HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Menaces et vulnérabilités sur les réseaux et les postes de travail

Réunion Gartner IAT-SERSI

23 mars 2005

Gartner

Hervé Schauer
<Herve.Schauer@hsc.fr>

Hervé Schauer Consultants

- Société de conseil en sécurité informatique depuis 1989
- Prestations intellectuelles d'expertise en toute indépendance
  - Pas de distribution, ni intégration, ni infogérance, ni investisseurs, ni délégation de personnel
- Prestations : conseil, études, audits, tests d'intrusion, formations
- Domaines d'expertise
  - Sécurité Windows / Unix et linux / embarqué
  - Sécurité des applications
  - Sécurité des réseaux
    - TCP/IP, téléphonie, réseaux opérateurs, réseaux avionique, ...
  - Organisation de la sécurité
- Certifications
  - CISSP, BS7799 Lead Auditor, ProCSSI

Plan

- Contexte et exemples d'enjeux en sécurité
- Progiciels
  - Vulnérabilités des logiciels
  - Cycle de vie des vulnérabilités
  - Enjeux autour des vulnérabilités
  - Vers et virus
  - Recommandations
- Infogérance/Télémaintenance
- Périmètre
- Conclusion
- Références

Contexte

- Contexte économique souvent difficile
- Le DSI doit
  - Gérer le quotidien et accroître la productivité interne
  - Supporter une foule d'anciennes applications et intégrer des applications nouvelles
  - Ouvrir sans arrêt le système d'information sur l'extérieur sans nuire à celui-ci en interne
  - Répondre aux exigences des métiers en matière de nouvelles technologies et d'hétérogénéité et développer la cohérence du parc informatique
  - Se justifier économiquement
    - Réduire les coûts, calculer des ROI, se transformer en centre de service, ...
- ⇒ **La sécurité n'est pas toujours une priorité**

Exemples d'enjeux en sécurité

- Gestion des vulnérabilités dans les logiciels
  - Virus et vers
  - Mise à jour des progiciels
  - Déploiement des correctifs de sécurité
- Maîtrise du périmètre du SI
  - Gestion de la mobilité
  - Nomades, assistants personnels
  - Equipements personnels
  - Accès au SI à distance
  - Clés USB
  - Réseaux sans fil

Exemple d'enjeux en sécurité

- Fusion télécom et informatique
  - Insécurité de la téléphonie sur IP / voix sur IP
  - Gestion du téléphone par les services généraux ➔ DSI
- Infogérance et télémaintenance
- Maîtrise des crises
  - Denis de services et chantages aux dénis de service
- ...

Progiciels : constat

- Au début et pendant longtemps, pour un éditeur de logiciel

  La sécurité il faut en parler le moins possible et ne pas en faire

- Puis sur la pression des utilisateurs, certains éditeurs ont adopté un nouveau discours :

  La sécurité il faut en parler le plus possible et en faire le moins possible

- Et maintenant le discours technico-marketing est désormais

  La sécurité il faut en faire pour soi et faire croire qu'elle est pour le client

- Il n'y a pas de notion d'assurance qualité dans le progiciel
  - Aucune raison de ne pas publier des logiciels sans vulnérabilités
  - Le responsable de la défaillance d'un logiciel est son utilisateur, pas son éditeur

Vulnérabilités des logiciels

- Vulnérabilité logicielle : bogue dans un **produit** ayant un impact sur la sécurité du système d'information
- L'industrie informatique tend à considérer que les bogues sont partie intégrante de tout produit
  - Ce qui s'applique par extension aux vulnérabilités
  - Peu de progiciels largement répandus intègrent la sécurité dans leur développement et de manière récente
  - Vulnérabilités systèmes classiques tel que les débordements de *buffers* restent présentes, au moins dans les systèmes d'exploitation et logiciels serveurs
  - Les applications web introduisent de nouvelles classes de vulnérabilités
    - Côté serveur : applications web ne se protégeant pas correctement des données fournies par des utilisateurs malveillants
    - Côté client : vulnérabilités des navigateurs web et des technologies associées (contrôles ActiveX, applets Java, ...)

Cycle de vie des vulnérabilités

- Exemple de cycle de vie des vulnérabilités
  - Un progiciel est publié avec un bogue
  - La faille peut être identifieé en interne ou de façon externe
  - L'éditeur peut être contacté ou non
  - Un correctif peut être développé et publié
  - Des détails sur la vulnérabilité et une exploitation peuvent déjà avoir été publiés
  - Potentiellement, des pirates exploitent cette vulnérabilité
  - Vous appliquez le correctif de sécurité sur tous les systèmes sous **votre** responsabilité sont corrigés
  - **Tous** les systèmes **affectés** sont corrigés

Cycle de vie des vulnérabilités

- Deux seules étapes systématiques
  - Naissance de la vulnérabilité lors de la sortie du logiciel
  - Disparition de la vulnérabilité lorsque tous les systèmes existants sont corrigés ou que le logiciel disparait
  - A toutes les chances de ne jamais arriver, de nouveaux systèmes étant installés et non corrigés immédiatement (exemple de CodeRed et d'IIS 5)
- Les autres étapes sont optionnelles et dans n'importe quel ordre
  - Une vulnérabilité peut ne jamais être découverte mais cela ne signifie pas pour autant qu'elle n'existe pas
  - La publication d'un correctif a tendance à accélérer le cycle de vie
    - Tous les chercheurs en sécurité font du *reverse-engineering* sur les correctifs publiés par les éditeurs (ex : éditeurs de d'IDS)

Enjeux autour des vulnérabilités

- Les vulnérabilités et codes d'exploitation (*exploits*) ont une valeur marchande certaine
  - Rémunération des découvreurs de vulnérabilités
    - Vulnerability Contributor Program (VCP) d'iDefense (http://labs.idefense.com/)
  - Sociétés dont le modèle économique se construit sur les vulnérabilités et la mise à disposition d'exploits
    - Ex : ImmunitySec (http://www.immunitysec.com/), Core-ST (http://www.corest.com)
  - Malveillance et criminalité sur Internet sont intéressées par les vulnérabilités affectant les systèmes ou le poste client
    - Éditeurs de *spywares*, spammeurs
    - Criminalité organisée, notamment pour faire de l'hameçonnage (*phishing*)
    - Gouvernements ou autres ayant un intérêt à utiliser des 0day pour mener des attaques

Vulnérabilités : perspectives

- De plus en plus de vulnérabilités
- Vulnérabilités systèmes
  - Ex : vulnérabilités dans les interfaces RPC des systèmes Windows
- Vulnérabilités du poste client
  - Multiples vulnérabilités des navigateurs web, lecteurs multi-média, ...
- Vulnérabilités dans des logiciels de sécurité
  - Vers Witty (mars 2004) exploitant une vulnérabilité dans le module de décodage d'ICQ des sondes de détection d'intrusion ISS
  - Vulnérabilités dans les antivirus F-secure, Symantec et Trend Micro découvertes par ISS (février 2005)
- Vulnérabilités dans des applications web largement répandues
  - Forums, Mailman, Awstats, phpBB, ...

Virus et vers

- L'exploitation des vulnérabilités est visible par les problèmes de virus et vers
- Les vers montrent les limites des infrastructures
- Slammer
  - Serveurs MS-SQL
  - Duplication rapide par diffusion
- Sobig
  - Envoi de messages en masse par un logiciel de messagerie
  - Intérêt financier
- Santy (décembre 2004)
  - Utilisation automatique de Google pour rechercher les serveurs web vulnérables
- Les vers s'attaquent plutôt aux logiciels répandus

Exemple de Blaster

- Lancé le 11 août 2003
- Utilise une faille dans une partie ancienne de Windows dont le correctif a été publié un mois avant (16 juillet 2003)
- Se réplique par des ports de communication normalement fermés par les *firewalls*
- Est volontairement très lent, environ 2000 ordinateurs par heure
- Ciblait à terme un déni de service que un serveur : `www.windowsupdate.com` qui a pu être facilement évité
- A provoqué la mise à jour de la majorité des postes de travail W2K & WXP
- S'est dupliqué sur des réseaux non connectés à l'Internet ou protégés de l'Internet via les postes nomades
  - Premier ver mettant clairement en avant ce type de risque

Exemple de Blaster

- Perte de temps par les équipes bureautique et sécurité
  - A pris les utilisateurs durant les vacances
- Un des éléments de la cascade de pannes dans la coupure électrique aux USA ?
- Un des éléments du défaut d'information au ministère de la santé lors de la canicule ?
- A permis d'éviter un incident beaucoup plus dramatique
- A permis à plusieurs équipes de se pencher sur la partie de Windows incriminée et d'en découvrir de nombreuses autres failles similaires
  - De nouveaux correctifs ont été publiés en conséquence
- A qui a profité Blaster ?

Vers et virus : perspectives

- Actuellement très peu de vers sont développés par rapport aux possibilités
  - Beaucoup de vulnérabilités expoitables par des vers, très peu de vers
  - Une population de plus en plus large capable d'exploiter les failles
- Des vers qui exploitent les nouveaux vecteurs de propagation :
  - Systèmes de messagerie instantanée
  - Logiciels poste à poste (*peer-to-peer*)
  - Assistants personnels
  - Téléphones portables
  - Voix sur IP
- Des vers s'attaquant à une cible précise comme un ensemble d'organismes
  - Si uniquement un organisme est visé, quel sera le support des éditeurs d'anti-virus et la publication de correctifs ?

Gestion des vulnérabilités

- Répertorier les actifs logiciels de son système d'information
- Assurer une veille en vulnérabilités
- Déterminer si ces logiciels sont vulnérables
- Tester/valider/homologuer les correctifs s'il y en a et s'il y a lieu
- Appliquer les correctifs de sécurité
  - Le déploiement est souvent complexe et couteux
- Mettre en oeuvre des solutions pour réduire l'impact de l'exploitation d'une vulnérabilité
- S'assurer que le risque a été correctement pris en compte et réduit

Virus et vers : recommandations

- Protéger son infrastructure sur un périmètre vis-à-vis de l'extérieur avec un filtrage IP adéquat
- Déployer de l'anti-virus pour cloisonner son réseau
- Utiliser une mise à jour automatique des signatures
- Appliquer une défense en profondeur
  - 3 lignes de défense
- Gérer la sécurité des postes nomades
  - Equiper chaque poste d'un système de sécurité complet
  - Prévoir la gestion de mise à jour de l'anti-virus
  - Faire un contrôle d'intégrité avant la connexion au réseau de votre organisme
  - Préparer des procédures de sécurité et d'alerte en cas d'incident
    - Information des utilisateurs par SMS
    - Cellule de décontamination à l'entrée des batiments avec un CD-ROM

Progiciels : recommandations

- Demander un système qui répond a ses besoins et ne pas accepter un système qui répond aux besoins du fournisseur
- Reprendre ses contrats
  - Engager la responsabilité de l'éditeur
  - Intégrer l'application de sa politique de sécurité dès l'appel d'offre
- Ne pas oublier que dans le cas de sécurité et la supervision, elle se fait par de l'organisation, pas par un logiciel structurant avec un ROI mirobolant
- Diversifier les systèmes d'exploitation et les logiciels de base : bureautique, messagerie, butineur
- Ne pas oublier que le droit de propriété est supprimé, il est remplacé par un droit d'usage à la demande

Infogérance & télémaintenance

- Le système d'information est inter-pénétré de part et d'autre par les infogérances et les télémaintenances
- Relation contractuelle entre prestataire et client
- Exemples en télémaintenance
  - Routeurs chez les opérateurs de télécommunication
  - PABX
  - Imprimantes, télécopieurs, photocopieurs
  - SAN : réseau de stockage de données
  - Logiciels de gestion d'entreprise
    - SAP

Infogérance/télémaintenance : recommandations

- Appliquer sa politique de sécurité
- Intégrer la sécurité dès le départ dans tout processus d'infogérance et de télémaintenance
  - Contractuellement, systématiquement, ne serait-ce que pour savoir qu'il y a de la télémaintenance
- Minimiser les télémaintenances
- Créer un portail de contrôle d'accès
  - Indépendamment des moyens de connexion
  - Authentifier individuellement chaque télémainteneur
  - Journaliser les connexions
  - Recopier si possible la session complète des informations qui remontent à l'extérieur

Périmètre : concepts

- Espace dont je suis responsable
  - Le système d'information de l'entreprise
- Espace dont je ne suis pas responsable
- Je dois appliquer ma politique de sécurité entre les deux afin de protéger l'espace dont je suis responsable : **périmètre**
- Il semble difficile de se passer de la notion de sécurité périmétrique même si le périmètre est poreux :
  - Il faut donc savoir où est le périmètre
- Quelques limites du périmètre :
  - Le réseau et les canaux de communication
  - Les utilisateurs
- L'entreprise étendue

Périmètre du SI : constat

- Le nouveau protocole de l'Internet dans les entreprises est HTTP/HTTPS
  - Le nouveau protocole des entreprises sur Internet n'est pas IPv6
  - La promotion des *Web Services* vise à ré-encapsuler tout un ensemble de protocoles sur HTTP au lieu de le faire sur IP, pour contourner le *firewall*
  - Les logiciels d'EDI, de messagerie instantanée, d'agenda et de messagerie basés sur les *Web Services* sont très souvent des outils de contournement de la politique de sécurité de l'organisme
- Les réseaux sans fil ouvrent une brèche dans l'aspect physique du périmètre du réseau
  - Un réseau local sans fil se sécurise (sauf déni de service) : WPA/802.11i
  - Avec de la sécurité dans le réseau : 802.1X, indépendante des réseaux sans fil

Périmètre du système d'information

- Les **télécommunications** et l'**Internet** ne font qu'**un**
  - Le PABX classique est un ordinateur Unix qui interroge l'annuaire d'entreprise
  - La télémaintenance par liaison téléphonique en PPP ne sert qu'à contourner le *firewall* sur les liaisons IP
  - Les liaisons séries des immeubles intelligents passent aussi à IP
    - RS232 devient Telnet sans authentification
    - Les protocoles propriétaires (LonTalk, BACnet) sont ré-encapsulés sur IP
  - La Voix sur IP / Téléphonie sur IP c'est :
    - Signalisation/contrôle et transport de la voix sur le même réseau IP
    - Aucune authentification mutuelle, aucun chiffrement
    - Les autres services comme le DNS, DHCP, etc qui deviennent **critiques**
    - Attaques accessibles à tout informaticien
    - Et pour respecter le ROI, tout mélangé sur la même infrastructure filaire chez soi
    - Le PABX ou Centrex remplace toutes les strates de *firewalls* IP

Périmètre : recommandations

- Si nécessaire se réorganiser
- Production réseau/télécom vs sécurité
  - La volonté de disponibilité du réseau est souvent difficilement compatible avec la politique de sécurité
  - Il faut donc distinguer les équipes opérationelles réseau et sécurité
  - L'équipe réseau/telecom gère le réseau
  - L'équipe sécurité gère les équipements sur le périmètre, dont la fonction principale est la sécurité
- Production réseau/télécom vs téléphonie
  - Le téléphone n'est plus un service général mais de l'informatique
  - Il doit être géré par la production informatique

Périmètre : recommandations

- Accepter et gérer des moyens de connexions hétérogènes
  - Le même PC portable ou assistant personnel est tantôt connecté au réseau d'entreprise :
    - Dans son bureau
    - Dans la salle de réunion
    - Via l'accès Internet ADSL de la maison
    - Via un modem GPRS dans le train
    - Via un HotSpot dans un aéroport
- Accepter et gérer des plates-formes hétérogènes
  - Intégrer dans le système d'information de l'entreprise les équipements choisis, achetés et appartenant à l'individu
  - La monoculture est source de fragilité
  - Fournir de quoi chiffrer pour tous les types d'assistants personnels
    - PalmOS, Symbian, Windows CE, ...

Périmètre : recommandations

- Prévenir les systèmes de contournement du périmètre
  - Exemples comparatifs ;
    - Sprint PCS Business Connection : Ré-encapsulation de TCP/IP sur HTTP, serveur central chez Sprint
    - Lotus Notes : Protocole propriétaire sur TCP/IP, serveur central dans l'entreprise
    - Ipracom : Protocole propriétaire en UDP sur IP ré-encapsulé sur HTTP sur TCP/IP, pas de serveur central
    - Enetshare : XMPP, XML et Webdav sur HTTP sur TCP/IP, serveur central dans l'entreprise
  - Skype
  - Blackberry
- Intégrer les extensions de plages horaires

Périmètre : recommandations

- Reconcevoir les passerelles de sécurité sur le périmètre en prenant en compte :
  - Analyse de contenu dans HTTP
    - Recherche de protocoles re-encapsulés
    - Anti-virus
  - Protocoles de messagerie instantanées et de téléphonie
  - Accès distants de toute nature
  - Journalisation permettant des analyses statistiques

Périmètre : recommandations

- Cloisonner le réseau et intégrer la sécurité dans le réseau
  - Le réseau est le dénominateur commun du système d'information
  - Le réseau est le premier composant réellement sous le contrôle de l'entreprise
  - Séparer les réseaux bureautique, supervision, téléphonie, etc
  - Prévoir les commutateurs/firewalls et la prise en compte de l'espace hertzien
  - Prévoir et accepter la sécurité entre les VLAN
  - Authentifier équipements et utilisateurs
  - Gérer dans le réseau des zônes de confiances telles qu'elles existent dans l'entreprise

Périmètre : recommandations

- N'utilisez pas votre PABX comme firewall
  - Ne le connectez pas en VoIP sur l'extérieur
- N'utilisez pas encore la téléphonie sur IP
  - Il n'y a encore aucun calcul de retour sur investissement
  - Attendez que la normalisation de la sécurité soit terminée
    - Protocole de gestion de clés VoIP : MiKEY
  - Attendez que les terminaux aient les moyens de supporter des négotiations de clés en cours de conversation et de chiffrer
- Si c'est trop tard faites faire un audit de sécurité

Conclusion

- Prendre en compte la sécurité et les conséquences de ce que l'on fait sur la sécurité
  - Le fait de penser à la sécurité dans toutes les phases d'un projet, d'une décision, aide à l'amélioration de la sécurité
  - La sécurité ne coûte que quand elle est prise à part ou après

Questions ?

Herve.Schauer@hsc.fr

Ressources

- Sur **www.hsc.fr** vous trouverez des présentations sur
  - Infogérance en sécurité
  - Sécurité des réseaux sans-fil
  - Sécurité des SAN
  - Sécurité des bases de données
  - SPAM
  - BS7799
  - etc

- Sur **www.hsc-news.com** vous pourrez vous abonner à la **newsletter HSC**