conformité doit être réalisé suivant le même processus qu'un audit de certification afin d'identifier au mieux les éventuels points bloquants.

La demande de certification ISO 27001 doit être formulée officiellement auprès d'un organisme accrédité. En France, c'est le COFRAC qui accrédite les organismes autorisés à certifier les entreprises vis-à-vis de la norme ISO 27001. Parmi ces organismes accrédités, on peut citer LSTI (<http://www.lsti.fr>).

Estimation de la faisabilité de l'audit de certification

Cette étape vise à expliquer à l'entreprise demandeuse ce qu'est la norme ISO 27001 et les contraintes qu'elle impose pour obtenir la certification et la conserver dans le temps. Elle permet aussi d'estimer si la demande de certification de l'entreprise est recevable, en vérifiant rapidement certains points clés de la documentation SMSI : analyse de risques, sélection des mesures de sécurité mises en œuvre, déclaration d'applicabilité du SMSI par la Direction. Si le résultat est concluant, les deux étapes de l'audit sont présentées et planifiées : la revue de documentation et l'audit sur site.

Revue de documentation

Cette phase consiste à vérifier la conformité de la documentation vis-à-vis de la norme. Elle comprend l'analyse des documents et du processus de leurs mises à jour. Les documents indispensables sont :

- Le document de Politique de Sécurité du SMSI,
- Le périmètre du SMSI,
- Les procédures et les contrôles supportant le SMSI,
- La description de la méthode d'évaluation des risques,
- Le rapport d'évaluation des risques,
- Le plan de traitement des risques,
- Les procédures documentées,
- Les enregistrements de sécurité,
- La Déclaration d'Applicabilité du SMSI par la Direction.

Il convient également de vérifier comment les documents sont protégés et contrôlés. En particulier, une procédure documentée doit être établie pour définir les actions d'élaboration, approbation, révision, identification et destruction.

Si la documentation est inadéquate, cela peut amener à la suspension de l'audit et donc à l'échec du processus de certification.

Audit sur site

Une fois la revue de documentation achevée avec succès, on passe à l'audit du SMSI sur le ou les sites intéressés. Entretiens, observations et études d'enregistrements ont pour objectif de vérifier que l'entreprise fait bien ce qu'elle énonce à travers sa documentation.

L'implémentation effective des mesures de sécurité sélectionnées dans le plan de traitement des risques et leur contrôle est au cœur de cette étape.

L'audit génère des constats de conformité et de non-conformité. Tout constat de non-conformité du SMSI est accompagné des preuves associées et se traduit par un écart de non-conformité et se traduit par un écart de non-conformité par rapport à la norme, ces écarts pouvant être majeurs ou mineurs. Plusieurs écarts majeurs peuvent conduire à l'échec du processus de certification ou du moins à sa suspension, tant que les corrections n'ont pas été mises en œuvre et les écarts réduits.

Certification pour 3 ans

Lorsque le SMSI satisfait à toutes les exigences des critères de l'audit, l'entreprise obtient sa certification par l'organisme accrédité, pour une durée de 3 ans, mais le processus ne s'arrête pas là. En effet, le SMSI est un processus vivant qui doit être périodiquement réévalué et audité.

Des audits de surveillance du SMSI doivent être menés tous les six mois durant les trois ans de validité de la certification. A l'issue de cette période, un audit complet de certification doit être reconduit, et ainsi de suite...

Conclusion

Cette seconde partie a présenté dans le détail les composantes d'un SMSI et le processus de certification ISO 27001. Les contraintes imposées et le caractère temporaire de la certification ne doivent pas faire oublier les apports du SMSI pour la sécurité de l'information et du business au sein de l'entreprise et la confiance qu'il apporte aux clients et partenaires.

ZOOM

⇒ Le nomadisme

Dans l'environnement économique actuel, les solutions de mobilité/nomadisme apportent une certaine agilité à l'entreprise. Néanmoins, ces solutions doivent être envisagées sous contraintes budgétaires et sécuritaires. Il apparaît qu'une des meilleures façons de respecter ces deux impératifs est de dresser préalablement une typologie des utilisateurs.

Aujourd'hui, la convergence numérique se réalise à travers l'utilisation du protocole IP. Des flux, comme la voix, l'image et les données, qui autrefois étaient véhiculés sur des réseaux dédiés, peuvent être transportés maintenant sur un même support, réduisant de facto les coûts notamment d'infrastructure, mais aussi créant de nouveaux usages. Par exemple, un salarié en déplacement, pourrait utiliser un accès internet local pour à la fois téléphoner au siège et se connecter à son système d'information distant, et ce pour un coût local.

Parallèlement, l'évolution des spécifications de l'Internet, corrélativement avec l'apparition de nouvelles techniques de transmission telles que l'ADSL ou le WI-FI et l'utilisation de tunnels chiffrés (VPN SSL ou IPSEC), ouvre la voie au nomadisme des terminaux. Certains de ces moyens de télécommunication, comme l'accès ADSL à domicile, se généralisent. Ce nomadisme des terminaux permet au salarié de disposer de ses outils informatiques dans d'autres endroits (hôtels, aéroports, domicile, etc.) que son lieu de travail habituel. L'essor des réseaux sans fil (GSM, GPRS, EDGE, UMTS, WiMAX, etc.) et l'évolution de la 3G vers le HSDPA, apporte la mobilité au nomadisme. Le lien entre le salarié et son entreprise peut alors être maintenu en tout lieu, à partir de n'importe quel terminal informatique et à n'importe quel moment. L'ubiquité est devenue une réalité sociétale. D'ailleurs, cette possibilité de mobilité apparaît être un des premiers axes de réflexion technologique des entreprises.

Par ailleurs, cette convergence numérique se retrouve dans une uniformisation des usages au niveau du terminal informatique : celui-ci devient, de plus en plus, multi-usages en rassemblant diverses fonctionnalités (téléphonie, traitement de textes, photo,...) qui autrefois étaient associées à un type de matériel unique (téléphone, ordinateur, appareil photo,...). De nouveaux outils de communication, telles que la messagerie instantanée ou la web conférence, se diffusent rapidement et peuvent maintenir la continuité entre le salarié nomade et son environnement professionnel. Multi-usages, les équipements associés au nomadisme et à la mobilité sont indubitablement issus des progrès réalisés en matière de miniaturisation électronique puisque l'encombrement étant un obstacle majeur à la portabilité. Etant divers et variés, et sans prétendre à l'exhaustivité, ils incluent notamment les notebooks/tablet PCs, les PDA, les smart phones et les produits de type assistant communicant.

La mise en place de solutions de nomadisme et de mobilité dans l'entreprise peut générer des gains potentiels, par exemple en améliorant la productivité, en réduisant les coûts de communication, en offrant une meilleure réactivité, ou en favorisant une meilleure adaptabilité face à une concurrence protéiforme. Mais, sa mise en œuvre nécessite d'abord que l'entreprise dispose d'une vision claire des situations de nomadisme et/ou de mobilité qui apparaissent dans son périmètre, puis qu'elle liste les besoins spécifiques des utilisateurs (applications, terminaux, etc.), enfin qu'elle étudie l'opportunité (technique, financière, opérationnelle...) de l'implantation de telles solutions.

Dans des problématiques de mobilité et de nomadisme, 6 types d'acteurs différents, correspondant à des usages et des besoins distincts d'accès au système d'information, peuvent être recensés :

1. **Le salarié mobile** a besoin d'une connexion permanente au système d'information en tout lieu et à tout moment.
2. **Le nomade externe** est un salarié de l'entreprise qui est amené, dans le cadre de ses missions, à effectuer des déplacements occasionnels ou fréquents, dans différents lieux, autres que les sites de son entreprise. Mais, il n'a pas besoin d'un accès permanent au système d'information. Le nombre de ces lieux pouvant être restreint géographiquement ou non.
3. **Le nomade interne** est un salarié pouvant travailler hors de son bureau, mais en restant toujours sur son site habituel de travail. Pendant ce laps de temps, où il ne se trouve pas dans son environnement habituel de production, il exprime un besoin fort de connectivité au SI.
4. **Le sédentaire externe** est un salarié pouvant se connecter au SI, de l'extérieur, mais toujours à partir du même lieu géographique, par exemple de sa maison.
5. **L'invité interne** est un salarié qui se trouvant sur un site différent de celui auquel il est habituellement rattaché, souhaite se raccorder à son SI.

6. **L'invité externe** est une personne, n'appartenant pas à l'entreprise, qui a besoin d'utiliser le SI de l'entreprise pour se connecter à l'extérieur. Ce nomade pouvant être un fournisseur, un client, un consultant, un stagiaire, etc.

Ainsi, un salarié peut appartenir à une ou plusieurs catégories différentes, sauf évidemment à celle des « invités externes ». Les 5 premiers groupes ne sont donc pas forcément exclusifs. Cette typologie des utilisateurs met en exergue qu'une solution de mobilité et de nomadisme n'est pas forcément mono technologique, ou reposant uniquement sur des technologies mobiles, mais elle consiste plutôt en des associations regroupant, selon les cas, des technologies fixes et mobiles, des réseaux filaires et sans-fil, de proximité et longue distance, des liens synchrones et asynchrones. A titre d'exemple, pour le type « invité interne », un simple accès réseau filaire, convenablement configuré et protégé, au lieu d'un hot spot Wi-Fi dédié, peut s'avérer suffisant dans certains cas.

Ensuite, les besoins applicatifs, qui ont été exprimés par les utilisateurs, peuvent restreindre drastiquement les différents choix technologiques. Par exemple, des applications, telles que la visioconférence, peuvent exiger une bande passante importante incompatible avec ce que peuvent offrir certaines techniques de transmission.

En contrepartie des gains potentiels générés par les solutions de nomadisme et de mobilité, la sécurité et les infrastructures de l'entreprise peuvent être fortement impactées.

Tout d'abord, ces solutions impliquent, pour le moins, une ouverture du système d'information vers l'extérieur avec pour corollaire l'apparition de nouvelles menaces dont il faudra impérativement tenir compte en déployant notamment des systèmes de contrôle d'accès et de gestion des identités.

Deuxièmement, les terminaux informatiques (PDA, assistant communicant, ...) pouvant être utilisés hors de l'enceinte protectrice de l'entreprise, leur probabilité d'être perdus, volés ou piratés informatiquement est beaucoup plus élevée que dans le cas d'un usage interne. Cette situation génère au moins 2 conséquences. D'une part, des procédures éprouvées doivent être définies, formalisées et testées régulièrement pour gérer et traiter la perte et/ou le vol d'un équipement afin d'interdire immédiatement tout accès frauduleux au système d'information. D'autre part, les terminaux informatiques, qui constituent des outils de travail, peuvent contenir des informations stratégiques pour l'entreprise ou des données critiques, et qui à ce titre doivent être convenablement protégées. De même, si un pirate s'approprie frauduleusement le contrôle du terminal, il peut s'introduire par rebond dans le système d'information de l'entreprise.

Des méthodes appropriées de protection du poste de travail (firewall embarqué, etc.) devront donc être mises en œuvre. Enfin, au delà des modifications de l'architecture du SI qui seront nécessaires pour déployer ces solutions de nomadisme et de mobilité, il ne faut pas éluder toutes les implications en termes de gestion de parc et de licences, de mises à jour logicielle, de sauvegardes des données, de maintenance, de Plan de Reprise d'Activités et enfin de résilience de l'architecture dédiée à ces solutions.

Conclusion

Contrairement à certaines idées répandues, la mobilité et le nomadisme n'impliquent pas obligatoirement une solution technique sans fil. La réponse à ces besoins est constituée, dans la plupart des situations, par une combinaison de différentes technologies adaptées aux types d'utilisateur. Enfin, la mise en place de telles situations a un impact fort sur d'autres éléments de l'entreprise (sauvegarde, gestion des licences, PRA...).

Pour vous inscrire à la newsletter, veuillez envoyer un mail à newsletter-subscribe@esec.fr.sogeti.com et pour vous désabonner, veuillez envoyer un email à newsletter-unsubscribe@esec.fr.sogeti.com

Conformément à la loi « Informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au directeur de l'agence ESEC.