



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Enjeux de la sécurité des réseaux



Séminaire Inkra Networks

14 octobre 2004



Virtualisation des architectures sécurisées

Perspectives pour simplifier et dynamiser, en baissant vos coûts.



Hervé Schauer

<Herve.Schauer@hsc.fr>

- x Exemples de cas réels
- x Segmenter le réseau
- x Comment segmenter le réseau ?
- x Défense en profondeur
- x Besoins d'un réseau
- x Besoins des individus
- x Etat des lieux des réseaux
- x Segmentation + virtualisation
- x Conclusion

- x Un utilisateur branche son ordinateur portable sur le réseau d'entreprise après l'avoir utilisé sur Internet et le virus ...
 - x Interdire les ordinateurs portables ? Déporter la responsabilité sur l'utilisateur ?
 - x Segmenter le réseau et minimiser les risques d'infections
- x Un stagiaire indélicat récupère les mots de passe des boîtes aux lettres, lit les boîtes aux lettres et perturbe l'entreprise
 - x Ne plus prendre de stagiaires ? Les sensibiliser mieux ?
 - x Segmenter le réseau et faire un réseau stagiaires
- x Un sous-traitant mécontent stoppe 300 serveurs Windows avec un déni de service
 - x Sécuriser les serveurs, appliquer les Service Packs et correctifs de sécurité en production, ...
 - x Segmenter le réseau et ne permettre le déni de service que sur les 6 serveurs dont le sous-traitant avait besoin d'un service

- x Les employés réclament les mêmes conditions que leurs collègues dans un pays voisin après avoir vu leurs avantages sur leur site web
 - x Ajouter un contrôle d'accès sur les centaines de serveurs web internes concernés ?
 - x Créer un segment de réseau à part dans chaque filiale pour les serveurs WWW accessibles de toute la société, configurer le filtrage IP pour n'autoriser l'accès que vers ce segment, et utiliser un relais HTTP pour permettre des exceptions à la règle de filtrage IP pour des utilisateurs authentifiés
- x Un individu provoque un transfert de fond en s'introduisant depuis le réseau internet sur un serveur relié à la banque et en falsifiant la base de données
 - x Couper le serveur bancaire du réseau interne ? Le sécuriser mieux ?
 - x Mettre en oeuvre un filtrage entre le serveur bancaire sensible et le réseau interne comme il était déjà fait dans le lien vers la banque

- x Un partenaire sur le développement de la version N d'un produit a volé les spécifications de la version N+1 sur des dizaines de serveurs applicatifs
 - x Gérer correctement les groupes d'utilisateurs et leurs privilèges sur l'ensemble des serveurs ?
 - x Doubler le nombre de serveurs, dupliquer les applications, affecter un ensemble de serveurs accessibles aux partenaires et les segmenter sur le réseau
 - x Virtualiser les serveurs logiques dans les serveurs physique
 - x VMware, etc
 - x Inutile de multiplier le nombre de serveurs physiques et leur maintenance

- x Un partenaire s'infiltré sur le système d'information d'un autre partenaire via une faille applicative dans mon extranet
 - x Sécuriser l'application ? Renvoyer un cahier des charges avec mes besoins de sécurité au développeur ?
 - x Filtrer aussi en sortie
 - x Dupliquer la partie applicative et ne garder qu'une base de donnée unique
 - x Virtualiser les serveurs comme précédemment

- x Contrôler l'accès aux serveurs ?
- x Gérer la sécurité des serveurs, des applications, d'un système d'information complexe et évolutif ?

Segmenter le réseau

Cloisonner le réseau

Compartimentaliser le réseau

- x Réutiliser l'existant ?
 - x Fonctionnalités des équipements hétérogènes
 - x Beaucoup d'équipements sont spécialisés et ne savent pas faire quelque chose de nécessaire
 - x VPN, filtrage IP entre VLAN, etc
 - x Réseau toujours en production \Rightarrow tests impossibles et reconfiguration délicate
- x Profiter d'une refonte, d'une extension ou d'une reconstruction du réseau
- x Choisir des équipements capables de gérer l'ensemble de vos besoins y compris la sécurité

- x Les tentatives d'intrusion sont externes et les intrusions réussies sont internes
 - x Gartner : 70% des intrusions sont internes (2002)
- x Un système de sécurité a toujours intérêt à être doublé d'une autre sécurité
 - x Contrôle d'accès et authentification sur le périmètre, dans le réseau et sur le poste de travail
 - x Anti-virus sur le périmètre, dans la messagerie, sur le serveur de fichiers, sur le poste de travail et dans le réseau
- x Pour appliquer ce principe simple, il faut toujours déployer de la sécurité
 - x Dans le réseau
 - x Sur plusieurs niveaux

- x Contrôle d'accès, analyse de contenu, génération de journaux
 - x Eventuellement : authentification (802.1X), détection d'intrusion, VPN chiffrés
- x Souplesse et évolutivité dans la gestion, facilité d'exploitation
- x Performance, routage, redondance, DHCP, ...
- x Qualité de service

- x De plus en plus difficile de séparer ces fonctions
 - x Technologies de base identiques et gestion de plusieurs équipements couteuse
 - x Impossible avec les réseaux sans fil

Commutateur multifonctions

- x Utilisateurs
 - x Transparence, convivialité
- x Exploitants du réseau
 - x Simplification de l'exploitation
 - x Vision globale et cohérente de l'ensemble
 - x Information temps réel et facilité d'intervention
- x Clients et partenaires
 - x Confiance, SLA, réactivité
- x Responsable sécurité
 - x Vision globale de l'application de la politique de sécurité dans le système d'information
 - x Tableaux de bord

- x Périimètre parfois poreux
 - x Ordinateurs nomades
 - x Ré-encapsulations d'IP sur un protocole autorisé
 - x VoIP & imbrications télécom/réseaux IP, réseaux sans-fil
 - x Extranets, applicatifs mal conçus, etc...
- x Plusieurs métiers, plusieurs services, plusieurs partenaires, plusieurs clients, plusieurs pays
 - x Politique de sécurité à appliquer différentes
- x Plusieurs offres de services, plusieurs typologies de clients
 - x Configurations différentes
 - x Isolation entre les clients

Appliquer une sécurité segmentée dans le réseau

- x Permet de gérer la croissance
- x Plus facile à gérer
- x Meilleure cohérence
- x Bonne granularité
- x Plus facile à mettre à jour
- x Plus optimisé donc plus économique

- x La **segmentation** et la **virtualisation** des services vont dans le sens de l'histoire
 - x Ils s'appliquent aux réseaux d'entreprise et aux hébergeurs
 - x Ils imposent d'acquérir la confiance dans ses équipements et leur gestion
 - x Qui sont à la fois commutateur, routeur, *firewall*, ...
 - x Il faut alors accepter un VLAN internet et un VLAN réseau privé sur le même équipement
- x La segmentation et la virtualisation sont un atout pour les clients du système d'information, pour les exploitants et pour le management

The Network is the Firewall © juin 1999

Questions ?

Herve.Schauer@hsc.fr

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

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

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