



Gérer l'insécurité des infrastructures spontanées ou Infogérance cachée

Eurosec

session S4 vers de nouvelles vulnérabilités

3 avril 2006

Hervé Schauer

CISSP, ProCSSI, ISO 27001 Lead Auditor

[<Herve.Schauer@hsc.fr>](mailto:Herve.Schauer@hsc.fr)

- Infrastructure
- Infrastructure spontanée
- Caractéristiques
- Aspects
- Rappels en sécurité
- Infrastructures spontanées
- Exemples
 - WebEx
 - Skype
- Actions
- Conclusion
- Prochains rendez-vous
- Références
- Ressources

**Les transparents seront
disponibles sur
www.hsc.fr**

- Ensemble de matériels, logiciels, services, ...
- Utilisateur a un besoin →
- Service informatique
- Projet
- Maîtrise d'ouvrage
- Maîtrise d'oeuvre
- Contrats de service
- Contrôle qualité
- Sécurité ←
- Besoin de l'utilisateur est satisfait

- Ensemble de matériels, logiciels, services, ...
- Utilisateur a un besoin
- Télécharge ou achète lui-même



- Besoin de l'utilisateur est satisfait

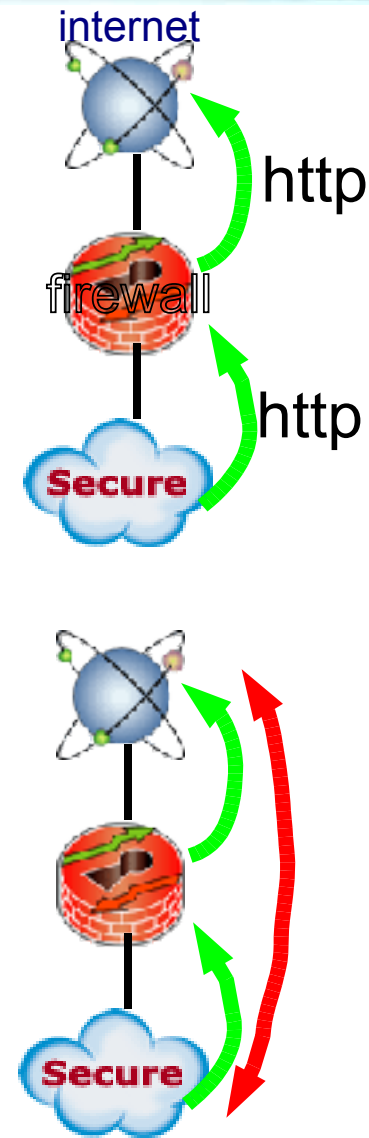
Spontaneous infrastructure

Click-and-run applications

- Service informatique inutile
- Pas de projet
- Pas de maîtrise d'ouvrage
- Pas de maîtrise d'oeuvre
- Pas de contrats de service
- Pas de contrôle
- Pas connaissance du besoin
- **Sécurité ?**

- Infrastructure qui apparaît de manière spontanée
- Par opposition aux infrastructures qui sont mises en place par la direction des systèmes d'information
- Principaux vecteurs
 - Services disponibles sur internet
 - Courrielweb, messageries instantanées
 - Téléchargement de logiciels sur internet
 - Libres : OpenWengo
 - Propriétaires et gratuits : tous les logiciels espions (*spywares*)
 - Propriétaires et payants
 - Achats de matériel
 - Par l'individu : téléphone, assistant personnel, lecture à distance de BAL
 - Par son département métier ou l'achat de consommables

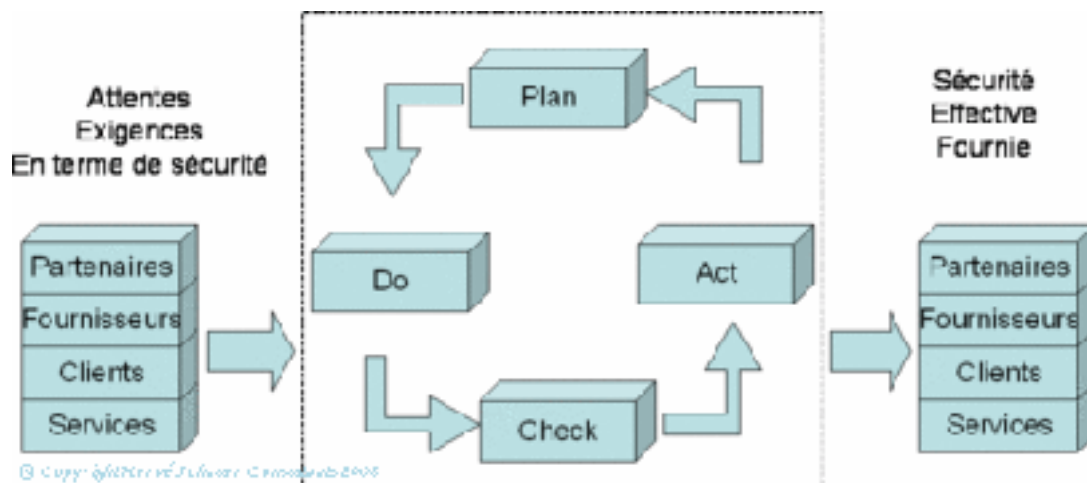
- Contournement de la protection périmétrique
 - Sur le poste de travail si pas de contrôle central avec des agents performants sur chaque poste
 - USB, bluetooth, SD-Card, etc
 - Sur le périmètre réseau par encapsulation dans HTTP ou HTTPS
 - Pas de limite aux ré-encapsulations avec les *firewalls* n'incluant pas de filtrage dans HTTP
- Utilisation d'un serveur sur internet
- Utilisation de dialogues poste à poste (*peer to peer*)
 - Création d'un réseau virtuel poste à poste
- Pas de contrat autre que le clic de souris



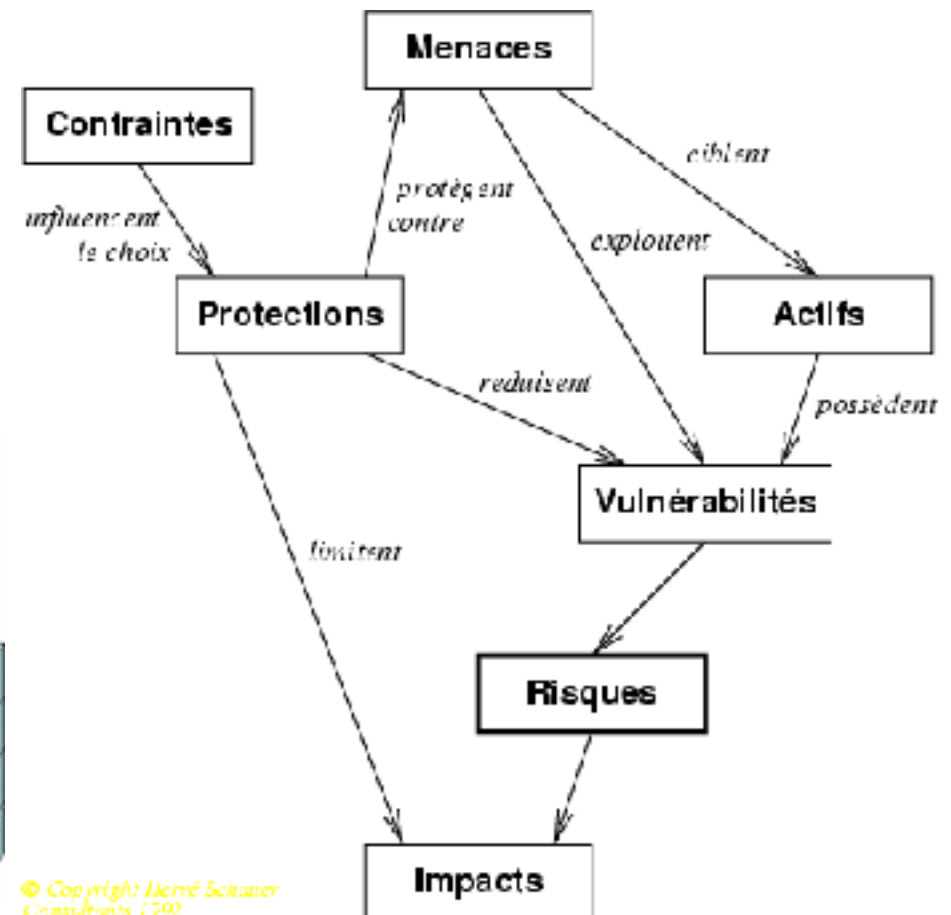
- X25 et réseaux privés : contrat de bout en bout
- Accès internet : contrat sur son extrémité
 - Qui potentiellement ne garanti rien
- Infogérance : contrat de service
 - Qui généralement incluera la sécurité
- Réseaux spontanés : pas de contrat
 - Infogérance cachée

- Appliquer sa politique de sécurité
- Analyser les risques
- Ne pas faire de choix par défaut, sans réflexion

ISO IS 27001 / ISO IS 17799



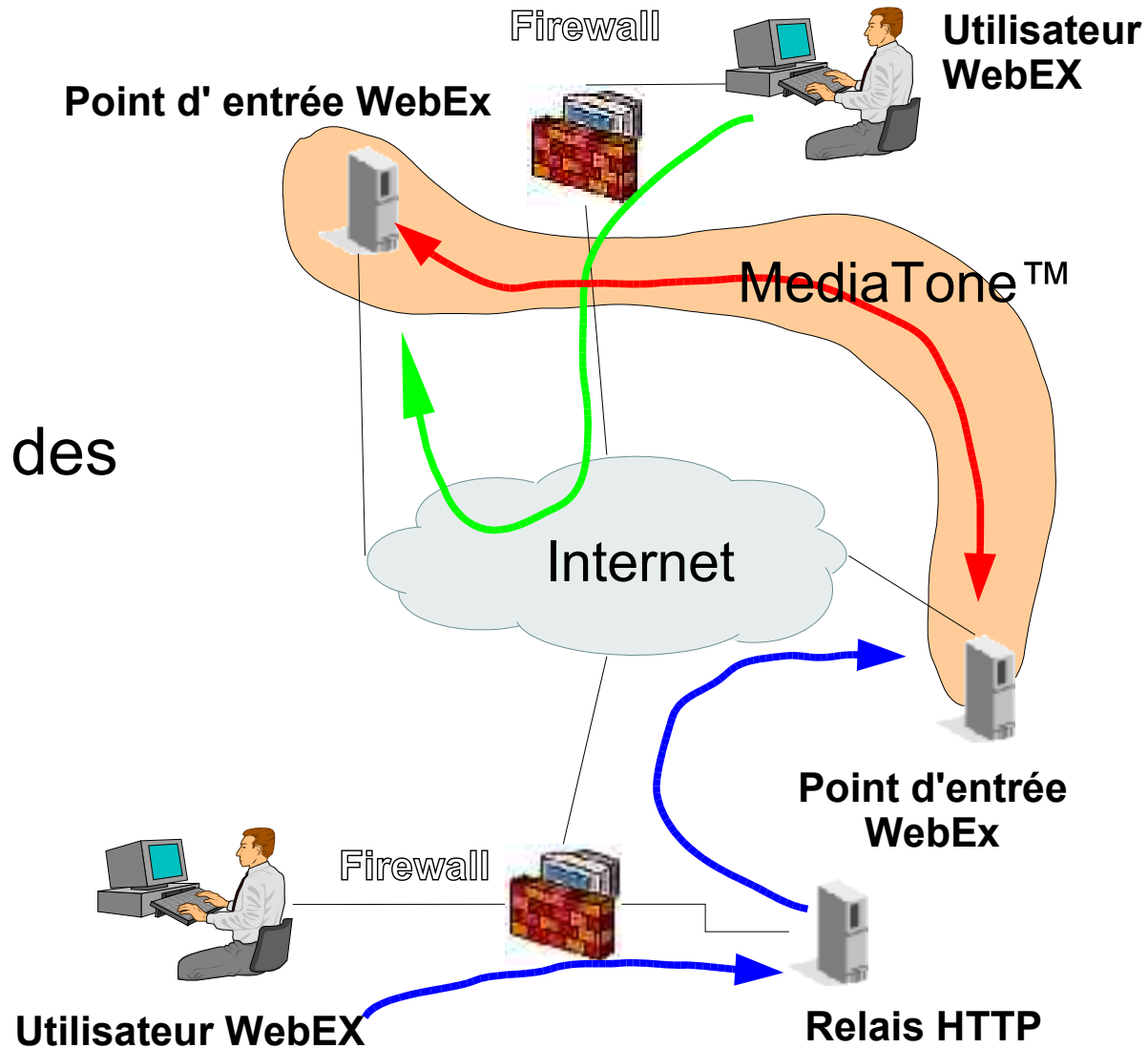
ISO TR 13335



- Infrastructures spontanées adaptées aux environnements sans gestion, sans contrôles et sans besoins spécifiques
 - Infogérées sans contrat de service
 - → **Utilisateurs grand public**
- Exemples à titre illustratif
 - WebEx
 - Beaucoup d'autres existent : InterWise, Genesys, MeetingOne, etc.
 - Skype
 - D'autres existent : Peerio
 - Alternatives libres existent : OpenWengo (neuf telecom)

- Pas médiatique
- Utilisé en entreprise
- Étudié par HSC en deux jours début 2005
- Windows : droits administrateurs à l'installation pour l'enregistrement du composant ActiveX
- MacOS & Linux : pas besoin de droits administrateurs (java)
- Un des participants doit avoir un compte sur le serveur web de WebEx
- Un des participants est maître de réunion, les autres sont élèves

- Réunions virtuelles
- Partage d'écran
- Partage d'application
- Prise de contrôle par l'un des participants
- Echanges : fichiers, messagerie instantanée
- Visioconférence



- Passage systématique par les serveurs web de WebEx
- Pas de chiffrement de bout en bout
 - HTTPS du poste de travail au serveur web de WebEx
 - Informations en clair sur les serveurs WebEx
- Pas d'authentification mutuelle entre participants
- Pas de journalisation
- Pas de limitation par participant, une fois le transfert de fichier accepté, c'est pour tous les participants

- Pas de demande de confirmation au participant lorsqu'un autre demande la configuration de son poste client

The screenshot shows a web browser window displaying a WebEx System Information page. The browser's address bar shows the URL: `https://supporttrial.webex.com/supporttrial/sc30/tool/docshow/support.php?Rnd=1299833045`. The page title is "System Information - Support Center".

On the left side of the page, there is a navigation menu with the following items: "System", "Hardware", "Browser" (which is selected and highlighted in blue), "Installed software", and "Running software".

The main content area displays a table of system information:

Item	Value
Browser Name	Microsoft Internet Explorer
Browser Version	6.0000
Java VM Version	
Proxy	Disabled
Proxy Override	10.*;192.70.106.*;synda.hsc.fr;hsc
Proxy Configuration	
Proxy Server	192.70.106.22:8080
Proxy By Pass	Yes
Intranet Name	Local intranet

At the top of the page, there is a search bar with the text "Search" and a "Favorites" button. Below the search bar, there are several icons for navigation and utility. The page also includes a "Refresh" button and an "Exit" button.

- Possibilité de journalisation des actions et échanges par l'éditeur
- Possibilités d'enregistrement par l'éditeur de tous les fichiers et données échangés
- Possibilités d'usurpation d'identité par l'éditeur
- Compromission d'un serveur de l'éditeur par un tiers compromettrait toutes les réunions dont il héberge un participant
 - Application en PHP

- Quiconque peut entrer dans une réunion avec le numéro de la session
 - Les n° de session sont incrémentaux
- Possibilité de prendre le contrôle de tout poste de travail utilisant WebEx
 - Potentiellement même sans être participant à sa réunion
- Possibilité de provoquer le lancement de WebEx par l'envoi d'un lien HTML sur lequel clique l'utilisateur

- Médiatique
- Sécurité de Skype pas une préoccupation des entreprises
- Jamais étudié par HSC, étudié par EADS CCR
- Pas besoin de droits administrateurs pour l'installation
- Acceptation par l'utilisateur de la prise de contrôle totale par Skype de son poste de travail
 - Ce dont cet utilisateur n'a pas forcément légalement le pouvoir
 - Usage apparent par Skype de ce pouvoir avec les supernodes
 - Pas besoin des droits d'administrateur
- Création d'un réseau poste à poste sur Internet
 - Supernodes permettent de gérer adresses IP dynamiques et traduction d'adresses

- Centralisation dans un annuaire de tous les utilisateurs ayant téléchargé Skype
- Journalisation possible des appels par l'éditeur
- Récupération possible des carnets d'adresses de chacun par l'éditeur

- Mécanisme de protection du code ne permettant pas de voir simplement ce que fait le logiciel
 - Justifié par l'éditeur par la nécessité de protéger son algorithme de compression de la voix
 - Facilite l'inclusion de code malveillant par l'éditeur
 - Complique l'étude du logiciel par des tiers
 - Arrête les curieux, une analyse sérieuse a contourné ce chiffrement
- Contrôle des postes de travail
 - Microsoft
 - Skype

- Chiffrement des échanges par un système propriétaire et méconnu
 - Possibilité d'écoutes et de détournement de communications par l'éditeur
 - Impossibilité d'appliquer la législation sur la journalisation des appels par l'opérateur
 - Difficultés ou impossibilité de réalisation des écoutes légales
 - Possibilité d'écoutes par celui qui possède une partie suffisamment longue de la clef secrète
 - Skype est européen
 - Skype racheté par Ebay
 - Autres candidats au rachat : Google, Microsoft, Yahoo

- Intégrez le PC d'entreprise comme élément qui est sur le périmètre du SI
 - Gardez la quarantaine, la lutte anti-virale, etc
 - Considérez les PC comme hors du réseau de confiance
 - Sauf les PC explicitement durcis ou les serveurs
 - Indépendamment du fait qu'ils soient fixes ou nomades
- Précisez explicitement dans sa politique de sécurité ses choix vis-à-vis des infrastructures spontanées
- Sensibilisez les utilisateurs
- Expliquez pourquoi une infogérance doit être explicite et contractualisée
- Filtrez les infrastructures spontanées avec votre protection périmétrique

- Infrastructures spontanées → **danger**
- PC sont sur le périmètre du SI
- Reprenez votre politique de sécurité
- Analysez explicitement les conséquences sur la sécurité
- Recherchez les infrastructures spontanées existantes
- Filtrez sur le périmètre

Questions ?

Herve.Schauer@hsc.fr

www.hsc.fr

- An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, Salman A. Baset & Henning Schulzrinne, 09/04
<http://arxiv.org/ftp/cs/papers/0412/0412017.pdf>
- VoIP and Skype Security, Simson L. Garfinkel, 01/05
<http://www.skypetips.internetvisitation.org/files/VoIP%20and%20Skype.pdf>
- Skype, Didier Benza, 03/05
<http://www-sop.inria.fr/semir/personnel/Didier.Benza/skype/skype.pdf>
- Les firewalls ne sont pas morts, Hervé Schauer, 05/05
<http://www.hsc.fr/ressources/presentations/jssi05-fw/>
- Skype uncovered, Fabrice Desclaux, EADS, 10/05
http://www.ossir.org/windows/supports/2005/2005-11-07/EADS-CCR_Fabrice
- Silver needle in the skype, Philippe Biondi, Fabrice Desclaux, EADS, 02/06
http://www.secdev.org/conf/skype_BHEU06.pdf

- Société de conseil en sécurité des systèmes d'information 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, BSI BS7799 Lead Auditor, LSTI ISO27001 Lead Auditor, IRCA, ProCSSI

- 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
 - ISO27001 / ISO17799
 - Sécurité de la voix sur IP
 - etc
- Sur **www.hsc-news.com** vous pourrez vous abonner à la **newsletter HSC**