Rapport de lecture

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	
Auteur	COMPAORE Harboure Hubert	
Année traitée	2004	

Résumé des points intéressants	
Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.

- Organisation
  - Prise en compte d'une unité de veille Technologique
  - Collaboration avec tout les autres équipes pour la réalisation du projet
  - Réalisation d'un planning clair
- Architecture
  - Architecture évolutive : différentes étapes qui permette à l'équipe attaque d'éprouver chaque architecture
  - Mise en place du « honey pot » par les équipes défense et analyse pour capter l'attention de l'équipe attaque.
- Système
  - Principalement Windows pour l'équipe défense
  - Windows et linux pour les équipes attaque et analyse
- Outils d'analyse :
  - Snifer
  - Snort
  - Back officer
  - Syslog
  - logwatch
- Méthodes d'attaque :
  - Usurpation d'identité : utilise la social engeniering pour avoir accès total à un système
  - Internet explorer : planter complètement la machine distante
  - Mail bombing
  - Spoofing DNS pour envoyer JPEG infecté…

Points à évoquer lors de la prochaine réunion	
Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Planification
- Comment maintenir la veille technologique

Rapport de lecture

Lecture des comptes rendus des années précédentes		
Rédigé le 26/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	
Auteur	Thomas Capraro	
Année traitée	2004	

Résumé des points intéressants	
Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.

- Attaque :
  - ARPSpoof
  - DNSSpoof
  - Outils pour avoir la cartographie du réseau :
    - Cheops Nessus Nmap Ettercap Ethereal ping traceroute
  - Mail Bombing
  - Génération d'un giga octets de logs pour noyer l'équipe audit sous une grosse charge de logs
  - FTP Bounce, surcharge de fichier sur le disque dur de la machine qui permet aussi de faire du bruit pour l'équipe audit

- Défense :
  - Mise en place d'une première infrastructure très simple et très peu sécurisé pour mettre en évidence les failles d'une architecture faible
  - 2eme architecture qui a pour but de représenter une architecture d'entreprise. Mise en place de VLAN.
  - Ajout d'un Firewall pour protéger les serveurs, et mise en place d'un pot de miel (honey pot) pour faire office d'appât.
  -

Points à évoquer lors de la prochaine réunion	
Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Niveau 1
  - Niveau 2

Rapport de lecture

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	
Auteur	Equipe attaque	
Année traitée	2005	
Résumé des points intéressants		
Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.	

➢ Organisation de l'équipe :

- 2 responsables
- Equipe découverte du réseau
- Equipe chargée de la diversion, génération de trafic, pollution et saturation du réseau
- Equipe exploit et renseignement sur les différentes failles de sécurité
- Equipe de flooding chargée de rendre inaccessible le réseau et usurpation d'identité

- Phase 1 : découverte du réseau
- Phase 2 : diversion, bruit de fond, analyse des logiciels utilisés
- Phase 3 : attaque par dénis de services et usurpation

➔ L'équipe a utilisée de façon très importante le social engineering pour obtenir certaines informations notamment l'accès à la messagerie interne.

➢ Découverte du réseau :

- Utilisation de divers outils : Tcpdump, Nmap, Scanrad, Amap, Atk, P0f, Netcat…
  - ➔ Penser à interdire le scan de ports et nettoyer le trafic en frontal
  - ➔ Etablir des règles de filtrage et limiteurs de connexions

➢ Attaque par dénis de services :

- Arp spoofing : utilisation de l'outil Arpspoof et Netcat

➢ Attaque par exploit :

- Utilisation importante de rootkit :
  - Metasploit : mise en place d'un shell à distance, accès VNC (injection d'un agent par dll)
  - HxDef : permet de cacher des fichiers, des process, des clefs de registre, des connexions… sur une station

➢ Attaque par diversion :

- Diverses attaques utilisées :
  - TCP Syn Flooding
  - Arp Spoofing
  - Mail Bombing
  - Saturation du réseau

Rapport de lecture

- Mail Bombing : Euthanasia 1.52, X-Mas 2000
- Flooders: Nemesis; MGen, Iperf, SynFlood

➔ Politique d'anti-spam à mettre en œuvre

Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Niveau 1
  - Niveau 2

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	
Auteur	Equipe audit	
Année traitée	2005	

Résumé des points intéressants	
Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.

Utilisation de scanner de vulnérabilités Nessus, du scnanner de ports Nmap, et de l'analyseur de trafic Snort / Acidlab (IDS)

Nessus : Vulnérabilités détectées au niveau du serveur FTP

Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Niveau 1
  - Niveau 2

Rapport de lecture

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	
Auteur	Equipe défense	
Année traitée	2005	
Résumé des points intéressants		
Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.	

- Services souhaités :
  - Mail
  - DNS
  - DHCP
  - Web
- Pare-feu : Netfilter (Debian)
- Politiques de sécurité :
  - Utilisation du réseau
  - Mail
  - Sécurité du routeur et des équipements
  - Sécurité des serveurs / pare-feu
- Serveur d'application distant (+ terminal server) pour alléger les clients
- Politique de mot de passe chiffré
- Limiter l'accès au réseau local : utilisation des adresses IP statiques et rejeter les adresses IP différentes.
  - ➔ PB : Si ces adresses sont connues des attaquants elles deviennent une menace en cas d'usurpation car elles sont déclarées comme étant de confiance.
- Ouvrir uniquement les ports nécessaires
- Empêcher les connexions entrantes et sortantes sur des services non autorisés
- Désactiver les commandes EXPN et VRFY pour les mails, qui peuvent fournir des informations intéressantes
- Mise en place d'un proxy web
- Changer le routeur en passerelle de niveau 2
- Changer les empreintes TCP/ IP grâce à l'outil Morph pour camoufler les OS utilisés lors d'un scan du réseau
- Mettre en place un système de leurre grâce à l'outil HoneyNet
- Routeur de type Cisco 2611 pour les règles *IP Advanced Services*
- Marquer les paquets de l'entreprise pour les règles de filtrage
- Les utilisateurs disposent d'un compte restreints en droits (impossible d'installer une application)
- Communication en Tunneling, chiffrée, entre les routeurs
- Utilisation de Fry et Leela comme serveurs DNS

Rapport de lecture

Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Mettre en place un système de messagerie interne pour palier au gestionnaire de projets mis en place par P. Latu. Ce dernier sera la cible d'inévitables tentatives d'attaques et d'intrusion. Un système de messagerie personnel pour la communication intragroupe semble plus sécurisé.

- Il existe certaines distributions linux qui une fois installées sur un support (CD, clé USB) permettent d'obtenir les mots de passe (même administrateurs) sur des stations de travail (Windows). Pour palier à ce problème il serait nécessaire de mettre en place une politique de sécurité autour des supports amovibles

- La supervision temps-réel du réseau est primordiale pour assurer l'intégrité du réseau et du parc informatique et ainsi détecter d'éventuelles intrusions (nouvelles stations sur le réseau…). Un système d'alarmes doit également être mis en place.

- Politique de certificats et signatures à mettre en œuvre pour certains services

Rapport de lecture

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	
Auteur	Wannes VOSSEN	
Année traitée	2006	

Résumé des points intéressants

Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.

- Il faut choisir un registre temporel pour la rédaction du rapport.
- Un contrat est établit avec l'équipe d'audit et en interne.
  - Divulgation de l'information interdite.
  - Nettoyage des postes après chaque utilisation.
  - Politique de mots de passes.
  - Politique de comptes rendus.
  - Toute demande d'informations de la part du groupe audit doit être formelle.
  - Un système de communication formelle à été mis en place. Des référents ont été désignés pour les communications internes et externes.
- Le projet se déroule en 3 Phases.
  - La phase 0 correspond à la période avant la première attaque.
  - La phase 1 correspond à la période après la première attaque.
  - …
- Un inventaire du matériel à été fait.
- Un espace de nommage des machines à été choisit. Ainsi qu'un plan d'adressage.
- Les mots de passe système ont été cryptés à l'aide de AES. (password encryption aes).
- Configuration de l'interface WAN du routeur en adresse « inside global » ?
- Mise en place de PAT à la place de NAT.
- Sécurisation de l'accès console et Telnet du routeur.
- Installation du module ModSecurity d'Apache pour pallier aux attaques de type wget (spam de formulaires)
- Blocage de la récursivité et du transfert de Zones DNS.
- Sécurisation du code PHP contre les Injections.
- Mise en place d'une politique de sécurité pour les utilisateurs
- Mise en place d'un système de sauvegarde.
- Informations recherchées par l'attaque
  - Adressage IP
  - Noms de domaine
  - Protocoles réseau
  - Services activés
  - Architecture des serveurs
- Utilisation des outils Nmap, Nessus et Saint par les attaquants.
- Mode d'attaque : Planification > Collecte d'informations > Balayage > Repérage des failles > Intrusion > Extension de privilèges > Compromission.
- Recours au DNS Spoofing (Ca à fonctionné). Pour éviter le DNS Spoofing, il faut des tables ARP Statiques.
- Nombreuses Attaques Web :
  - L'outil dirb scanne un serveur web par dictionnaire pour trouver des répertoires listables
  - L'attaque wget consiste à envoyer de nombreuses requêtes pour remplir la BDD. La solution est par exemple l'utilisation d'un Captcha.
  - Le XSS (Cross Site Scripting) consiste à insérer du javascript dans les formulaires. Le code s'exécute alors chez le client qui affiche le code précédemment entré dans le formulaire.
  - Il est possible grace à XSS de mettre en place des Keylogger Javascript.
  - L'injection SQL peut être solutionnée par l'utilisation de la fonction get_magic_quotes().
  -

Points à évoquer lors de la prochaine réunion

Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Nous devons choisir un nom pour notre groupe/société.

Rapport de lecture

- Location d'un nom de domaine. (Je propose l'utilisation de Google Apps)
- Sécurisation du BIOS par de mot de passe.
- Mise en place d'une réunion hebdomadaire (au moins).
- Les mots de passe doivent changer périodiquement. (Surtout avant chaque attaque officielle)
- En 2006, il à été fait usage des mots de passe Windows distribués lors du TP BDD. Il faut les changer !

Rapport de lecture

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	
Auteur	Jérémie BELMUDES	
Année traitée	2007	

Résumé des points intéressants	
Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.

- Défense
  - Architecture organisationnelle différente (communication, technique et politique de sécurité)
  - + politique de sécurité (livré en annexe de la défense 2007)
  - + contrat avec l'audit, réserve sur certaines clauses
  - Sécurisation progressive selon les jalons
  - – pas d'usage des services mandataires dès le départ
  - – telnetd en place jusqu'à l'intervention de l'audit
  - – DOS pendant les attaques
  - + bonne regles sur firewall
  - +méfiance vis-à-vis de l'equipe attaque
- Analyse
  - + grande communication
  - + étude de différentes méthodes d'analyse (Mehari choisie)
  - Mise en place d'une sonde selon le contrat avec la défense
  - installation d'une base de données mysql pour le fonctionnement de snort et acidbase
  - + étude des services inutiles pour une purge
  - Ntop, Hobbit ie BB4. pour visualisation de résultats de log
  - Analyse et compte rendu sur les logs
  - – DOS de la sonde
  - Nessus
  - pénétration réseau en faisant fi du pare-feu installé à l'aide des outils Firewalk et Itrace
  - + bonne regles sur firewall
  - trafic erroné détecté de diverses manières
  - contrat en PJ
- Attaque
  - + flooding icmp
  - attaque dictionnaire sur SSH
  - avec aide de la défense tentative d'injection de code dans une page PHP
  - récupération du site
  - bad_checksum portscan en bruit de fond
  - tentative d'injection de scripts CGI via VPN
  - flood sur port 80
  - attaque web debordement de pile
  - Les daemons mysqld, squid et spamd redémarré chez la défense
  - Equipe « diversion », « cartographie », « DOS », « force brute » et « exploit ».
  - Attaque DOS de divers types
  - récupération d'un compte gmail des analystes pour découverte de l'architecture défense
  - accès au réseau défense via une machine « zombie »
  - accès externe négatif (cause firewall)
  - usage de tracert pour découvrir l'architecture du réseau
  - découverte des services du réseau défense nmap & co
  - Test inefficace de winnuke (old win)
  - Test firewalk, Hping
  - Attaque Javascript, VBScript, rainbowtable, Trojan, arp via cain, bruteforce via brutus.

Points à évoquer lors de la prochaine réunion	
Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Pour communiquer en toute sécurité
  - Bonne réception de mon message ?
  - Chiffrement

Rapport de lecture

- Signature
- Password biométrique
- Clé RSA/Token
- Mise en place d'un système de communication

- Idées de services à mettre en place :
  - Wifi
  - Téléphonie IP
  - Visio conférence
  - Web 2.0, Service web
  - Hébergement web, SQL
  - Streaming
  - VLAN filliales
  - Bureau à distance
- Groupe système :
  - Veiller à utiliser des mandataires pour les services
  - OpenBSD, LinuxSE, Debian
  - Veille sur les failles des services
  - Reprise sur activité : outil de sauvegarde des disques
  - Cacher la bannière des services
- Groupe réseau :
  - Veille sur les failles des matériels, matériels virtuels…
  - Bien cacher l'archi des attaque par tracert, la bannière des OS…
- Groupe communication :
  - Ecrire des guides pour l'usage de OpenVPN
  - Prévoir un template de guide pour tous les services fournis
  - Faire un template pour toute communication dont le contrat avec l'audit
  - Etablir une charte / politique de sécurité
  - Prévention sur mot de passe, comptes mails et portail captif

Rapport de lecture

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite, toutes les informations intéressantes relatives au projet sécurité.	
Auteur	Cédric Harismendy	
Année traitée	2008	

Résumé des points intéressants	
Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.

- Gestion des échanges de documents
  - Mise en place d'un wiki sécurisé
  - Cryptage des documents
- Parc informatique : choix de l'utilisation de machines virtuelles
  - Remise en service rapide après incident
  - Limite le nombre de machines physiques à sécuriser
- Attaques utilisées :
  - ICMP Flooding
  - ARP Spoofing
  - IP Flooding
  - Mail Bombing
  - Mac Flooding
  - Attaques STP
  - Man in the middle
  - Social Engineering
  - Key loggers
  - Micro caché dans un PC
  - Pishing
  - Intrusions physiques type « femme de ménage »
  - Fake Caller ID
  - Virus, Trojan
  - Vol de sessions TCP
- Moyens de défense
  - NAT
  - ACL
  - VLAN
  - Définition de politiques de sécurité
  - Ghost (reprise d'activité)
  - Firewall
  - Antivirus
  - Supervision
  - VPN
  - Gestion des logs

Points à évoquer lors de la prochaine réunion	
Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Relation avec le groupe d'audit
  - Modalités de transmission d'information
  - Contrat (périmètre d'action, confidentialité etc.)
- Définition de l'architecture réseau
- Finalisation de l'organigramme

Rapport de lecture

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	
Auteur	Joseph Ndayra	
Année traitée	Analyse 2008	
Résumé des points intéressants		
Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.	

- Niveau organisation
  - On ne voit pas le rôle de chaque personne et le travail qui a réalisé

- Niveau technique
  - Très bien traité
  - La gestion du projet peut être beaucoup mieux
  - Manque d'un planning

- Niveau Présentation
  - Pas de table de figures

Points à évoquer lors de la prochaine réunion	
Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Définir le rôle de chaque personne
- Faire un planning
- Les premières idées pour la politique de défense

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	
Auteur	Joseph Ndayra	
Année traitée	Attaque 2008	
Résumé des points intéressants		
Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.	

- Niveau technique
  - Richesse dans les types d'attaque
  - Etude des vulnérabilités et collecte d'informations
  - Très bonne conduite de projet

- Niveau Présentation
  - Très complète et bien organisée au niveau du font et de la forme

Points à évoquer lors de la prochaine réunion	
Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Il faut prévoir une plateforme d'échange sécurisée, gmail le plus simple …

Lecture des comptes rendus des années précédentes		
Rédigé le 25/09/2010	Version : 1	Du le 27/09/2010
Description	Ce document à pour but de résumer, à l'aide des rapports disponibles à l'adresse http://www.linux-france.org/prj/inetdoc/securite , toutes les informations intéressantes relatives au projet sécurité.	

Rapport de lecture

Auteur	Joseph Ndayra
Année traitée	Défense 2008

Résumé des points intéressants

Description	Doivent figurer ici tous les points intéressants relevés lors de la lecture. Il peut s'agir de détails techniques, de menaces, de bonnes ou de mauvaises idées.

- Niveau communication
  - Ils disent « Après les réunions et les négociations avec l'équipe analyse, certaines modification ont étaient réalisées ». Serait il pas intéressent de mentionner ce qui a été modifier ? pourquoi …
- Niveau technique
  - Très bien traité
- Niveau Présentation
  - Pas de table de figures
  - Petite interrogation « est il normal que les annexe prennent 1/3 de la totalité du rapport »
  - La planification (Gantt) je pense que sa peut être beaucoup mieux

Points à évoquer lors de la prochaine réunion

Description	Doivent figurer ici les points les plus importants et qui doivent être traités lors de la réunion de lundi.

- Définir le rôle de chaque personne
- Faire un planning
- Les premières idées pour la politique de défense

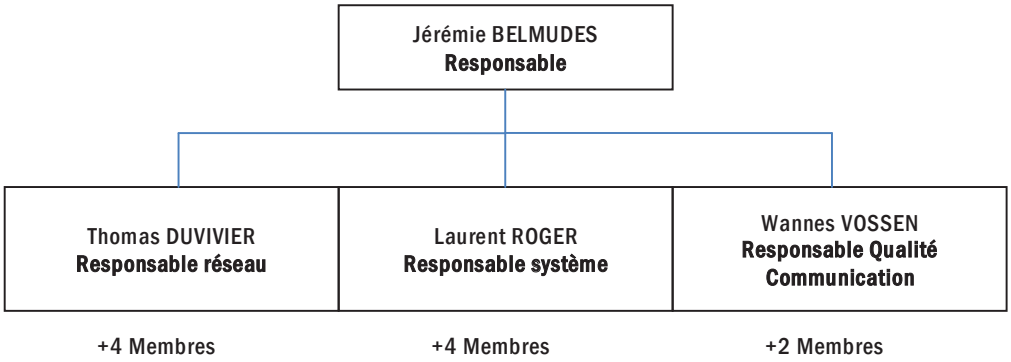
Compte rendu de réunion

Préparation de la séance de Travaux Pratiques du Lundi 27 Septembre 2010.			
24/09/2010	De 11:50 à 12:25		Bâtiment U3 Salle 2
Réunion organisée par	Le groupe Défense du projet Sécurité M2 STRI.		
Type de réunion	Réunion de planification, d'organisation.		
Animateurs	Jérémie BELMUDES, Julien DESVEAUX		
Version du document	1	Rédacteur	Wannes VOSSEN
Participants	Laurent ROGER, Cyrille DUMAS, Jérémie BELMUDES, Wannes VOSSEN, Julien DESVEAUX, Joseph NDAYRA, Nattapong TIWAPORNCHAROENCHAI, Mohamed BARRY, Thomas DUVIVIER, Raphaël DUJARDIN, Cédric HARISMENDY, Harboure HUBERT COMPAORE, Thomas CAPRARO		

Organisation et hiérarchisation du groupe sécurité

Conclusions	

L'organigramme suivant à été décidé par le groupe. Le choix de l'organisation s'est fait à l'unanimité et les responsables ont été élus à main levée. La répartition des autres membres du groupe reste à définir.



Répartition de la lecture des documents de l'année précédente

Conclusions	

Il à été décidé que chaque membre aurait à lire et à résumer – sous forme de points clés – les documents relatifs à une année. La répartition des lectures se trouve dans le tableau ci-dessous.

2004	Thomas C., Harboure Hubert
2005	Thomas D., Laurent
2006	Cyrille, Wannes
2007	Raphaël, Jérémie
2008	Cédric, Joseph
2009	Mohamed, Nattapong, Julien

Points d'action	Personne responsable	Délai à respecter
		27/09/2010

Mode de communication distante au cours du projet

Discussion	Il s'agit de savoir comment nous communiquerons, organiserons et partagerons nos connaissances tout au long du projet.
Conclusions	Nous utiliserons les listes de diffusion jusqu'à nouvel ordre. Le point reste à débattre et des solutions techniques doivent être envisagées.

Compte rendu de réunion

Réunion d'action			
30/09/2010	Début 09:45 Fin 11:00	U2 – Salle des machines	
Réunion organisée par	Jérémie Belmudes		
Type de réunion	Prise de décisions urgentes		
Animateur	Jérémie Belmudes		
Auteur du document	Wannes VOSSEN	Version	1
Participants	Laurent ROGER, Cyrille DUMAS, Jérémie BELMUDES, Wannes VOSSEN, Julien DESVEAUX, Nattapong TIWAPORNCHAROENCHAI, Thomas DUVIVIER, Thomas CAPRARO.		

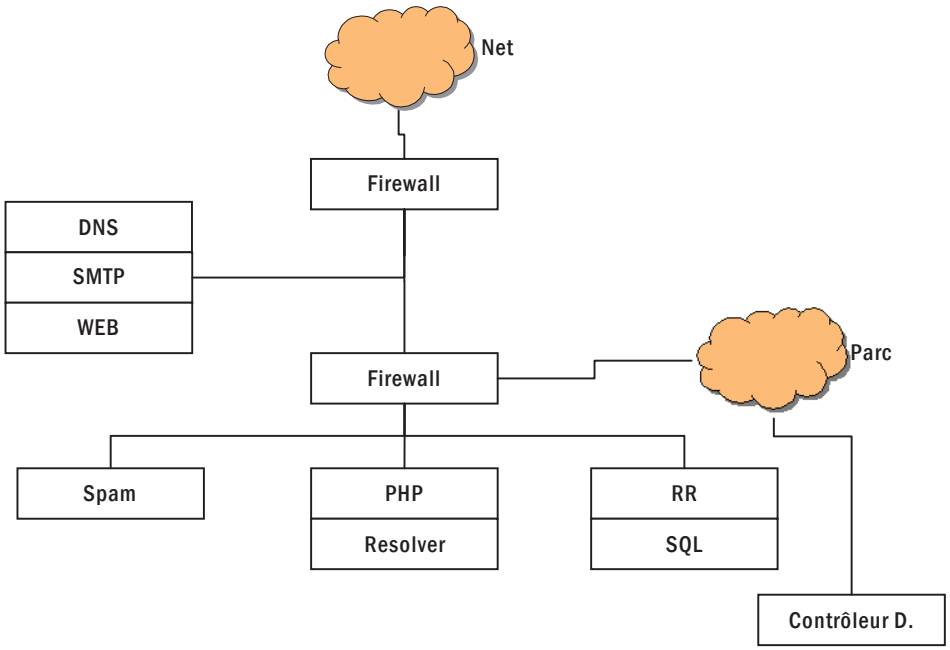
Délégation de taches au groupe Audit			
	Jérémie Belmudes		
Après discussions, il à été décidé que nous étions d'accord sur la délégation de l'ensemble des taches demandées par l'audit. Toutefois, les points suivants devront être détaillés dans le contrat : - L'accès du groupe audit à l'équipement frontal (Besoins de configuration) doit être strictement contrôlé. Nous pourrions exiger un guide d'intervention et effectuer la configuration en interne. - L'insertion du groupe audit dans le réseau reste à définir avec précision. La mise à disposition d'accès peut s'échelonner dans le temps.			
Conclusions	C'est au travers de l'appel d'offre que nous ferons transparaitre un partie des points discutés avec le groupe audit. Suite à leur réponse, nous devrons préciser les points ci-dessus dans le contrat.		
Points d'action		Personne responsable	Délai à respecter
Rédaction d'un appel d'offre			Urgent

Demande de confrontation du groupe Attaque			
[Temps imparti]	Jérémie Belmudes, Wannes Vossen		
Le groupe attaque nous à écrit sur notre liste de diffusion pour fixer une première confrontation le 11 octobre. Il s'agit de la date retenue par Ph. Latu et c'est aussi la date que nous avions arrêté lors de notre réunion hebdomadaire du 27 septembre.			
Conclusions	Nous décidons d'accepter cette date.		
Points d'action		Personne responsable	Délai à respecter
Envoi d'une réponse par email au groupe attaque, depuis le compte contact@aerodef.fr		Cyrille Dumas	48h

Réponse au groupe Audit			
[Temps imparti]	Wannes Vossen		
Le groupe Audit nous à demandé des adresses de contact. L'arrêt des mails cryptés a aussi été évoqué.			
Conclusions	Nous continuerons d'envoyer des mails cryptés et fournirons les adresses @aerodef.fr des responsables.		
Points d'action		Personne responsable	Délai à respecter
Envoie des adresses email @aeroef.fr de manière cryptée		Wannes	48h

Choix d'une architecture réseau	
[Temps imparti]	Thomas Duvivier
Nous avons 4 machines à notre disposition pour établir une architecture. Il serait intéressant d'avoir recours à une architecture 2 ou 3 tiers. Nous avons également la possibilité d'utiliser des machines virtuelles. Pédagogiquement, les machines virtuelles peuvent être présentées comme des machines réelles mais la virtualisation présente aussi des avantages qui doivent être étudiés. Le contrôleur de domaine sera hébergé sur une machine virtuelle de M. Galindo. L'architecture suivante à été retenue et validée.	

Compte rendu de réunion



Points d'action	Personne responsable	Délai à respecter
Mise en œuvre de l'architecture		Urgent

Compte rendu de réunion

Réunion de prise de contact entre l'Audit et la Défense		
28/09/2010	Début 10:15 Fin 10:35	Bâtiment U3
Réunion organisée par	L'Audit et la Défense	
Type de réunion	Prise de contact	
Participants	Maxime Viaud, Pierre-Michel Leboulch, Tristan Delgrange, Romain Lavernhe, Jérémie Belmudes, Julien Desveaux, Cyrille Dumas, Wannes Vossen.	

Communication entre les équipes

La communication et la prise de contact entre les deux équipes se fera au travers des responsables de la communication de chacun des groupes. Il s'agit des personnes présentes lors de la réunion, leurs adresses email seront échangées ultérieurement.
Toute communication par email devra se faire à l'aide d'une signature et d'une clé de chiffrement.
Un organigramme réduit pourra également être échangé entre les deux groupes.
Le compte rendu de réunion pour la présente réunion sera à la charge du groupe Défense.

Points d'action	Personne responsable	Délai à respecter
Echange d'adresses email	Bilatéral	

Délégation de taches du groupe Défense au groupe Audit

Les points suivants ont été évoqués et discutés. Toutefois, ils ne constituent en rien un engagement de l'un ou de l'autre des partis.

- Le groupe Audit aurait à charge la surveillance Système et Réseau.
- Le groupe Audit aurait la possibilité de positionner une machine sur le réseau de la Défense pour en effectuer la surveillance.
- Le groupe Audit aurait la possibilité d'installer des Plugins (Nagios) sur les équipements de la Défense pour en effectuer la surveillance.
- Le groupe Défense transmettrait au groupe Audit des informations quand à l'architecture physique et logique de son réseau. Le groupe audit pourrait alors émettre des conseils.
- Le groupe Défense communiquerait également ses politiques d'utilisation au groupe audit, dans le but d'en prendre conseil.
- Le groupe Audit pourrait avoir recours à des méthodes intrusives mais s'engagerait à ne causer aucun dégât.
- Le mode d'intervention du groupe Audit sur le système de la Défense doit être contractualisé. Ont été évoquées les possibilités de guide d'installation ou d'intervention directe.
- Le groupe Audit nécessiterait un accès sur l'équipement frontal pour mettre en place un système IPS. Il s'agit de modifier la configuration de l'équipement frontal.
- Si les contraintes techniques le permettent, le groupe Audit pourrait effectuer sa surveillance avant et après le pare-feu frontal.

Conclusions	Les deux groupes sont à priori tombés d'accord sur les points ci-dessus. Toutefois, rien ne peut être exigé avant contractualisation.

Contractualisation des accords

Les groupes Audit et Défense se sont mis d'accord sur la procédure suivante pour officialiser leurs accords :

- La Défense doit rédiger un appel d'offre.
- L'Audit doit répondre à cet appel d'offre (Une notion de coûts serait souhaitable).
- La Défense doit alors rédiger un contrat spécifiant les engagements des uns et des autres.

Points d'action	Personne responsable	Délai à respecter
Rédaction d'un appel d'offre	Groupe Défense	

Compte rendu de réunion

Réunion Hebdomadaire		
27/09/2010	Début 08 :00 Fin 12 :00	U2
Réunion organisée par	Le groupe Sécurité AeroDef	
Type de réunion	Réunion Hebdomadaire	
Animateur	Jérémie BELMUDES	
Secrétaire		
Participants	Laurent ROGER, Cyrille DUMAS, Jérémie BELMUDES, Wannes VOSSEN, Julien DESVEAUX, Joseph NDAYRA, Nattapong TIWAPORNCHAROENCHAI, Mohamed BARRY, Thomas DUVIVIER, Raphaël DUJARDIN, Cédric HARISMENDY, Harboure HUBERT COMPAORE, Thomas CAPRARO, TARRERIAS Frédéric	

Intervention de M. Latu	
	Philippe LATU

Il nous faut prévoir des paliers pour notre projet : commencer par un noyau minimum que l'on enrichit au fur et à mesure.
Puisque nous n'avons aucun moyen de contrôler l'accès physique, un point à ne pas négliger est la reprise d'activité. Un disque dur iSATA de 1 To est également mis à disposition pour les sauvegardes (Ghost par exemple). Nous pouvons toutefois crypter le disque dur et mettre un mot de passe au BIOS par exemple.
Pour réaliser notre architecture, nous disposons de 3 commutateurs (de niveau 3), de 2 routeurs CISCO et d'un Serveur. Il est également possible d'utiliser 3 machines dédiées supplémentaires et d'installer des machines virtuelles sur les postes de TP KVM + VDE (commutateur).
Le groupe Audit a fait la demande de travailler sur la ToIP. C'est une bonne idée de le leur déléguer, les routeurs ont des modules ToIP 4 ports PoE. C'est aussi une bonne idée de déléguer la partie identification des flux au dessus de la couche transport. En tout cas, il est important d'éviter la redondance entre Audit et Défense.
Coté Parc, nous disposerons très probablement d'une licence XP et d'une licence 7. Il est intéressant de caractériser la différence et par exemple de négliger la maintenance du poste XP.
Coté mobilité, nous avons à disposition un point d'accès Wi-Fi autonome (DHCP) et suffisant dans le cadre de notre projet. Le Wi-Fi peut être délégué ou gardé pour la fin du projet.
Pour nous, le groupe Défense, la recherche doit se faire en parallèle au déploiement de services. Il faut garder un équilibre entre sécurité et utilisation. L'axe important à suivre est la continuité de service.

Conclusions	Première confrontation prévue pour le 11 Octobre, la suivante pour le 25 Octobre. La dernière confrontation aura lieu le 15 Novembre.

Compte rendu de lecture des rapports	
[Temps imparti]	Jérémie BELMUDES

La liste de diffusion n'est pas un moyen de communication sécurisé…
Les attaques suivantes ont fonctionnées les années précédentes :

- ARP Spoofing
- DNS Spoofing
- Le « Social Engeneering » est le principal danger !

Il est possible d'utiliser des emails signés. Cette solution est à étudier.
Il est possible d'utiliser des mots de passe/alertes SMS. Cette solution est à étudier.

Conclusions	Gare aux mots de passes redondants et aux boites mail.

Points d'action	Personne responsable	Délai à respecter
Choix d'un nouveau mode de communication : Google Apps.	Joseph Ndayra	28/09/2010
Etude des possibilités en termes de signature email et des solutions SMS	Groupe Système	04/10/2010

Mots de passe sur ntelline	
[Temps imparti]	Jérémie BELMUDES

Les mots de passe de ntelline ont circulé en clair lors du TP Base de données.

Conclusions	Pas d'utilisation de comptes mail, FTP ou autres sur ntelline.

Choix d'un nom / nom de domaine pour la société	
[Temps imparti]	Jérémie BELMUDES

Il s'agira d'une société de prestations informatiques dans le domaine de l'aéronautique. Le nom retenu pour la société est AeroDef. Le nom de domaine aerodef.fr à été adopté.
Evocation d'une technique anti-keylogger, cette technique ne sera pas décrite ici pour des raisons de sécurité.
Evocation d'une politique de mots de passe : Chacun doit avoir un mot de passe dédié au projet. Le mot de passe doit être raisonnablement sécurisé. Le stockage centralisé des mots de passe à également été évoqué.
Toujours dans le contexte d'une société de service, il serait intéressant d'un point de vue pédagogique d'estimer un coût de mise en œuvre pour notre architecture.

Conclusions	AeroDef aura pour nom de domaine aerodef.fr

Compte rendu de réunion

Points d'action	Personne responsable	Délai à respecter
Réservation du nom domaine aerodef.fr	Wannes VOSSEN et Thomas DUVIVIER	Immédiat
Utilisation de la technique anti-keylogger sur tout poste public	Groupe Défense	Immédiat
Utilisation de mots de passes dédiés au projet. Changement périodique des Mots de passe.	Groupe Défense	Immédiat

Choix des services à mettre en place

[Temps imparti]	Jérémie BELMUDES

Les services suivants constituent une liste non exhaustive des services pouvant être mis en place :

- ToIP : Délégué Audit.
- Supervision : Délégué Audit.
- Visio
- Web/2.0/Webservices : Urgent
- Base de données SQL
- Service de streaming
- VLAN
- Bureau à distance
- DNS : Urgent
- Mail : Urgent
- FTP
- VPN : Urgent et en partie fait
- LDAP
- Virtualisation
- SSH : Urgent
- Service de Stockage
- Service de Sauvegarde

Conclusions	Les services Urgents doivent être mis en place avant la première confrontation.

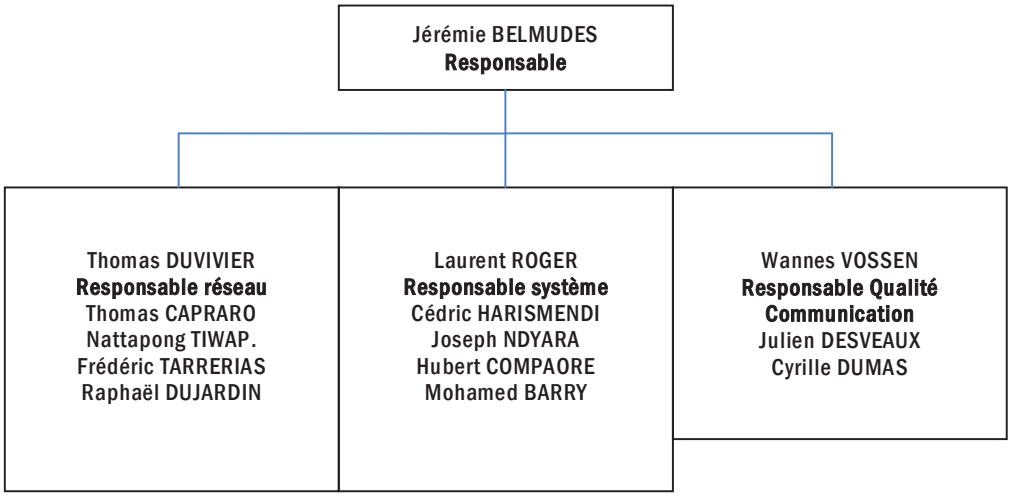
Points d'action	Personne responsable	Délai à respecter
Le groupe architecture est chargé de l'intégration de ces services dans la future architecture.	Thomas DUVIVIER	04/10/2010

Complément d'information organisationnelle

[Temps imparti]	Jérémie BELMUDES

Un compte rendu de réunion devra être rédigé pour chaque réunion. Chaque intervention technique devra donner lieu à un rapport d'activité. Pour uniformiser ces documents, des Modèles de documents doivent être conçus au plus tôt.
Une réunion Hebdomadaire est un strict minimum pour une bonne communication dans le groupe.
A l'extérieur de notre groupe, toute information technique dois circuler de manière officielle : c'est-à-dire à travers un document.
Une politique de sécurité devra être rédigée. Elle concernera à la fois les utilisateurs du système et les professionnels informatiques que nous sommes.
Un annuaire d'entreprise peut être mis en ligne. Cette option doit être étudiée.
Une liste de Noms/Prénoms/Email/Téléphone doit être diffusée.
La répartition des taches à également été complétée par rapport à la précédente réunion. A présent, l'organigramme est le suivant :

Compte rendu de réunion



Conclusions	La prudence est de mise quand aux communications avec les autres groupes.

Points d'action	Personne responsable	Délai à respecter
Mise en place d'une politique de sécurité	Cyrille DUMAS	04/10/2010
Rédaction d'un compte rendu de la réunion	Wannes VOSSEN	27/09/2010
Diffusion des informations de contact de tous les membres du groupe	Julien DESVEAUX	27/09/2010
Prochaine réunion Hebdomadaire le 04/10/2010	Groupe Sécurité	04/10/2010

Objectifs pour le 04/10/2010

[Temps imparti]	Jérémie BELMUDES

Les objectifs suivants ont été posés pour les différentes équipes

- Archi : Inventaire des équipements, architecture 3 tiers, Veille Cisco/Pare-feu
- Communication : Rédaction de templates, rédaction de contrats, charte de sécurisation, politique de sécurité, feuille de contact.
- Système : Etude DNS, SMTP, http, SSH, Etude des systèmes de mots de passe, de Google Apps et de l'OS Debian

Compte rendu de réunion

Micro-réunion de mise au point			
18/10/2010	Début 08:30 Fin 08:45	U2-212	
Réunion organisée par	Jérémie BELMUDES		
Type de réunion	Mise au point		
Animateur	Jérémie BELMUDES		
Auteur du document	Wannes VOSSEN	Version	1.0
Participants	Laurent ROGER, Jérémie BELMUDES, Wannes VOSSEN, Julien DESVEAUX, Joseph NDAYRA, Nattapong TIWAPORNCHAROENCHAI, Mohamed BARRY, Thomas DUVIVIER, Raphaël DUJARDIN, Cédric HARISMENDY, Thomas CAPRARO.		
Avancement Système			
[Temps imparti]	Laurent Roger		
- Postfix est en cours, Joseph y a travaillé ce weekend. - Le cloisonnement n'est pas pour tout de suite car compliqué : il faut recompiler le noyau. - Un serveur DHCP doit être mis en place sur le contrôleur de domaine.			
Conclusions	Nous allons essayer de mettre en place un système stable d'ici la seconde confrontation. Nous ne ferons donc qu'optimiser l'existant.		
Points d'action		Personne responsable	Délai à respecter
Mise en place d'un serveur DHCP sur le contrôleur de domaine.		Système	25/10/2010
Mise en place du serveur Postfix sur Zeus.		Système	25/10/2010
Avancement Architecture			
[Temps imparti]	Thomas Duvivier		
- L'inventaire est terminé. - Est-il vraiment nécessaire de toucher aux VLAN alors que ceux-ci fonctionnent ? - L'Audit souhaite mélanger les VLAN Parc et ToIP. A étudier.			
Conclusions	Pour le moment nous ne toucherons pas aux VLAN. Comme pour le système, nous allons optimiser pour la prochaine confrontation.		
Avancement Communication			
[Temps imparti]	Wannes Vossen		
- Espace sécurisé Utilisateur / Admin en place. - Contrat quasiment finalisé et à signer aujourd'hui. - Il faut centrer le site aeroDef.fr sur Internet Explorer. - Nous avons, suite à cette réunion, toutes les informations pour répondre au groupe Audit.			
Conclusions	La signature du contrat est l'élément le plus urgent.		
Points d'action		Personne responsable	Délai à respecter
Espace dynamique du site web		Communication	25/10/2010
Finaliser le contrat		Communication	18/10/2010
Centrer AeroDef.fr sur Internet Explorer		Communication	20/10/2010
Objectif principal			
[Temps imparti]	Jérémie Belmudes		
Conclusions	Le système doit être prêt pour la seconde confrontation d'ici vendredi.		

Compte rendu de réunion

Débriefing de la première confrontation			
13/10/2010	Début 12 :00 Fin 12 :30	U3	
Réunion organisée par	Jérémie Belmudes		
Type de réunion	Réunion de mise au point		
Animateur	Jérémie Belumdes		
Auteur du document	Wannes VOSSEN	Version	
Participants	Laurent ROGER, Cyrille DUMAS, Jérémie BELMUDES, Wannes VOSSEN, Julien DESVEAUX, Joseph NDAYRA, Nattapong TIWAPORNCHAROENCHAI, Thomas DUVIVIER.		

Etat d'avancement Architecture	
[Temps imparti]	Thomas Duvivier

Avant la confrontation, Nattapong avait mis en place un pare-feu basique. Le matin de la confrontation, Ph. Latu à déployé un pare-feu « state-full » plus avancé.
Les VLAN posent problème pour l'intégration du groupe Audit dans notre architecture. Acutellement, l'Audit à son propre VLAN et passe par le pare-feu pour atteindre tous les autres réseaux. Les VLAN sont à repenser pour faciliter l'intégration de l'audit.
De manière à partager toute l'information architecturale, une série de tableaux devraient décrire, entre autres, les éléments suivants :

- VLANs et ports correspondants.
- Utilisation des IPs dans le réseau.
- Translation des ports sur le routeur (NAT).

Conclusions	Après signature du contrat, le groupe audit bénéficiera d'une confiance totale. Un travail documentaire permettra plus d'autonomie dans les différents groupes.

Points d'action	Personne responsable	Délai à respecter
Restructurer l'architecture VLAN	Architecture	
Faire un inventaire (cartographie) de l'architecture.	Architecture	

Etat d'avancement Système	
[Temps imparti]	Laurent Roger

Les services suivants sont en place :

- SFTP.
- MySQL/PHP
- Apache
- Postfix (A revoir)
- DNS
- Active Directory

Il est à noter que suite à la confrontation, les machines client sont vérolées. La décision à été prise de les reformater.

Conclusions	Nous n'allons pas étendre nos services pour le moment mais nous concentrer sur leur sécurisation.

Points d'action	Personne responsable	Délai à respecter
Reformater/Réinstaller les machines client.	Système	
Vérifier si le boot CD au démarrage est désactivé pour les deux postes client.	Système	
Sécurisation de tous les services	Système	
Prévoir un moyen de réinstallation rapide des machines/serveurs	Système	
Prévoir un système de Sauvegarde	Système	

Conclusions de la confrontation	
[Temps imparti]	Jérémie Belmudes

- Le routeur était en mode Debug, ce qui à eu pour conséquence de le saturer. En mode Debug, le routeur affiche toutes les requêtes qui lui parviennent. Cela est consommateur de ressources.
- Un DNS Spoof a été réussi. Plusieurs solutions sont possibles. L'utilisation de serveurs mandataires est un début mais cette solution n'empêche pas le problème. L'authentification des réponses DNS est à étudier.
- L'attaque par virus dans le fichier PDF à été contenue: En plus d'avoir installé une vielle version d'Adobe Reader, nous avons du désactiver l'antivirus et ouvrir la session administrateur pour que cette attaque réussisse. Il n'y a donc pas de mesures à prendre à ce niveau là.

Conclusions	L'attaque DNS à réussie, nous devons empêcher qu'elle ne se reproduise. L'attaque Virus à été contenue.

Points d'action	Personne	Délai à

Compte rendu de réunion

	responsable	respecter
Empêcher le DNS Spoofing	Système	Prochaine Confrontation

Compte rendu de réunion

Réunion de mise au Point avec Ph. Latu			
11/10/2010	Début 08:30 Fin Heure de fin 08:55	U2	
Réunion organisée par	Ph. Latu		
Type de réunion	Mise au point avant confrontation		
Animateur	Ph. Latu		
Auteur du document	Wannes VOSSEN	Version	1.0
Participants	Laurent ROGER, Cyrille DUMAS, Jérémie BELMUDES, Wannes VOSSEN, Julien DESVEAUX, Thomas DUVIVIER, Philippe Latu.		

Services actifs pour la première confrontation

[Temps imparti]	Ph. Latu

Les services suivants sont actifs sur le serveur :

- SSH
- SFTP
- DNS (Pas sur)
- Apache
- Php/Mysql (Non utilisé)

Conseil: Lancer les logs pour tous les services.

Conclusions	La priorité est d'avoir du trafic sortant pour les postes client.

Difficultés d'accès au serveur (VPN) le Weekend dernier

[Temps imparti]	Jérémie Belmudes

Le délai était très important : 20 secondes pour taper un caractère.
Selon Ph. Latu, le groupe Audit aurait « lancé un truc carrément borderline » et aurait perdu le contrôle par la suite.

Conclusions	La surcharge était donc justifiée, cela ne devrait pas se reproduire. Il n'y a donc pas d'action à envisager.

Surveillance des Systèmes

[Temps imparti]	Laurent Roger

Pour surveiller le serveur, il faut utiliser des services console (La serie TOP). Nous avons :

- ApacheTop
- AIOTop (Pour les accès disque)
- HTOP
- MySQL Tuner

L'avantage de ces services c'est qu'ils ne consomment que très peu de ressources sur le serveur ainsi que très peu de ressources réseau.

Conclusions	Les outils TOP sont une bonne solution pour avoir un état instantané du serveur.

Points d'action	Personne responsable	Délai à respecter
Mettre en place la surveillance système avec les outils xTOP	Système	

Interaction avec l'Audit

[Temps imparti]	Ph. Latu

Dans l'immédiat, l'Audit va se concentrer sur l'analyse de traffic (Port SPAN).
Par la suite, il est souhaitable de leur déverser tous nos logs système + Cisco (Netflow).

Conclusions	Les logs Netflow ayant été délégués dans la matinée, il reste à déléguer les logs système.

Points d'action	Personne responsable	Délai à respecter
Mettre en place la délégation des logs système	Système	Etendu.

Compte rendu de réunion

Réunion hebdomadaire 2			
04/10/2010	Début 08 :15 Fin 10 :00	U2 – 213	
Réunion organisée par	Le groupe Défense		
Type de réunion	Réunion Hebdomadaire		
Animateur	Julien Desveaux		
Auteur du document	Wannes Vossen	Version	1.0
Participants	Laurent ROGER, Cyrille DUMAS, Jérémie BELMUDES, Wannes VOSSEN, Julien DESVEAUX, Joseph NDAYRA, Nattapong TIWAPORNCHAROENCHAI, Mohamed BARRY, Thomas DUVIVIER, Raphaël DUJARDIN, Cédric HARISMENDY, Harboure HUBERT COMPAORE, Thomas CAPRARO, TARRERIAS Frédéric.		

Intervention de Ph. Latu	
[Temps imparti]	Philippe Latu

Deux options nous sont offertes pour la gestion des adresses.

- Simuler une plage d'adresses publiques avant notre réseau et faire du NAT au niveau du deuxième routeur.
- Avoir recours au NAT sur notre routeur frontal.

Dans tous les cas, 172.16.99.0/29 serait notre @ publique virtuelle.

Concernant notre architecture, il nous faut procéder par étapes. Nous n'aurons certainement pas le temps de mettre en place notre choix d'architecture en 1 semaine. De plus, notre représentation de l'architecture (schéma) est dépassée.

Le plus long dans le déploiement de notre système sera probablement la partie Système. Ce peut être une bonne idée d'avoir recours à un déploiement réseau moyennant des images binaires. C'est un plus pour la reprise. Ghost est à écarter d'avance puisque ce système n'est plus d'actualité avec 2008 Server et Windows 7. Il y a quand même un aspect pédagogique dans ce projet qui veut que l'on déploie des technologies susceptibles de revenir en entreprise. Dans le cadre précis des déploiements d'images, qui est un secteur en mouvement, il peut être intéressant de faire une petite analyse des différentes offres.

Sinon, pour faire simple, on peut utiliser ImageX sur Cooper et déployer a l'aide d'un CD bootable.

Question virtualisation, Ph. Latu nous déconseille VMWare, parce que nous risquerions dêtre frustrés sur la partie réseau incomplète. comme alternative, il y a deux outils valables : VDE et OpenVSwitch.org. Les postes de TP sont tout à fait valables pour la virtualisation (Ils ont le fameux bit à 1).

Mais la virtualisation peut être complexe à mettre en place en 1 semaine. On peut donc aussi faire du cloisonnement. Chroot est très couteux en temps d'administration mais des réglages simples, comme la consomation processeur des processus peut être pratiques et faciles à mettre en place. Les Containers et Jails sont de bonnes solutions. Ces solutions sont celles utilisées dans les hébergements mutualisés bon marché.

Pour des questions de délais toujours, on va s'en tenir à une archi à deux paliers.

- Palier 1 : Tous les services DNS Apache PHP et MySQL sur un même serveur, avec cloisonnement si le temps le permet. Nous n'aurions qu'un seul routeur frontal et utiliserions des VLAN pour séparer les le réseau serveur et le parc. le contrôleur de domaine pourrait se trouver sur une machine physiquement.
- Palier 2 : Sortir le cache DNS, PHP et MySQL du serveur initial et mettre ces services en retrait pour aboutir à une archi 2 tiers.

Nous n'aurions à priori pas le temps de de faire une véritable découpe 3 tiers en ce projet. C'est-à-dire que nous n'aurions pas le temps de séparer MySQL (Database) de la couche middleware. MySQL serait d'ailleurs le premier problème de sécurité tout au long du projet.

Il faudra enfin faire du tuning pour sécuriser/optimiser nos systèmes :

- Sur PHP il n'y a pas grand-chose à régler.
- Apache est assez autonome, sauf gros tuning à faire sur les pre-fork et les mpm.
- MySQL à un cache extrêmement fluide jusqu'à 95% d'utilisation. Après, le service est fortement dégradé. Il ne faudra jamais dépasser ce seuil.

Conclusions	Dans l'immédiat, nous utiliserons un NAT frontal pour la gestion des adresses. Nous nous en tiendrons également au Palier 1 de l'architecture Latu avec des containers et du cloisonnement.

Compte rendu de la semaine passée	
[Temps imparti]	Julien Desveaux

Conclusions Système :

- L'étude du cryptage aboutit sur les conclusions suivantes : le cryptage de mails avec clé asymétriques est très difficile à mettre en œuvre, particulièrement quand les communications ont plusieurs destinataires. Il est bien plus simple d'avoir recours à un cryptage symétrique
- La signature des emails est assez simple à mettre en place.
- Les systèmes de notification par SMS fonctionnent par abonnement et sont liés à de solutions logicielles très spécifiques pour lesquels il faut une licence.
- Les méthodes de cryptage de systèmes de fichier sont envisageables et même assez simples à

Compte rendu de réunion

mettre en œuvre sous Debian. - L'utilisation d'une clé pour crypter un système de fichier est également envisageable même si un peu plus compliqué. Dans le principe, il faudrait un code PIN sur la clé pour se protéger de sa perte. Conclusions Architecture : - L'architecture ayant été remise en cause dans cette réunion, il faut la faire évoluer au plus vite. - L'inventaire des équipements n'a pas encore été fait, mais cela ne saurait tarder. Conclusions Communication - La politique de sécurité à été rédigée par Cyrille. - Les contrats avec le groupe Audit ont été rédigés par Julien. - De manière à uniformiser les documents, il est demandé à ceux qui ne parviennent pas à mettre en forme d'envoyer la source (.docx) à l'adresse communication@aerodef.fr pour remise en forme.	
Conclusions	Il nous faut nous dépêcher de mettre en place un système minimal dans un délais de 1 semaine. Le SMS est rejeté. Le cryptage peut être envisagé pour les emails utilisateur, ainsi que la signature. Le cryptage de systèmes de fichiers sans USB est à faire au plus tôt.

Points d'action	Personne responsable	Délai à respecter
Lecture de la Politique de sécurité	Tout le monde	48h
Mettre à jour les documents en accord avec la charte graphique (se référer au modèle compte rendu de réunion)	Tout le monde	
Cryptage des systèmes de fichiers.	Système	11 Octobre
Déploiement de l'architecture Latu Palier 1	Architecture	11 Octobre
Déploiement du système Latu Palier 1	Système	11 Octobre

Réunion informelle avec le groupe Audit	
[Temps imparti]	[Présentateur]
Réunion informelle raide pour discuter les appels d'offre. Ils ne les avaient pas reçus (Tristan étant malade) et nous les présentons donc sur place. Le seul commentaire c'est que la « supervision » n'inclut pas forcément la détection d'intrusion. Mais nous sommes d'accord sur le fait que le groupe audit fera de la détection d'intrusion.	

Appel d'offres

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Supervision du parc informatique : systèmes et réseaux	
Avis d'appel public à la concurrence fictif	
Département	31 (Haute-Garonne)
Date de parution	3/10/2010
Date de péremption	7/10/2010
Année	2010

Nom et adresse fictifs de l'organisme acheteur :
SAD/DSI/SI : Société AeroDef, Direction du Système d'Information, Service Communication.
Correspondant : VOSSEN Wannes Université Paul Sabatier, Bât U3, IUP STRI, 118 route de Narbonne, 31062 Toulouse Cedex 9 tél. : 06-46-31-63-02

Objet du marché :
Supervision du parc informatique : systèmes et réseaux.

Lieu d'exécution :
Local de l'Université Paul Sabatier U2.

Caractéristiques principales :
Quantités (fournitures et services), nature et étendue (travaux) : Etude de la sécurité (humaine et technique) du système d'information (petite taille, peu de services) de l'agence mère de la société AeroDef avec installation et configuration d'équipements et de logiciels nécessaires à la surveillance du trafic réseau.

Forme juridique que devra revêtir le groupement d'opérateurs économiques attributaire du marché :
Il est interdit aux candidats de présenter plusieurs offres en agissant à la fois : (a) en qualité de candidats individuels et de membres d'un ou plusieurs groupements ; (b) en qualité de membres de plusieurs groupements.
L'exécution du marché est soumise à d'autres conditions particulières : le marché débutera à compter de la notification du contrat jusqu'au 30/11/2011.

Langues pouvant être utilisées dans l'offre ou la candidature :
Français et Anglais.

Unité monétaire utilisée :
L'euro fictif (€f).

Conditions de participation :
Situation juridique - références requises :
Déclaration du candidat - renseignements de l'entreprise, situation fiscale, sociale, capital social, chiffre d'affaires, renseignements particuliers à un marché, moyens du candidat, références, qualification et certification.
Qualification de l'entreprise :
Le soumissionnaire indiquera son positionnement par rapport aux normes ISO d'assurance qualité. Il fournira les éventuels certificats qualité délivrés par l'afaq ou tout autre organisme. Il fournira de préférence une liste de références similaires aux prestations demandées.
Qualification des intervenants :
Le soumissionnaire devra préciser le niveau de qualification des intervenants et indiquera : Le niveau de certification délivré par les constructeurs pour chaque type d'équipement concerné. La composition de l'équipe de réalisation et la qualification des principaux intervenants (CV) s'il le souhaite. Certification fictive « Secret Def STRI » requise pour garantir la confidentialité des données partagées vis à vis de AeroDef et ses clients.

Critères d'attribution :
Offre économiquement la plus avantageuse appréciée en fonction des critères énoncés ci-dessous avec leur pondération :
- prix des prestations : 20 % ;
- valeur technique : 45 % ;
- conduite de projet et maintenance : 35 %.

Aucune enchère électronique ne sera effectuée.

Appel d'offres

Type de procédure :
Procédure négociée.

Date limite de réception des offres :
7 octobre 2010, à 12 heures.

Durée de marché ou délai d'exécution :
2 mois à compter de la publication de cette offre.

Informations complémentaires :
Conformément à la législation française, l'ouverture des offres n'est pas publique. Dématérialisation des procédures : l'organisme acheteur préconise la transmission des plis par voie électronique. Il accepte cependant les plis adressés par d'autres moyens permettant d'en garantir la confidentialité et la date de réception. Le fuseau horaire de référence sera celui de (Gmt+01:00) Paris, Bruxelles, Copenhague, Madrid. Tout document non PDF ou contenant un virus informatique fera l'objet d'un archivage de sécurité et sera réputé n'avoir jamais été reçu. Il est conseillé aux candidats de soumettre leurs documents à un anti-virus avant envoi.

Date d'envoi du présent avis à la publication :
2 octobre 2010.

Adresse auprès de laquelle des renseignements d'ordre technique peuvent être obtenus (pour toute question) :
communication@aerodef.fr

Adresse à laquelle les offres/candidatures/demandes de participation doivent être envoyées :
wannes.vossen@aerodef.fr

Classe d'Activité :

Classe	Description de la classe d'activité
72	Services informatiques

Appel d'offres

Fourniture, installation et configuration sécurisée d'équipements et logiciels de communication pour la mise en œuvre de la téléphonie sur IP sur deux postes informatiques	
Avis d'appel public à la concurrence fictif	
Département	31 (Haute-Garonne)
Date de parution	3/10/2010
Date de péremption	20/10/2010
Année	2010

Nom et adresse de l'organisme acheteur :
SAD/DSI/SI : Société AeroDef, Direction du Système d'Information, Service Communication.
Correspondant : VOSSEN Wannes Université Paul Sabatier, Bât U3, IUP STRI, 118 route de Narbonne, 31062 Toulouse Cedex 9 tél. : 06-46-31-63-02

Objet du marché :
Fourniture, installation et de la configuration sécurisée d'équipements et logiciels de communication pour la mise en œuvre de la téléphonie sur IP sur deux postes informatiques.

Lieu d'exécution :
Local de l'Université Paul Sabatier U2.

Lieu de livraison :
Local de l'Université Paul Sabatier U2.

Caractéristiques principales :
Quantités (fournitures et services), nature et étendue (travaux) : fourniture des téléphones (hard ou soft), installation et configuration sécurisée d'équipements et logiciels de communication pour la mise en œuvre de la téléphonie sur IP sur deux postes informatiques.
Evaluation de la métrologie et du coût pour un déploiement à plus grande échelle sur les agences de la région (40 postes).

Forme juridique que devra revêtir le groupement d'opérateurs économiques attributaire du marché :
Il est interdit aux candidats de présenter plusieurs offres en agissant à la fois : (a) en qualité de candidats individuels et de membres d'un ou plusieurs groupements ; (b) en qualité de membres de plusieurs groupements.
L'exécution du marché est soumise à d'autres conditions particulières : le marché débutera à compter de la notification du contrat jusqu'au 30/11/2011.

Langues pouvant être utilisées dans l'offre ou la candidature :
Français et Anglais.

Unité monétaire utilisée :
L'euro fictif (€f).

Conditions de participation :
Situation juridique - références requises :
Déclaration du candidat - renseignements de l'entreprise, situation fiscale, sociale, capital social, chiffre d'affaires, renseignements particuliers à un marché, moyens du candidat, références, qualification et certification.
Qualification de l'entreprise :
Le soumissionnaire indiquera son positionnement par rapport aux normes ISO d'assurance qualité. Il fournira les éventuels certificats qualité délivrés par l'afaq ou tout autre organisme. Il fournira de préférence une liste de références similaires aux prestations demandées.
Qualification des intervenants :
Le soumissionnaire devra préciser le niveau de qualification des intervenants et indiquera : Le niveau de certification délivré par les constructeurs pour chaque type d'équipement concerné. La composition de l'équipe de réalisation et la qualification des principaux intervenants (CV) s'il le souhaite. Certification fictive « Secret

Appel d'offres

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

Def STRI » requise pour garantir la confidentialité des données partagées vis à vis de AeroDef et ses clients.

Critères d'attribution :
Offre économiquement la plus avantageuse appréciée en fonction des critères énoncés ci-dessous avec leur pondération :
- prix des prestations : 10 % ;
- valeur technique : 50 % ;
- conduite de projet et maintenance : 40 %.
Aucune enchère électronique ne sera effectuée.

Type de procédure :
Procédure négociée.

Date limite de réception des offres :
20 octobre 2010, à 12 heures.

Durée de marché ou délai d'exécution :
2 mois à compter de la publication de cette offre.

Informations complémentaires :
Conformément à la législation française, l'ouverture des offres n'est pas publique. Dématérialisation des procédures : l'organisme acheteur préconise la transmission des plis par voie électronique. Il accepte cependant les plis adressés par d'autres moyens permettant d'en garantir la confidentialité et la date de réception. Le fuseau horaire de référence sera celui de (Gmt+01:00) Paris, Bruxelles, Copenhague, Madrid. Tout document non PDF ou contenant un virus informatique fera l'objet d'un archivage de sécurité et sera réputé n'avoir jamais été reçu. Il est conseillé aux candidats de soumettre leurs documents à un anti-virus avant envoi.

Date d'envoi du présent avis à la publication :
3 octobre 2010.

Adresse auprès de laquelle des renseignements d'ordre technique peuvent être obtenus (pour toute question) :
communication@aerodef.fr

Adresse à laquelle les offres/candidatures/demandes de participation doivent être envoyées :
wannes.vossen@aerodef.fr

Classe d'Activité :

Classe	Description de la classe d'activité
72	Services informatiques

Contrat de prestation de service

La société d'audit Assurancetourix France au capital de 1€, ayant son siège social

À Toulouse, prise en la personne de M.

(fonctions),

Ci-après dénommé le Prestataire,

Et

La société Aerodef au captital de 4 020 123 €, ayant son siège social

À Castanet Tolosan, prise en la personne la personne de M.

Belmudes Jérémie

Chef de projet,

Ci-après dénommé le Client,

S'engagent à respecter scrupuleusement le contrat de prestation de service suivant.

Objet du contrat :

Dans le cadre du déploiement et de la sécurisation du système d'information d'une grande entreprise du secteur aéronautique, le Client, ayant été choisi pour la réalisation de ce projet, a décidé de faire appel à un prestataire de services : le Prestataire. Cette dernière va se décliner en deux volets : la supervision système et réseau et le déploiement de la téléphonie sur IP.

Article 1 – Partage des informations :

D'un côté, le Client s'engage à fournir les pièces nécessaires à la réalisation des tâches confiées au Prestataire suivantes:

- Les informations sur l'architecture physique et logique du système d'information :
    - Un schéma détaillé de l'architecture physique et logique du système d'information.
    - Les adresses IP correspondantes NAT/PAT.
    - Les services utilisés avec correspondance des ports.
    - Le schéma complet depuis le VPN du Prestataire vers l'infrastructure du Client.

  Le Prestataire pourra conseiller le Client en termes d'amélioration à ce sujet.
- Une copie des fichiers de configuration pour certains équipements. Ce partage se fera au cas par cas selon les besoins du Prestataire et les informations que le Client sera prêt à partager.
- La politique d'utilisation des équipements.
- Un organigramme de la société.
- La charte utilisateur du Client.
- La politique de sécurité du Client ?
-

D'un autre côté le Prestataire s'engage à fournir au Client :

- Un guide d'installation, d'utilisation et de gestion des pannes rencontrées de tous les outils et équipements utilisés par le Prestataire et appartenant au Client.
- Une trace de toutes les modifications effectuées sur les équipements du Client.
- Tous les scripts de configuration valides utilisés sur les équipements du Client.
- Un compte rendu hebdomadaire de l'activité système et réseau sauf si le Client a du retard dans la livraison au Prestataire des informations nécessaires à ce travail.
- Un organigramme de sa société.

Les deux parties s'engagent à fournir les pièces ci-dessus dans un délais d'une semaine suivant la signature du contrat.

Tous les documents, fichiers ou travaux produits par le Prestataire, dans le cadre de la prestation de service et à destination du Client, sont exploitables librement et sans limite de temps par le Client. Cet accès concerne donc tous les documents que le Prestataire partage avec le Client comme listé ci-dessus.

Toutes interventions sur les équipements du Client devront être au préalable validées par les responsables techniques du Client. Ces dernières devront également être tracées par écrit et faite en présence d'un responsable technique du Client.

Le Client s'engage à informer le Prestataire de tout changement ou évolution dans les documents ou les équipements. Le Client garanti que le Prestataire sera prévenu au minimum 24h avant de possibles coupures volontaires (du Client) dans l'accès au système d'information et l'informera de la raison générale entrainant cette coupure.

Article 2 – Clause de confidentialité :

Le Prestataire s'engage à ne divulguer aucune information à un tiers ayant un quelconque lien avec le Client, que ce dernier l'ai partagée avec lui ou non. Si tel était le cas le Prestataire assumera l'entière responsabilité d'une telle divulgation en dédommageant le Client pour les informations, le temps et les ressources financières perdues.

Il en est de même pour le Client concernant les documents que le Prestataire lui aurait transmis.

Article 3 – Moyens mis à disposition au Prestataire pour la supervision et utilisation de ces moyens

Dans le cadre de la supervision, faite par le Prestataire, le Client s'engage à mettre à disposition du Prestataire les éléments suivants :

- Un accès au réseau du grand groupe travaillant dans l'aéronautique afin que le Prestataire puisse y installer une machine de surveillance du réseau.
- Un accès aux équipements.

Ces deux accès permettront uniquement au Prestataire d'implanter les outils Nessus, Netflow, FAN (Fully Automated Nagios), de travailler sur la gestion de logs générés par le réseau et de faire de l'analyse complémentaire.

- Un accès à l'équipement pare-feu frontal du réseau :
    - Afin d'y mettre en place un système IPS (Système de prévention d'intrusion) et IDS (Système de détection d'intrusion) en vue de modifier la configuration de l'équipement.
    - Afin de placer deux postes de surveillance : un avant et un après l'équipement. Ce point sera possible si les contraintes techniques le permettent, en fait si le pare-feu est capable de le supporter.
- Un accès VPN pour configurer à distance leur serveur, les équipements ToIP (Téléphonie sur IP).

Utilisant les différents accès, le Prestataire pourra faire des tests intrusifs sur le réseau afin d'en tester sa robustesse mais s'engage à ne faire aucun dégât. Chacun de ces tests sera daté et validé par les deux parties et un compte rendu les concernant sera produit par le Prestataire.

Le Client autorise le Prestataire à mettre en œuvre tous les procédés énoncés dans la réponse à l'appel d'offre. Cette dernière figure en annexe de ce contrat.

Article 5 – Frais

Le Client s'engage à couvrir l'ensemble des frais en Euros fictifs que le Prestataire a fait passer dans son appel d'offre mis à part la prise en charge des frais de restauration et de pauses cafés, c'est à dire 59 600€f. Les frais de restauration et de pauses café du Prestataire seront donc à la charge de ce dernier.

Article 6 – Communication

Toute communication entre les deux parties se fera en priorité à travers les services communication respectifs. Cette dernière se fera par email mais en utilisant une signature numérique et une clé de chiffrement.

Les communications d'ordre technique pourront se faire directement entre les personnes compétentes. Ces personnes seront désignées par chacune des parties. L'utilisation de signatures numériques et de clés de chiffrement reste obligatoire. Les employés du Client ne souhaitant pas avoir recours à ce type de sécurité pourront transiter par l'adresse contact@aerodef.fr. Cela implique donc un délai supplémentaire.

Les deux parties s'engagent à accuser réception des différentes requêtes de l'autre partie dans un délai de 24h maximum. Les deux parties auront un délai de 72h pour établir une réponse technique. Toutefois, si ce délai ne peut être respecté, le retardataire s'engage à informer l'autre partie 24h avant la fin du délai.

Article 7 – Modification du contrat

Toute modification de ce contrat devra se faire par un avenant au contrat signé par les deux parties.

Tout manquement dans l'engagement d'une des parties devra être reconnu par écrit.

Toulouse, le
Signatures précédées de « lu et approuvé » :

Assurancetourix :	AeroDef :
Tristan Delgrange	Jérémie Belmudes

AeroDef.fr
CONSULTANTS EN AÉRONAUTIQUE

POLITIQUE DE SECURITE DE L'INFORMATION

MATERIEL, PERIPHERIQUES ET EQUIPEMENTS DIVERS

L'intégrité physique des installations informatique doit être considérée comme perpétuellement compromise.

Voici une liste non exhaustive d'actions qui devront être déployées de manière à limiter l'impact d'un accès physique :

- Limiter l'accès aux informations à l'intérieur des machines. (Ex : mots de passe BIOS, cryptage du système de fichier, cadenas…).
- Mettre fin à tout privilège avant de s'éloigner d'une machine.
- Mettre en place une stratégie résistante de reprise d'activité en cas de détérioration physique ou logicielle des matériels.
- Mettre en place une méthode de surveillance des machines connectées au réseau interne.
- Vérifier la présence de keyloggers, micros, caméras ou tout autre périphérique pouvant compromettre la sécurité.

TRAVAIL EN DEHORS DE LOCAUX DE L'ORGANISATION ET UTILISATION DE PERSONNEL EXTERNE

Il est interdit de communiquer une quelconque information concernant le système d'information à des personnes extérieures à l'entreprise. Toutefois, la sécurité du système ne peut reposer sur une éventuelle méconnaissance de ces informations.

Toute communication d'informations à d'éventuels intervenants externes habilités doit se faire de manière contrôlée et doit être officialisée par écrit.

Toute prise de contact avec un tiers doit passer par le groupe de communication ou par le responsable du projet.

L'utilisation d'ordinateurs publics n'est pas prohibée mais doit être réduite au strict minimum. Dans le cas d'une telle utilisation, il est de la responsabilité de l'utilisateur de ne pas laisser trace de son passage (mots de passe enregistrés, sessions ouvertes…).

Les périphériques (Téléphones, Clés USB,…) ne disposant pas de contrôle d'accès ou de cryptage doivent être considérés comme des ordinateurs publics.

Il est interdit de travailler sur un réseau sans-fil non crypté.

CONTROLE DE L'ACCES AUX SYSTEMES D'INFORMATION ET AUX CONTENUS QUI Y SONT PRESENTS

Le système d'information de l'entreprise étant connecté à Internet, aucun document ou fichier y circulant ne peut être considéré comme fiable. Lorsque l'utilisateur utilise un fichier, renseigne un mot de passe ou valide une action du système, celui-ci est responsable des conséquences éventuelles de ses actes.

Tout document fournit par un intervenant (Client, Fournisseur, …) externe à l'entreprise doit être traité avec grande précaution. Les précautions suivantes peuvent notamment être prises :

- Exécution sans privilèges.
- Utilisation d'un antivirus.

Tout mot de passé doit respecter les contraintes suivantes: Le mot de passe doit comporter au minimum huit caractères dont des chiffres, des lettres (majuscules et minuscules) ainsi que des caractères spéciaux. Exemple : AQ40gp69 !

TRAITEMENT DE L'INFORMATION

De manière à minimiser le risque de failles logicielles, seuls les services utiles à la production devront être activés sur les machines.

De manière à minimiser la dépendance du système à un nombre réduit d'intervenants, ceux-ci doivent partager l'information au travers de listes, d'emails ou de notes de service.

De manière à minimiser les pertes de données, un système de sauvegarde des données métier doit être mis en place.

L'utilisation d'antivirus est obligatoire sur les postes de travail. Leur désactivation est interdite.

Tout logiciel du système d'information doit être systématiquement mis à jour. Si pour une raison exceptionnelles de compatibilité ou de licence, la mise à jour est impossible, une défense en profondeur doit être mise en place.

MESSAGERIE ELECTRONIQUE ET ACCES INTERNET/INTRANET/EXTRANET

Toute transmission d'informations sensibles relative au projet doit se faire :

- Soit de vive voix et à l'abri des oreilles indiscrètes.
- Soit à l'aide de la plateforme GoogleApps.

Le mot de passe GoogleApps est un élément clé de la sécurité du système d'informations. Ce mot de passe ne peut être :

- Utilisé pour un autre système ou compte de messagerie.
- Communiqué à qui que ce soit.
- stocké ou noté en clair.
- Avoir un niveau de sécurité en dessous de « Fort » sur GoogleApps.

Les responsables peuvent, à tout moment, demander le changement des mots de passe. Chacun doit alors spécifier un nouveau mot de passe respectant les règles précédemment évoquées.

La liste de diffusion est considérée comme un moyen de communication non fiable. Toutefois, le mot de passe de la liste de diffusion ne peut être celui par défaut.

REMARQUES

Cette politique de sécurité cherche un équilibre entre faible contrainte et sécurité élevée. Plutôt que de transgresser une règle énoncée dans ce document, vous pouvez adressez vos remarques à communication@aerodef.fr.