VIPAWAN
A CONFIDENTIAL IT SECURITY COMPANY

Lire Décider Agir

La lettre d'informations technologique et juridique de **VIPAWAN** • Numéro 6 - Janvier 2007

Édito

par Sabine Arnaud
Directrice marketing
& communication de VIPAWAN

Une année passionnante

L'année 2006 marque un tournant dans le monde de la sécurité des systèmes d'information. Les entreprises françaises ont en effet pris conscience que sans un véritable management de la sécurité elles ne peuvent espérer une gestion maximale des risques et une maitrise de leurs investissements.

Elaboration et mise en place de politiques de sécurité, contrôle de l'intégrité des données par le biais du contrôle de l'intégrité des systèmes, des réseaux et des postes clients, mise en conformité de la sécurité des systèmes d'information en regard des politiques définies et de la loi…Que de chemin parcouru depuis le début du XXIème siècle ! Le marché se rationalise. Les entreprises s'attachent enfin à mesurer le résultat de leurs investissements ainsi que leur capacité et celle de leurs prestataires à dimensionner les risques.

Le marché de la sécurité des systèmes d'information prend une voie rassurante, celle des procédures, de la méthode, du recul, du contrôle et du respect de la loi. Monitoring, surveillance, NAC, contrôle d'intégrité, contrôle interne ou conformité feront désormais partie de votre quotidien.

2007 promet d'être une année passionnante...

En pages 2 et 3
Dossier "Cadre juridique et légal et sécurité des systèmes d'information "

Contact
Vipawan S.A.S.
66, rue Lemercier 75017 Paris
Tél. : **01 58 59 39 39**
Fax : 01 58 59 39 38
Mail : **info@vipawan.fr**
Site : **www.vipawan.fr**

Actualité

par Igor Herrmann
Directeur général et directeur des opérations de Vipawan

Sécuriser les réseaux internes ou renforcer le maillon faible

Le contrôle d'accès des utilisateurs, la gestion des habilitations et la traçabilité, sont des concepts clés de l'application et du contrôle d'une politique de sécurité. Pourtant, les réseaux locaux (LAN) qui constituent sans doute l'un des maillons les plus critiques du système d'information (SI), en sont bien souvent exclus.

Le LAN : une aire de jeux ?

Intrusions, détournement de ressource, fuite d'information, indisponibilité, pandémie virale…Les acteurs de l'Intelligence économique et les Hackers internes font du LAN une aire de jeu.

Les switches permettent le contrôle d'accès au niveau utilisateur (802.1X) avec un bon ratio coût/débit gigabits/densité de ports. Mais, les fonctions de filtrage ou de traçabilité sont insuffisantes. De leur côté, les pare-feux, IPS et autres UTM, même s'ils offrent un haut niveau de sécurité et d'administration, présentent un très mauvais ratio coût/débits gigabits/densité de ports. Pire, les politiques de filtrage manquent de précision (cause : DHCP) et ne testent pas la conformité du poste client à la politique de sécurité avant d'ouvrir l'accès au SI.

Pour le LAN, les outils classiques rechignent à nous offrir un ratio coût/sécurité adapté aux enjeux sécurité.

Fort heureusement, en veille technologique constante, nous découvrons des éditeurs, qui, pendant que nous réfléchissons encore sur les lacunes évoquées, ont déjà mis en œuvre des solutions qui les comblent ; et même au-delà de ce à quoi nous aspirons.

Consentry CS : une gamme puissante qui s'offre le luxe de cumuler les avantages de diverses solutions

Les avantages d'un switch

- Mise en œuvre transparente pour les topologies logiques (VLAN, Spanning Tree, IP).
- Déploiement en cœur de réseau (pour le LANShield Controller) ou en Edge (LANShield switch).
- Densité de port comparable à celle d'un switch.
- Capacité de filtrage et le décodage protocolaire à vitesse "filaire" (jusqu'à 10 gbits/s).
- Boîtier 1U doté d'ASIC dédiés, sans parties mobiles avec alimentations redondantes.

La puissance fonctionnelle d'équipements sécurité haut de gamme :

- Politique de filtrage de type "deep inspection" avec mode "monitor only" et "fail-open".
- Prévention d'intrusion par analyse comportementale (sans signature).
- Support de la haute disponibilité en mode actif / actif avec synchronisation de session.
- Management centralisé et traçabilité des flux de tous les CS avec la console Insight.

Consentry innove à l'aide de deux fonctions majeures :

- Grâce à l'analyse transparente des requêtes d'authentification système (Kerberos/LDAP/Radius et même 802.1x) Consentry réalise une authentification passive et applique la politique de sécurité à une IP source et un nom d'utilisateur.
- Au travers de son portail Web, Consentry permet l'authentification des utilisateurs externes (consultant, visiteurs, …) par portail captif et à l'aide d'une applet non permanente (Java ou Active X). Consentry peut vérifier la conformité de tout poste utilisateur.

Consentry offre une vision performante et innovante de ce qu'il convient de marier dans un LAN : contrôle d'accès, gestion des droits et conformité au niveau utilisateur.

CONSENTRY™
NETWORKS
www.consentry.com

Zoom sur...

Cadre juridique et légal et sécurité des systèmes d'information

Les investissements en matière de sécurité et réseau sont une stricte déclinaison de la stratégie d'une entreprise qui se doit de considérer et respecter son environnement, les enjeux humains, économiques et financiers, juridiques et légaux ainsi que technologiques et techniques. Les prises de décision qui en découlent, transforment le plus simple investissement technique, en une démarche de management des risques.

par Thierry Edwiges
Président de VIPAWAN

Administrateur, gestionnaire et visionnaire

Les administrateurs sécurité et réseau se sont inévitablement rapprochés des problématiques liées aux enjeux stratégiques de leur propre entreprise. Le Législateur s'est en effet « efforcé » de transférer la responsabilité civile et pénale aux mandataires sociaux puis, très récemment, à l'entité morale. **De ce fait, les mandataires ont transféré à leur tour, le risque pénal auprès, notamment, de leurs propres administrateurs sécurité et réseau ou des prestataires de services.**

En examinant les dispositions du Code du Travail, du Code Civil et du Code du Commerce, il est aisé de trouver une foultitude d'articles « prêts à l'emploi » qui viennent aisément justifier la position des mandataires sociaux. 0r, **il est indispensable de respecter les limites fixées par ces mêmes codes et par les dispositions de la CNIL.**

C'est alors dans la mise en œuvre, que les difficultés croissent. Inutile de perdre votre temps à ester en justice si vos solutions techniques ne sont pas déclarées à qui de droit. Pas davantage vous ne pourrez intenter une action en justice sur la base d'un contrat de travail qui ne stipule pas les fonctions précises de votre administrateur en matière de sécurité des systèmes d'information. Est-il également nécessaire de préciser que l'achat d'une solution technique directement auprès d'un éditeur californien vous obligerait à demander réparation d'un préjudice auprès des instances californiennes ?

Le cadre juridique, légal et contractuel revêt une importance d'une ampleur sans précédent en matière de sécurité des systèmes d'information et des réseaux :

• Charte d'utilisation des moyens informatiques annexée au règlement Intérieur.

• Protocole d'accès au SI par des prestataires informatiques externes.

• Adaptation des contrats de travail des administrateurs incluant une clause de transfert de risque.

• Déclaration des outils de surveillance et de contrôle de l'activité des salariés auprès des instances représentatives (CE) et de la CNIL.

• Contrat de prestation incluant une clause de transfert de risque.

• Contrôle auprès des prestataires de l'existence d'une police d'assurance « Responsabilité Civile Professionnelle » et bien entendu, d'une police d'assurance de ses locaux, en cas de stockage temporaire de matériel appartenant au client.

Le responsable de l'administration de la sécurité et des réseaux de prendre en compte cette procédure, dans son quotidien ; tout en assurant les opérations permettant de maintenir dans le temps, le niveau de sécurité minimum requis pour l'exploitation de l'activité de son entreprise. Et, sans négliger pour autant, les règles de performances et d'optimisation.

Voilà que nous pouvons ajouter à la définition du poste d'administrateur, les termes de gestionnaire et visionnaire, souvent oubliés par les mandataires sociaux.

L'intégrité de la preuve

Les technologies évoluent à une telle rapidité, qu'un administrateur ne vit pas simplement sous la contrainte de maintenir à jour ses connaissances. **Un administrateur sécurité et réseau vit sous la contrainte de faire évoluer ses connaissances en même temps que de nouvelles technologies voient le jour, en même temps que de nouvelles menaces voient le jour, en même que de nouveaux besoins exprimés par sa propre entreprise voient le jour** (fusion, acquisition, partenariat, nouveaux produits et services, nouvelle ligne de production, internationalisation…) Une alchimie qui ne laisse pas de place à l'à-peu-près.

La récurrence quotidienne des dysfonctionnements techniques est une contrainte supplémentaire que l'administrateur connaît bien et qu'il doit résoudre en un temps record pour permettre aux utilisateurs finaux d'exécuter les tâches permettant de produire les richesses économiques et financières de leur entreprise. Il est sur ce point nécessaire de considérer quatre aspects fondamentaux qui justifient un travail consommateur de ressources :

> **« les solutions implémentées assurent-elles véritablement les tâches qui leur sont demandées ? »**

• La réalité des performances d'une solution technique qui souffre très souvent de dysfonctionnements.

• La qualité relative de l'implémentation parfois inadaptée.

• L'évolution constante du système d'information et des réseaux qui remettent en cause l'efficacité d'une solution technique telle qu'initialement déployée.

• Les erreurs de manipulation par les utilisateurs finaux.

Ainsi peut-on expliquer en partie, la complexité de l'application des textes de loi en environnement informatique. **La Jurisprudence s'impose souvent à la règle de Droit. Non pas en regard d'un vide juridique, mais plutôt en regard de tout ce qu'il convient de mettre en œuvre, de manière structurée et procédurière pour parvenir à prouver l'intégrité d'une preuve et affecter à un individu une responsabilité.**

Intégrité et conformité

Au-delà de toute solution technique, de procédure et d'organisation, de budget et de relation client/fournisseur, se situe naturellement la relation humaine. Dans une entreprise, chacun cherche le mariage idéal entre le bien-être et les nécessités économiques et financières.

Les premières années du XXI[ème] siècle ont été marquées par un dévolu jeté sur la protection du périmètre, caractérisée par un empilement de solutions techniques. Certains ont quand même fini par se demander comment optimiser le contrôle et valider l'efficacité de tous ces outils consommateurs de ressources humaines.

Les problématiques d'intégrité et de conformité des SI nées notamment de la contrainte imposée par les Etats-Unis, au travers de la Loi Sarbanes-Oxley, ont souligné une évidence : **nous ne savons pas précisément si les solutions implémentées assurent véritablement les tâches qui leur sont demandées, et à quel niveau de performance.** Si tant est que lesdites solutions font un « fabuleux travail », il n'est pas pour autant aisé de le démontrer. Enfin, quand bien même leur travail est « fabuleux » (intégrité), encore faut-il l'expliquer par rapport à un référent (conformité).

L'administration de systèmes d'information et de réseaux prendrait une nouvelle forme, plus compliquée.

Il convient, en effet, de considérer qu'il n'y a pas de sécurité optimale sans prise en compte de ce qui se passe sur son réseau. Il est ensuite nécessaire de s'assurer et de démontrer que les outils font bien ce qui est requis. Enfin, ce qui est requis doit être formalisé, au travers d'une politique de sécurité déclinée en schéma directeur et, c'est à cette ultime étape que l'on peur parler de conformité par rapport à une norme édictée.

Révélateurs d'une carence en matière de maîtrise de l'environnement des systèmes d'informations et réseaux, Sarbanes-Oxley, Bâle II, ou Mifid ont lancé, à juste titre, la mode des solutions d'intégrité et de conformité.

Sur un plan marketing côté éditeurs, les solutions qui ont vu le jour ont été segmentées : Intégrité systèmes et serveurs, intégrité réseaux et intégrité poste client.

Toutefois, la mise en œuvre de démar-

ches aussi fines que sont l'intégrité et la conformité, ne doivent en rien occulter la problématique de base : l'évaluation et la gestion du risque.

Evaluation et gestion du risque

Si le management de la sécurité des systèmes d'information et réseau est devenu une phase incontournable, n'oublions pas que nul n'a inventé de nouveaux risques ; c'est la forme de risques déjà existants qui est nouvelle. Or, la nature humaine a besoin de temps pour s'adapter à toute nouvelle situation qu'elle créée elle-même. Ce constat s'accompagne d'un paradoxe au niveau informatique : **l'homme fait évoluer l'informatique constamment et plus rapidement qu'il ne peut en absorber les conséquences dans son quotidien.**

En matière de risques, nous avions évoqué à l'occasion de séminaires, la cyndinique (science des dangers) et l'axiologie (déclinaison de la cyndinique, en environnement informatique). Agissant de la même manière qu'un actuaire chargé de déterminer la valeur d'une police d'assurance en évaluant le couple probabilité de survenance/gravité potentielle, un mandataire social dispose souvent de peu d'informations pour le faire appliquer au niveau informatique. Inversement, un responsable de la sécurité des SI dispose de peu d'informations lui permettant de déterminer la valeur financière et humaine de ce qu'il doit protéger.

> **« certains confondent le risque d'un évènement donné, avec le risque qu'un évènement donné survienne »**

Partant de la notion parfois opaque de détermination du risque maximum tolérable, **certains confondent le risque, qui est effectivement la réalisation d'un évènement donné, avec le risque, en tant que probabilité qu'un évènement donné survienne.**

Tout prestataire de services en matière de sécurité des SI se doit, vis-à-vis de ses clients, d'analyser les risques selon un objectif à atteindre clairement identifié et, d'évaluer si les risques identifiés sont de nature à empêcher l'atteinte dudit objectif.

Sans entrer dans les détails, et pour faire le lien avec la nature humaine, il est démontré que :

• Une prise de décision s'appuie sur une analyse coût/gain. Mais c'est plutôt au ratio « coût estimé/gain attendu » qu'il faut s'attacher, sachant qu'en général, le coût estimé et le gain attendu sont plus ou moins éloignés des coûts et gains réels.

• Un entrepreneur (ou un investisseur) a un comportement risqué. Une personne qui décide de prendre un risque le fait car à son avis le bénéfice (gain) vaut le risque encouru.

> **« Une démarche qualitative entraîne une relation saine et synergique »**

Paradoxalement en matière de sécurité des SI, la démarche est loin d'être aussi radicale. Il est très difficile pour certains chef d'entreprise, de faire le lien avec le coût d'un investissement nécessaire, établi en regard de la probabilité (et la gravité) pour qu'un éventuel accident informatique survienne et impacte la société à un niveau supérieur à l'investissement réalisé.

En conclusion, il est pensable de prendre la décision de ne pas investir dans la sécurité des SI en ayant évalué le plus précisément possible ce que l'on économise et la valeur de ce que l'entreprise perdra en n'ayant pas investi. Mais, il est irresponsable de ne pas investir en ayant juste considéré le coût des investissements et sa récurrence.

2007 : approche globale et exigences

La nouvelle année qui s'approche sonnera donc le glas de « l'achat d'impulsion » et, du conseil qui ne prend pas le temps de se reposer sur une approche globale et affinée du système d'information. Il est fort probable et c'est déjà le cas dans certaines entreprises, qu'il soit nécessaire de fournir de manière simultanée, une démarche conceptuelle, organisationnelle et opérationnelle, tout en offrant des garanties en terme de suivi client. Suivi client qui intégrera de plus en plus la garanties de pérennité des solutions et de fiabilité de leur l'intégration.

Faut-il préciser qu'il faudra mettre aux oubliettes les supports réduits à leur plus simple expression ? En s'obligeant à mettre en œuvre des processus d'intégrité et de conformité, les entreprises exigeront qu'il en soit de même pour les prestataires, afin de transférer le risque pénal et les responsabilités liées aux prestations déportées.

L'année 2007 se couvre donc d'un voile d'exigences. Cela signifie qu'un plus grand nombre de sociétés est arrivé à maturité en matière de maîtrise et d'expressions de leurs besoins.
Ce qui est certain, c'est que cette démarche qualitative entraîne de facto, une relation saine et synergique entre les 4 principaux acteurs du marché : les clients, les intégrateurs, les distributeurs et les éditeurs.

Zoom sur...

Le NAC : de la chimère, au Nouvel Animal de Compagnie de nos réseaux.

Par Igor Herrmann
Directeur général et directeur des opérations de Vipawan

Si le terme de NAC a pu échapper à quelques personnes, celles-ci restent rares en cette fin d'année 2006. Les NAC débarquent… D'Amérique pour la plupart.

Un NAC ambitieux

Le NAC ou Network Access Control a pour objectif d'être le Cerbère, "le gardien sans égal" des accès réseaux au système d'information. Mêlant à la fois contrôle d'accès au niveau utilisateur, gestion des habilitations, filtrage des flux, inspection de la conformité et "re-médiation" (mise à jour) du poste de travail, les NAC surprennent par leur ambition.

Ambition stratégique tout d'abord : faire appliquer, sans faille, la politique de sécurité de l'entreprise à l'utilisateur et à son équipement, dès les portes d'entrées du système d'information (connexion RJ45, Wifi ou accès VPN).

Ambition fonctionnelle ensuite : améliorer les capacités de contrôle et d'action tout en limitant les impacts sur l'existant et mieux, en valorisant les investissements déjà réalisés.

Ambition technologique enfin : assurer la synergie, la compatibilité, la communication et la stabilité entre couches systèmes et réseaux hétérogènes.

Mythe ou réalité ?

Peu à peu, les présentations plus vraies que nature font place à des gammes de produits bien réelles et opérationnelles.

Diverses tendances et nos propres expériences nous en ont convaincu. La course aux normes et aux appellations est de grande ampleur. Les NAC (Cisco), NAP (Microsoft), UAC (Juniper), TNC (Trusted Computing Group) et autres NEA (IETF) sont autant d'initiatives au cœur des stratégies et des activités de R&D des grands noms du réseau.
Des dizaines d'éditeurs du monde du logiciel, du réseau et de la sécurité se rallient aux initiatives en cours. Microsoft et Cisco ont même décidé récemment, de rendre leur approche inter opérable.

Mais l'un des faits les plus marquants réside dans la diversité, la puissance et l'excellence des solutions de "NAC" propriétaires. En effet, les grandes initiatives restent des "fédérateurs", sortes d'ossatures fonctionnelles qui codifient les relations entre briques techniques, plus que des solutions réellement complètes et opérationnelles.

Parallèlement, des éditeurs à la pointe de la technologie et de la sécurité, proposent des solutions au spectre fonctionnel et à la puissance inégalés.

D'ailleurs les leaders ne sont pas dupes ! Ils acquièrent les technologies avec une stratégie de développement marché.

2007 sera l'année des NAC

L'année 2007 marquera un véritable point d'inflexion fonctionnelle, technologique, économique et impactera largement tous les acteurs du marché.

Reste à faire en sorte, que nos nouveaux gardiens et **N**ouveaux **A**nimaux de **C**ompagnie de nos réseaux, soient à la hauteur des défis et menaces cru 2007.

Les intégrateurs, dans leur capacité de conseil et de délivrance devront être à la hauteur. Mais là, il ne tient qu'à vous de vous faire votre propre opinion sur les NAC … et leurs dresseurs.

Par Igor Herrmann
Directeur général et directeur des opérations de Vipawan

Contrer l'angle mort sur l'analyse des contenus en SSL

Le SSL constitue sans doute l'un des piliers technologiques du commerce électronique. Inventé au milieu des années 90, il a pour raison d'être la « pleine confiance » du consommateur dans ses actes d'achat via le Web.

Simplicité et premier niveau de sécurité

Le SSL remplit deux fonctions techniques fondamentales :

- Rendre opaques les contenus directement échangés entre deux machines, à l'aide d'un tunnel chiffré.
- Permettre l'identification des deux parties à l'aide de certificats.

Ces deux fonctions ne sont pas révolutionnaires. **L'une des forces du SSL réside dans la simplicité d'accès offerte aux utilisateurs** (gratuit dans tous les navigateurs et gestion des autorisations enfantine au travers d'un pare-feu d'entreprise).Une autre est **d'offrir un premier niveau de sécurité en minimisant les contraintes du côté fournisseur et utilisateur.**

En effet, il est attribué aux utilisateurs, une double responsabilité.

- Au niveau de l'identification, l'utilisateur a le choix d'accepter des certificats qui ne seraient pas validés par une **autorité** digne de confiance, dont la **date** serait expirée ou pour lequel le titulaire ne correspondrait pas au site Web demandé. L'utilisateur peut également accepter des certificats sans faire de contrôle sur leur éventuelle révocation.
- En terme d'échange de contenus, le tunnel chiffré met en échec l'analyse de contenu des protections « périmétriques » (pare-feu, proxy, IPS) dans les phases de contrôle antiviral, d'exfiltration de données confidentielles ou de connexion distante (VPN) ainsi que pour le contrôle de l'utilisation illégale ou non conforme de l'Internet.

Considérer le SSL comme un risque ?

La réponse relève tant de vos propres enjeux liés aux échanges que du contexte Risques de votre entreprise. Inévitablement, la gestion du SSL soulève néanmoins deux problèmes :

- **Protéger les entreprises et les individus des fraudes et abus.**
- **Respecter la Législation et les Codes de bonne conduite.**

Inscrite dans notre démarche d'analyse comparative et de veille technologique, nous vous invitons à vous pencher sur la solution **Webwasher SSL Scanner 6.0 de Secure Computing.**

Webwasher SSL Scanner 6.0 dispose d'une expertise unique sur le SSL couplée au meilleur du filtrage de contenu : décryption, inspection (antivirale, filtrage URL et de contenu) et réencryption.

La solution de l'Editeur Secure Computing est bien « pensée » :

- Maintien de l'authentification client avec certificats,
- Vérification des certificats serveur,
- Traçabilité complète pour l'administrateur.

L'ensemble est bien entendu embarqué sur un seul boîtier, au mieux en partage de charge avec de l'I-CAP.

Webwasher SSL Scanner 6.0 offre une politique de filtrage affinée :

- **Respect de l'individu :** la combinaison avec le filtrage d'URL évite de porter atteinte aux échanges personnels ou privés (banque en ligne,...)
- **Protection contre les abus :** pour des sites inconnus, le choix est laissé à l'utilisateur d'accepter l'inspection et accéder au site ou ne rien pouvoir faire.
- **Protection contre les menaces :** mise en garde des utilisateurs, vérification des CRL, antiphishing.

www.securecomputing.com

AVOCENT – DSVIEW 3 : à piloter depuis la plage en toute sécurité.

Permettre une disponibilité ininterrompue des services. Le défi est de taille. Et c'est actuellement ce que l'on exige de nous et de nos outils.

La contrainte des "services critiques permanents" ne concerne plus simplement et uniquement les data centers, mais également les outils de communication, d'accès Internet, mail et web en tête. Pour cela, il existe des outils : serveurs, routeurs, switches, appliances, de toute marque, toute puissance, de tous âges ; sous Windows, Unix… Et à chacun ses méthodes d'accès in-band et out-of-band : Telnet, SSH, TSE, VNC, câble série, carte de management et GUI de toutes sortes.

Le temps est l'ennemi de l'informatique et des hommes ; tôt ou tard, les incidents mécaniques, patch nuisant gravement à la santé du serveur, machines gelées à rebooter électriquement, vous obligent à vous retrouver physiquement face à la console, en urgence.

Accéder à n'importe quel moment à tout équipement critique via un accès physique est d'abord une mesure préventive avant d'imaginer les mesures correctives. Certes, cela est déjà possible. Mais avec quel niveau de sécurité (accès) et quel niveau d'organisation ?

Quid de la politique de gestion des mots de passe déficiente, des accès directs sur des cartes de management depuis les postes, des accès KVM ou des séries mobiles… Le danger est souvent lié à l'absence d'une réelle organisation. La sécurité est en jeu.

Si vous êtes en pleine réflexion sur ce sujet, prenez le temps de découvrir les solutions techniques de l'éditeur Avocent. Enlevez-lui l'étiquette « KVM » ! Cela va bien au-delà ! Avec **DSView 3** Avocent fait réellement changer de dimension :

- Authentification forte,
- journalisation et gestion des droits des administrateurs,
- arrêt électrique à distance,
- connexion de type Virtual Media,
- accès KVM IP,
- support d'IPMI,
- accès aux cartes DRAC, ILO, RSA, IPF,
- support de HTTPS, VNC, Telnet et SSH,
- accessibilité au travers d'un simple navigateur…

DSVIEW 3 s'inscrit dans une logique de plateforme sécurisée, centralisée et hautement disponible des accès logiques des infocentres.

Avocent™
www.avocent.fr