Université Paul Sabatier
TOULOUSE III

STRI
| Télécoms & Réseaux |

Candide S.A

Projet
Sécurité des SI

Groupe Défense – Novembre 2009

Contributeurs :

AMOUZOU Guillaume	BONIN Nathanaël	GILLET Micaël
ARIBAUD Julien	CHEYNIER Pierre	GOUZY Kévin
AVERSENC Nicolas	CROUZAT Florian	MOUTON-DUBOSC Vincent
BERARD David	DINARQUE Sylvie	XAVIER Mathieu
BLAIZE Raphaël	DEROUINAU Marion	

Table des matières

Introduction

Afin de rapprocher l'enseignement de **sécurité des systèmes d'information** d'un contexte d'entreprise, l'ensemble des étudiants se sont vus attribuer un rôle et une équipe de travail visant à aborder de manière concrète certaines problématiques propres à la sécurisation et au maintien de la disponibilité d'une infrastructure de SI.
L'entreprise Candide S.A. constitue une entreprise fictive représentant un cas d'exploitation typique. Cette société se place dans un contexte de sous-traitance d'une industrie convoitée, manipulant des informations à forte valeur ajoutée, et dépendant fortement de son système d'information pour sa crédibilité et sa pérennité.
Notre promotion étant composée de 42 étudiants, plusieurs groupes d'intérêts ont été formés :

- **Groupe Défense** : Il constitue l'entreprise Candide S.A. qui déploie une architecture *sécurisée* et propose un ensemble de services à ses utilisateurs et au réseau public ;
- **Groupe Audit** : Ce groupe constitue une entreprise agissant en étroite collaboration avec la société Candide S.A., en permettant de superviser le réseau et de prévenir certains risques et attaques ;
- **Groupe Attaque** : Collectif *anonyme* de personnes ayant pour objectifs d'infiltrer et de compromettre l'entreprise Candide S.A., afin de rendre indisponible tout ou partie du système d'information.

Le projet s'est effectué en une série de **trois confrontations** (rencontre durant lesquelles le groupe attaque déroulait chacun de ses scénarios préalablement définis), la granularité du niveau de sécurité devant augmenter progressivement dans le temps, mais également en fonction des préconisations et des conséquences des attaques précédentes. Afin de mettre en œuvre notre architecture, certains équipements présents dans la salle U2-213 ont été mis à notre disposition.
Ce document s'attachera à détailler l'organisation fonctionnelle et technique de l'entreprise dans un premier temps. La seconde partie nous permettra ensuite d'aborder une vision constructive basée sur l'analyse de différentes thématiques mais également sur les impacts recensés. Enfin, les grands principes de la sécurisation d'un système d'information seront approchés afin d'en dégager des préconisations d'ordre conceptuel ainsi que des retours sur expérience.

I. Présentation organisationnelle

Afin de s'approcher le plus possible d'un contexte professionnel, nous avons mis en place - *à priori* - un découpage métier présenté sur l'organigramme suivant :

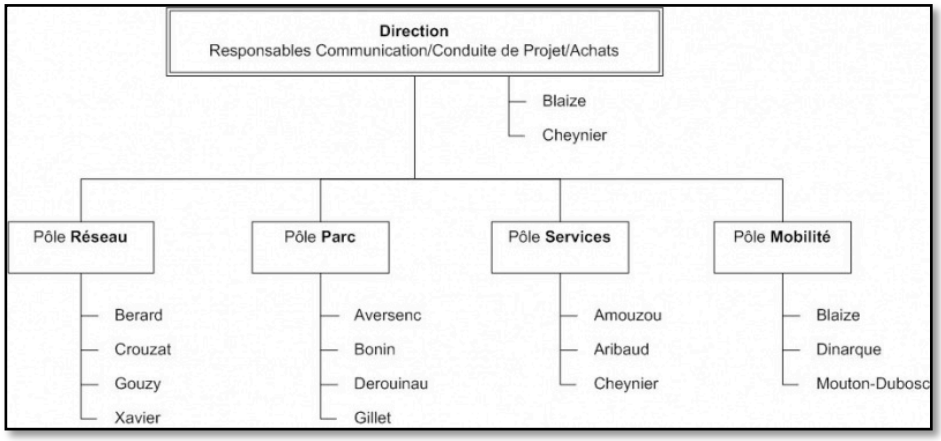

Figure 1 *: Organigramme de la société Candide S.A.*

Les membres du groupe sont divisés en **cinq pôles** distincts dont les rôles respectifs sont explicités ci-après.

1. Groupes

Direction

- Collecte des informations relatives aux différentes thématiques ;
- Rédaction des comptes-rendus d'activités ;
- Planification et priorisation d'activités ;
- Vis-à-vis de la société d'Audit :
  - Gestion des aspects contractuels ;
  - Interface de communication privilégiée : au quotidien pour informations et synchronisation d'activités, mais aussi pour l'émission d'alertes et de comptes-rendus d'audit par le prestataire.

Réseau

- Étudier les besoins et déduire les schémas d'interconnexion ;
- Mettre en œuvre cette interconnexion :
  - Par l'installation et la configuration des équipements d'interconnexion à disposition ;
  - Par la configuration des différents équipements terminaux ;
- Maintenir et permettre l'évolution de la solution proposée ;
- Renforcer la sécurité de celle-ci sur préconisation.

Les principaux thèmes qui ont pu être abordés sont les suivants : Configuration des équipements d'interconnexion, Adressage IP, VLAN, Routage et Filtrage.

Services

- Offrir les éléments de communication active et passive de la société :
  - Portail Web collaboratif ;
  - Mise en œuvre du service de messagerie.
- Proposer et mettre en œuvre la sécurisation de la partie applicative ;
- Définir une charte d'utilisation des ressources informatiques (préconisations au niveau des usages).

Les principaux thèmes qui ont pu être abordés sont les suivants : Services Web & Ftp, Serveurs et Relais de messagerie, Politiques de sécurité applicative.

Parc

- Définir les ressources système nécessaires pour répondre au besoin, en termes de services ;
- Mettre en place les équipements terminaux et définir les éléments de sécurisation à apporter à ceux-ci ;
- Concevoir et mettre en œuvre un plan de reprise d'activité :
  - Par la sauvegarde et la synchronisation des configurations.
- Mettre en œuvre le service de communication sur l'ensemble du domaine ;
- Permettre au prestataire d'auditer en temps réel le fonctionnement de l'ensemble des systèmes (logs).

Les principaux thèmes qui ont pu être abordés sont les suivants : Configuration des différents OS, développement système, configuration des modules système, virtualisation, sauvegarde et synchronisation, DNS, Active Directory W2k3 Server, Logs.

Mobilité

- Mise en œuvre de solutions d'accès distant et mobile ;
- Gestion de l'impact d'un parc client en situation de mobilité :
  - Préconisations réseau et système afin d'éviter la régression du niveau de sécurité.

Les principaux thèmes qui ont pu être abordés sont les suivants : VPN, Wifi et Usages de clients "nomades", Étude d'impacts.

Au fur et à mesure de l'avancée du projet, il s'est vite avéré que **le besoin en ressources était plus important dans certains groupes**. Par conséquent, le cloisonnement défini ci-dessus a rapidement été mis en défaut. L'ensemble des participants a effectué diverses missions contribuant au bon développement de l'infrastructure.

2. Répartition des membres

Nous décrivons ci-dessous les membres actifs ainsi que les services et développements auxquels ils ont contribué, suite à la modification des groupes décrite précédemment :

- **Filtrage & Routage, VPN** : David BERARD ;
- **Développement, Base de Données, Web, FTP** : Pierre CHEYNIER, Sylvie DINARQUE, Nathanaël BONIN, Florian CROUZAT, Vincent MOUTON-DUBOSC, Mathieu XAVIER ;
- **Virtualisation & Parc** : Micaël GILLET, Kevin GOUZY, David BERARD, Marion DEROUINAU ;

- **Mobilité & Wifi** : Vincent MOUTON-DUBOSC ;
- **Sauvegardes** : Nathanaël BONIN, Sylvie DINARQUE, Nicolas AVERSENC, Florian CROUZAT ;
- **Mails & DNS** : Nathanaël BONIN, Pierre CHEYNIER, Florian CROUZAT, David BERARD ;
- **Contacts avec le groupe Audit** : Raphaël BLAIZE, Pierre CHEYNIER, Sylvie DINARQUE ;
- **Rédactionnel Projet** : Nathanaël BONIN, David BERARD, Pierre CHEYNIER, Florian CROUZAT, Sylvie DINARQUE ;
- **Édition du support oral** : Nicolas AVERSENC, Marion DEROUINAU, Kevin GOUZY, Mathieu XAVIER.

3. Planification du projet

Le déroulement des différentes étapes, les confrontations avec le groupe Attaque ainsi que les différentes réunions que nous avons pu tenir avec le coordinateur du projet, M. Latu, sont décrites dans le diagramme de GANTT ci-dessous :

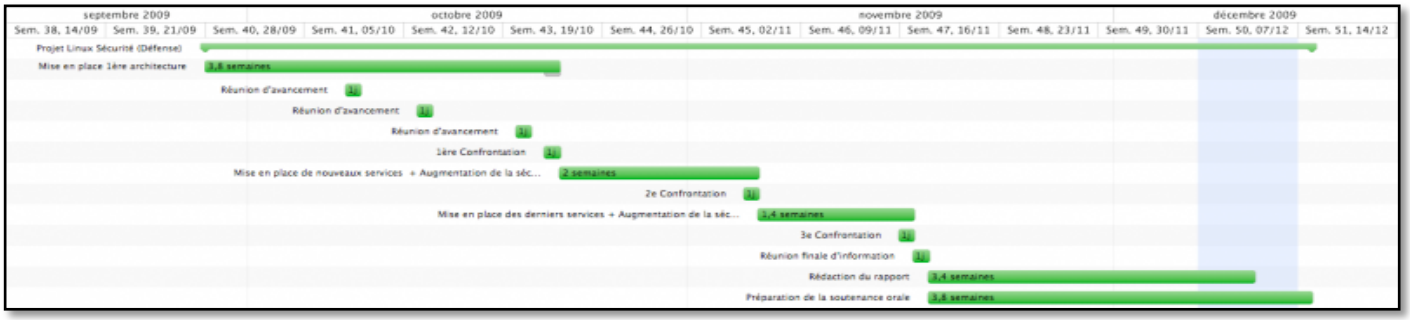

Figure 2 *: Diagramme de Gantt*

Seules les grandes étapes de la réalisation de l'infrastructure y sont mentionnées.

II. Architecture Technique

1. Contraintes

Lors du déroulement du projet, nous avons été confrontés à des problèmes ne reflétant pas un cas d'utilisation professionnel réel. Par exemple, l'extinction de nos machines tous les soirs nous a empêché d'être alerté d'un **downtime** d'un des serveurs (puisque celui-ci était déjà éteint!) le temps que l'équipe audit fasse une copie du disque.
Récapitulatif des contraintes rencontrées :

- Salle de TP :
  - Discontinuité de la disponibilité des serveurs (ne reflète en **aucun** cas la réalité) ;
  - Accès physique simple au matériel par les autres équipes (ceci justifiant le chiffrement des partitions avec LVM Luks).
  - Premier niveau de firewall/proxy, mutualisant les flux sur une seule source IP, ce qui a mis en défaut notre politique de filtrage par listes noires.

- Distant :
  - Configuration du VPN changeante côté UPS, nous forçant à remonter le tunnel persistant et à modifier la configuration du firewall.

2. Schéma de l'infrastructure

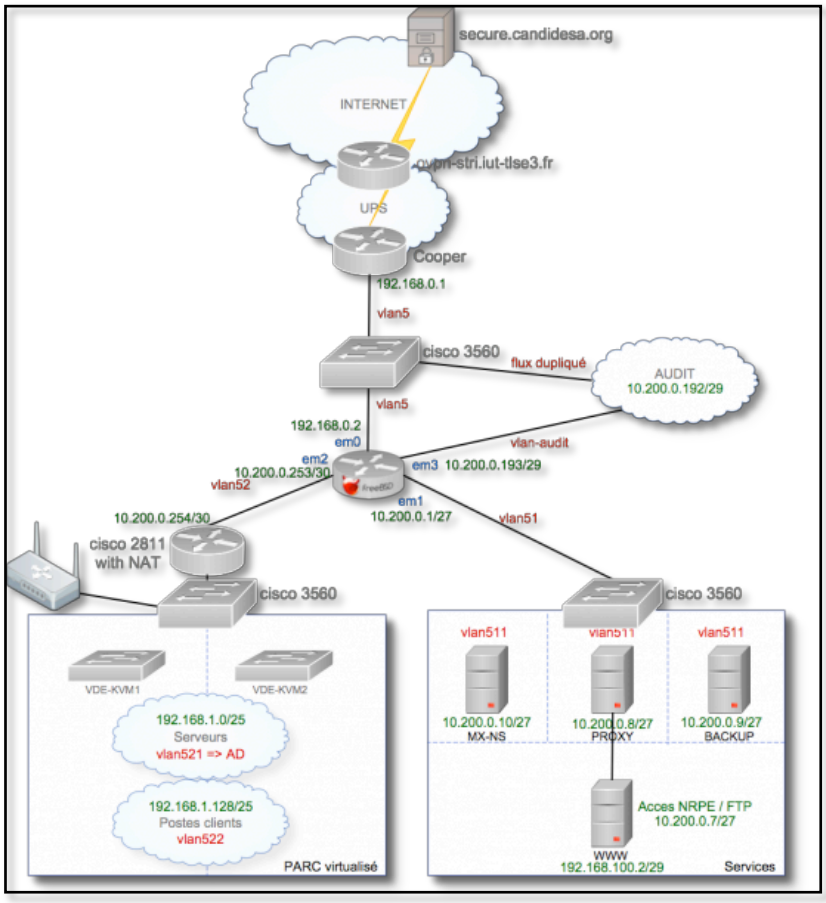

Figure 3 *: Infrastructure de l'entreprise Candide S.A.*

3. Éléments techniques propres à l'infrastructure

- Découpage en VLANs ;
- Routage OSPF vis-à-vis du réseau "public" (correspondant au reste des salles de TP) ;
- Simulation d'une utilisation d'adressage public pour les services, découpage d'une classe d'adresse IP privée "A" en classless avec des petits masques (/27, /29, /30 le tout dans un /24) ;
- Simulation d'une liaison P-t-P (adsl, fibre, etc...) pour le parc de l'entreprise, utilisation des mécanismes standard de translation d'adresses ;
- Utilisation d'équipements CISCO et FreeBSD pour le routage et la commutation.

4. Évolutions fonctionnelles de l'architecture

Nous nous intéressons dans cette section à l'évolution de l'architecture schématisée précédemment, permettant de présenter les différents services qui ont été mis en place. Les choix effectués quant aux solutions logicielles retenues seront explicités ultérieurement.

♦ Première confrontation

Notre choix s'est tout d'abord axé sur la mise à disposition des services suivants :

- Serveur Web NATé derrière un proxy (deux machines différentes). Ce serveur proposant :
  - Site *statique* sans base de données ;
  - Blog de la société ;
  - Wiki de la société ;
- Serveur DNS ;
- Serveur de machines virtuelles (intégrant des postes clients Windows XP SP2 et Linux Debian) ;
- Firewall de tête ;
- A l'attention du groupe Audit :
  - Déversement des logs de tous les serveurs sur l'infrastructure du prestataire.
  - Déversement des résultats de la sonde NetFlow

Il était dans un premier temps prévu que le service mail soit mis en place, son déploiement a été repoussé à la seconde confrontation.

♦ Seconde confrontation

Pour la seconde confrontation, notre infrastructure a évoluée avec les services suivants :

- Mise en place d'un FTP (sur le serveur Web) ;
- Mise en place d'un site Web dynamique avec bases de données ;
- Mise en place du service de mail ;
- Mise en place d'un serveur de sauvegarde distante ;
- Mise en place d'une duplication intégrale des disques durs de nos serveurs ;
- Installation des suites bureautiques sur les postes clients ;
- Installation d'une machine dans le parc client de type Windows XP SP0;
- Modification du filtrage pour rendre actifs tous les services ajoutés.

Les problèmes que nous avons pu rencontrer correspondaient principalement à la mise en œuvre de KVM et VDE (virtualisation).

♦ Troisième confrontation

La dernière confrontation a donné lieu à la mise en œuvre de peu de services, au vu des délais et des impératifs suite à la publication d'informations sensibles par le prestataire :

- Borne Wifi avec protection ;
- Augmentation de la sécurité.

5. Candidesa.org

Le domaine **candidesa.org** a initialement été acheté dans le but de fournir un moyen propre de communiquer entre étudiants du groupe Défense. En effet, cette machine a hébergé durant le projet nos services de communications **hors projet**. Nous entendons par là qu'il ne s'agissait **en aucun cas** d'un canal officiel de discussion/publication de l'entreprise Candide S.A mais d'un canal officieux

entre étudiants, de la même façon que nous aurions pu utiliser une solution de travail collaboratif en ligne (Google Groups, Google Docs, Ulteo) ou même une messagerie instantanée.
Cette machine hébergeait donc nos services de communications :

1. Webmail (roundcube) : Le serveur SMTP et le webmail sont positionnés sur la même machine ;
2. Wiki (médiawiki) : ce service a permis de documenter nos avancées et de centraliser l'information ;
3. VPN OpenVPN (ssl) permanent avec la machine ovpn-stri.iut-tlse3.fr:443 ;
4. Monitoring (nagios) et alerte par email et par téléphone ;
5. SSH : accès authentifiés par chiffrement à clés (GPG) permettant de consulter des éléments de sécurité de l'infrastructure.

Figure 4 *: Développement d'une identification anti Keylogger pour RoundCube et MediaWiki*

III. Réaction face aux différentes attaques menées

Plusieurs types d'offensives à l'égard du système d'informations ont pu être constatées. Certaines étaient "scénarisées" (préconisation émise par un représentant du groupe d'Attaque), et permettaient de caractériser les impacts qu'elles pouvaient occasionner. Ces offensives, différentes par leurs natures et leurs implications, ont impliqué certaines modifications et évolutions.

1. Lors des confrontations

Comme nous l'avons souligné précédemment, le projet s'est scindé en trois confrontations. Durant celles-ci, certaines failles ont été mises en avant par l'équipe Attaque. Cette partie expose les points fructueux concernant les attaques et les actions entreprises pour remédier le plus rapidement possible à ces problèmes.

- **La première attaque** mettant à mal un élément de notre architecture fut l'attaque sur le service de blogging Wordpress (Confrontation 2), version 2.8.4. Afin de stopper cette attaque, plusieurs modifications ont été apportées sur le serveur Web :
  - Mise à jour de la version de Wordpress (mise à jour vers la version 2.8.6) ;

- Ajustement de la configuration :
  - Du serveur Web Apache2 : *Max client* ;
  - De PHP : *max exec time* ;
  - De MySQL : nous ne l'avons cependant pas implémenté.

- **La seconde attaque** était basée sur la transmission d'un mail et d'une pièce jointe au format PDF à l'un des membres du parc (Confrontation 3). Ce fichier était spécialement conçu pour déclencher une exécution de code sur la machine qui l'ouvrait avec le lecteur PDF FoxitReader. Afin de s'en prémunir, nous avons pris les initiatives suivantes :

  - Utilisation d'un lecteur PDF insensible à ladite faille (potentiellement tous les clients autres que FoxitReader) ;
  - Mise en place d'un logiciel antivirus sur les postes clients.

- **La troisième attaque** s'est concentrée à tenter d'outre passer notre sécurité Wifi en en cassant la protection. Cette sécurité était basée sur le chiffrement WEP réputé faible et déprécié depuis le début des années 2000. Il est désormais conseillé d'utiliser le protocole WPA2 qui présente quant à lui une forte robustesse.

Plusieurs autres tentatives ont été observées et caractérisées par la société d'Audit mais n'ont pas mené à une compromission. Parmi elles, nous pouvons citer les suivantes :

- Dissimulation d'un serveur au sein des locaux de la société (faux plafonds) :
  - Cependant son exploitation n'ayant pu être effective (en partie à cause du cloisonnement des serveurs (VLANs) et de l'accessibilité de la salle (*cf. la partie sur les **contraintes***) il n'y a pas eu d'effets sur l'entreprise Candide S.A.
- Utilisation d'outils d'injection XSS et de bruteforce sur le site web dynamique développé ;
- Mail Bombing sur notre serveur de messagerie :
  - Aucun trafic ou surcharge n'a été détecté sur notre serveur (problème de configuration du logiciel côté attaquant ?).
- Scan de ports (attaque automatique de Nessus) :
  - Bannissement automatique des IP effectuant un nombre de requêtes trop important depuis le firewall.

2. À l'initiative de la société d'Audit

L'accord **contractuel** passé avec les responsables de la société d'audit ne prévoyait pas de scénario conduisant à la fuite d'informations. Cependant, cette initiative leur a permis de mesurer notre réactivité face à ce type de situation et ainsi de déterminer les actions à entreprendre pour en minimiser les dégâts. En pratique, ladite équipe a rendu public les images et informations contenues sur les différents serveurs (une partie des mots de passe, ainsi que le contenu hébergé sur Candidesa.org qui avait pu être atteint via un compte compromis). La source de la fuite des mots de passe n'a pas été identifiée, la seule trace de l'attaque trouvée est une attaque de type "bruteforce" sur le compte Wiki compromis, visant à trouver la clé de l'identification visuelle.
Nous avons détecté l'intrusion et ceci peu de temps avant cette fuite d'information, un système d'alertes étant en place sur le Routeur-Firewall dès lors qu'une personne s'identifiait sur cette machine (Une notification Nagios étant envoyée par email et SMS).

Afin de se prémunir des actions compromettantes, plusieurs mesures ont été prises :

- Coupure momentanée des services *internes* impactés (Wiki et webmail) le temps de modifier les mots de passe des utilisateurs ;
- Mise en place sur le Wiki (sur Candidesa.org) d'un nombre limité de tentatives de connexion ;
- Modification de la passphrase pour accéder à nos groupes LVM (Augmentation considérable du nombre de caractères) ;
- Modification des mots de passe de tous les serveurs ;
- Instructions :
    - Considérer les postes (hors serveurs) de la salle de TP comme compromis par un éventuel Keylogger ;
    - Restauration des différentes sauvegardes datant d'avant la compromission, et réinstallation des applicatifs suivant les procédures documentées tout au long du projet.

Il s'est avéré lors de la dernière confrontation, que les claviers d'origine de nos serveurs avaient été remplacés par des modèles identiques incluant une carte d'acquisition matérielle de la frappe au clavier (Keylogger matériel) dans un tampon étant vidé par la suite afin d'analyser la saisie et d'extraire les mots de passe qui auraient pu être tapés.

- **Dérive des pratiques de la société d'Audit**

L'accord conclu avec le prestataire Analyste ne précisant pas qu'une action de simulation de fuite d'informations pourrait être menée, celle-ci a outrepassé son cadre tel qu'il était contractuellement défini, basculant ainsi dans le contexte relatif au groupe d'Attaque, par la publication intégrale des éléments d'architecture, de configuration, de communication et de sécurité. Cette dérive fut positive pour le projet pour les raisons évoquées précédemment, mais reflète bien les difficultés éprouvées quant à la communication et aux risques et stress induits par des situations de type donneur d'ordre/prestataire.

IV.Retour sur expérience

1. Respect des grands principes de sécurité et de haute disponibilité

Nous illustrerons les concepts majeurs qui définissent la sécurité au travers d'un cas concret : le stockage des mots de passe administrateur de nos serveurs (information critique). La sécurité s'appuie sur les éléments suivants :

- **Authentification**

L'authentification pose la question : "*Qui êtes-vous ?*" Il s'agit du processus visant à identifier de façon unique les clients des applications et services, qui peuvent être des utilisateurs finaux, d'autres services, des processus ou des ordinateurs.

- En pratique, chacun de nos serveurs était doté de son propre mot de passe administrateur de longueur 8 caractères alphanumériques générés aléatoirement.

♦ Confidentialité

La confidentialité permet de s'assurer que les données restent privées et confidentielles et qu'elles ne peuvent pas être vues ou détournées par des utilisateurs non autorisés ou des indiscrets qui surveillent le flux du trafic sur un réseau. Le chiffrement est souvent employé pour renforcer la confidentialité. Les listes de contrôle d'accès (ACL) sont un autre moyen d'imposer la confidentialité.

- En pratique, chacun des mots de passe évoqués dans le point ci avant était stocké dans plusieurs fichiers chiffrés avec GPG permettant ainsi aux membres du groupe de n'avoir à retenir qu'une passphrase pour débloquer l'accès à tous les mots de passe de son cœur de métier, ceci dans le but d'éviter une mémorisation difficile de la dizaine de mots de passe (générés aléatoirement) et d'obliger une communication *en clair* des mots de passe susdits.

Problématique :

- Doit-on avoir un point **central** de stockage des mots de passe ?
  - **Pour** :
    - L'utilisation est plus facile ;
    - On évite ainsi la dispersion de l'information sur, au choix : bloc-notes, papier, post It et autres gribouillis ;
    - Les mots de passe peuvent devenir **très compliqués** puisque l'on ne doit plus les retenir.
  - **Contre** :
    - En cas de cassage du chiffrement GPG ou de vol d'une clef privée et de sa passphrase associée, les mots de passe d'un cœur de métier sont tous dévoilés ;
    - Criticité de la machine qui héberge ce service.

♦ Autorisation

L'autorisation pose la question : "*Qu'avez-vous le droit de faire ?*" Il s'agit de déterminer les ressources et les opérations que le client authentifié sont autorisées à consulter ou à effectuer. Les ressources englobent des fichiers, des bases de données, des tables, des lignes, etc., ainsi que des ressources dites "système" telles que des clés de registre et des données de configuration. Les opérations incluent l'exécution de transactions telles que l'achat d'un produit, le transfert d'argent d'un compte à un autre ou l'augmentation du taux de crédit d'un client.

- En pratique, nous avons choisi d'opter pour un point central de stockage des mots de passe, de façon chiffré avec GPG. Nous avons cependant pris soin de cloisonner les différents métiers entre eux afin de préserver les mots de passes d'un cœur en cas de faille sur un autre cœur (Exemple : voler la clef privée et la passphrase d'un membre du groupe *Mobilité* ne donne pas le droit de déchiffrer le fichier de mot de passe *Réseau*) : **c'est le principe des moindres privilèges**.

Cette solution est tout à fait envisageable dans la réalité, en prenant soin de stocker les clefs privées de façon sécurisée (coffre-fort ?).

♦ Audit et journalisation

Un audit et une journalisation efficaces sont essentiels pour la non répudiation. La non répudiation garantit qu'un utilisateur ne peut pas refuser l'exécution d'une opération ou le déclenchement d'une transaction. Par exemple, dans un système de e-commerce, des mécanismes de non-répudiation sont nécessaires pour s'assurer que le consommateur ne peut pas nier une commande qu'il aurait passé auparavant.

- En pratique, nous déversions une copie de l'intégralité des journaux de tous nos serveurs à l'équipe Analyse ce qui a permis d'avoir une trace de toutes les actions réalisées. Il faut savoir que la conservation des journaux est inscrite dans la loi et est obligatoire (un certain temps) et peut être utile lors de conflits ou d'enquêtes.

♦ Intégrité

L'intégrité garantit que les données sont protégées contre toute modification accidentelle ou délibérée (malveillante). Comme la confidentialité, l'intégrité est une préoccupation majeure, notamment pour les données transmises sur des réseaux. L'intégrité des données en transit est généralement assurée par des techniques de signature numérique et d'authentification des messages.
Une problématique développée et actuellement en contradiction avec le concept d'intégrité, est l'émergence des applications Web orientés utilisateur, qualifiées de "Web 2.0". Celles-ci utilisent fréquemment des sources d'informations dynamiques actualisées par le biais de différents fournisseurs de contenus, contenus pour la plupart non-authentifiés. A ce titre, une problématique développée est **l'impact d'une infrastructure supportant des applications riches de type Web 2.0**, celles-ci pouvant permettre d'exécuter du code malveillant à distance.
Une des solutions à ce problème serait la structuration en couche Présentation/Middleware/Database.

- La couche **Présentation** servant comme son nom l'indique à "présenter" sur le réseau public un produit fini qui sera construit en aval par les deux autres couches. Ce produit fini peut être une page Web ne nécessitant pas d'interrogation d'une base de donnée pour être construite par exemple, on parle de page Web Composée. Ce pourrait aussi être du courrier électronique avec des en-têtes figées donc non modifiables.

- La couche **Middleware** serait quant à elle responsable de la composition et de la construction du produit fini présenté par la couche Présentation. Elle réalise les traitements nécessaires sur l'information afin de la rendre exploitable par chaque utilisateur en fonction de ses besoins et contribue donc à l'évolutivité du système. Pour réaliser ce travail, elle dispose de langages comme PHP et ASP.

- La couche **Database** servirait alors uniquement au stockage de l'information brute de façon structurée. Les informations à stocker pouvant être des fichiers textes, des feuilles de style, des fichiers SQL, etc., on peut utiliser pour cela des systèmes de fichiers, des systèmes de bases de données relationnelles, etc.

Cette architecture multi-tiers présente en effet l'avantage d'améliorer la sécurité. Tandis que dans un système client-serveur tous les clients accédaient à la base de données ce qui la rendait vulnérable ; Avec une architecture multi-tiers l'accès à la base n'est effectué que par le serveur applicatif. De ce fait, il est le seul à connaître le mode de connexion à cette base et il ne partage aucune des informations permettant l'accès aux données, en particulier le login et le mot de passe de la base. La gestion de la sécurité se fait alors uniquement au niveau de ce serveur applicatif :

- Mise en place et mise à jour constante d'une liste des utilisateurs avec leurs mots de passe ainsi que leurs droits d'accès aux fonctions du système ;
- Mise en place d'une architecture réseau interdisant totalement l'accès au serveur de base de données pour les utilisateurs finaux.

Cette architecture permet d'assurer l'intégrité des données puisque l'accès à celles-ci est restreint à un groupe réduit de personnes.

♦ Disponibilité

Dans un contexte de sécurité, on entend par disponibilité la capacité pour des systèmes de rester opérationnels ou fonctionnels pour les utilisateurs légitimes. La principale caractéristique des attaques par Déni de Service ('DoS') est de mettre à mal cette exigence d'exploitation.
Comme détaillé précédemment, deux événements ont fortement contribué à restreindre la disponibilité du SI au cours du projet :

- La mise à mal du serveur Web entraînant une indisponibilité totale du service Web, pendant des durées relativement courtes, mais nécessitant toutefois une analyse et l'apport de correctifs.
- Le vol et la publication de données de l'entreprise, effectués par la société d'audit. Dans ce cas, une coupure de longue durée a été observée, coupure nécessaire pour restaurer l'intégralité des systèmes mais également intervenir sur l'ensemble de la politique de sécurité définie (Mots de Passe, clé privées SSH, ...). De telles périodes d'arrêt pouvant avoir de lourdes conséquences sur la situation économique de l'entreprise.

La perte de disponibilité constatée est ici difficilement quantifiable, principalement par les contraintes d'exploitation citées plus haut, mais également par la scission observée entre Candide S.A. et son prestataire d'audit suite au deuxième événement.
L'exigence de disponibilité peut être satisfaite par l'utilisation de différents moyens. Bien qu'un certain nombre d'entre eux aient été mis en œuvre, plusieurs processus non-indépendants peuvent être envisagés dans un contexte d'entreprise :

○ Étude de la présentation de l'infrastructure

Le cloisonnement des services défini par le **mode de présentation de l'infrastructure de services**. Ces "bonnes pratiques" visent à concevoir et cloisonner les différents éléments d'architecture en couches, des éléments de différentes natures (réseau, applicatifs) intervenant dans la composition de ces couches.

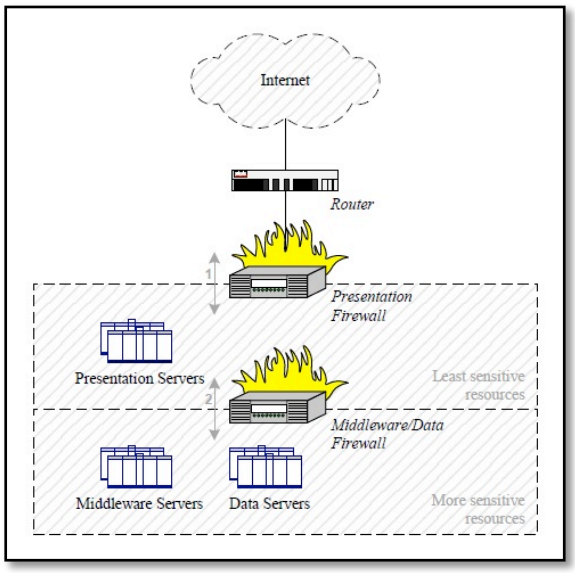

Figure 5 *: Architecture N-Tiers*

Pour ceci, une séparation évidente doit être effectuée entre :

- la couche **présentation**, offrant des "produits finis" et prenant en charge le dialogue client-serveur ;
- la couche **middleware**, effectuant le travail de composition et de logique applicative (transformations opérées par des "briques" PHP ou J2EE par exemple) ;
- la couche **database**, garante de la persistance des données (via un ou plusieurs SGBD dans la plupart des cas).

Ces concepts s'appuient massivement sur des techniques de répartition dans le cas de projets ou d'applications métiers de grande envergure, mais également sur des mesures de sécurité telles que le filtrage multi-niveaux et la création de VLAN. Ce type d'architecture dite "trois-tiers" présentent l'avantage d'isoler les éléments à forte criticité mais également de ne pas impacter l'ensemble du système (la partie frontale étant la plus exposée, elle n'héberge ni les données ni la logique).

- **Étude des politiques de reprise sur activité**

La restauration des données sur incident est une composante majeure de la disponibilité. Toutefois, celle-ci peut être considérée à plusieurs échelles:

- Archivage pour restauration de l'état "J-1" via des concepts de centralisation du backup tels que ceux mis en place dans le cadre du projet ;
- Gestion d'images de disques incrémentales ou "snapshots", offerte par LVM, la sauvegarde et l'interruption pour basculement ne prenant ici que quelques secondes.

Dans notre cas d'utilisation, la remise en état des configurations après fuite d'informations par le serveur de Backup a été compromise à cause de l'incertitude concernant l'intégrité des données.
Il apparaît donc opportun dans ce contexte de pouvoir se servir de solutions différentes mais complémentaires, d'une part pour assurer la disponibilité, d'autre part pour garantir l'intégrité des données. A ce titre, il apparaît que l'utilisation d'images disque standard, couplée à l'utilisation des fonctionnalités de bascule LVM et de sauvegarde périodique vers une unité dédiée via Rsync est optimale en granularité.

- **Utilisation d'un proxy de type haute disponibilité**

La répartition de charge, ou *load-balancing*, est une technique utilisée en informatique pour distribuer un travail entre plusieurs processus, ordinateurs, disques ou diverses ressources. Elle s'applique, en particulier, au domaine des connexions réseau, où elle permet d'assurer l'extensibilité et la haute disponibilité d'applications et de sites web.
HaProxy est une solution libre, fiable et performante pour la répartition de charge de niveau 4 et de niveau 7. Fiabilité reconnue dans le domaine de l'informatique et qui ne s'est pas faite au détriment des performances. En effet, HaProxy requiert peu de ressources et son architecture évènementielle mono-processus lui permet de gérer plusieurs milliers de connexions simultanées sur plusieurs relais sans effondrer le système.
Les avantages d'utilisation de ce système sont les suivants :

- Augmentation de la qualité des services ;
- Amélioration des temps de réponse des services ;
- Capacité à palier la défaillance d'une ou plusieurs machines ;
- Possibilité d'ajouter des serveurs sans interruption de service (dans le cas par exemple où le nombre de visites par jour augmenterait considérablement).

Au vu de ces qualités, nous avons retenu cette solution pour router l'ensemble du trafic Web de notre parc, le but étant de permettre à la machine WWW de fournir les services qui justifient son existence (blog, wiki et site de l'entreprise). Cependant, ce choix peut être remis en cause car la puissance de l'outil n'a pas pu être exploitée de par notre architecture. De même qu'HaProxy ne s'est pas substitué aux vraies couches **Présentation / Middleware / Database**.

- **Utilisation généralisée des solutions de virtualisation**

De plus en plus dans le monde industriel, la virtualisation de serveurs est au cœur des projets de consolidation des infrastructures. Elle permet de réaliser des économies d'infrastructure mais facilite également les plans de reprise d'activité. En effet, que ce soit pour le simple poste client, ou que ce soit pour une ferme de serveurs, il est assez trivial de faire des sauvegardes incrémentales (ou snapshots) journalier par exemple, permettant ainsi en cas de panne, de remettre très rapidement en route une machine à J-1 (selon la politique de sauvegarde de l'entreprise). Ceci permettant de s'approcher à moindre frais d'un taux de disponibilité de 99,99%.

- **Utilisation d'un firewall applicatif**

Un firewall est un point central dans la mise en place de politiques de sécurité d'un réseau. Il permet de protéger un ou plusieurs ordinateurs des intrusions provenant d'un réseau tiers comme Internet en filtrant les paquets de données échangés depuis ou vers le réseau à sécuriser. Il offre la mise en place d'un véritable contrôle sur le trafic réseau de l'entreprise et permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi de l'utiliser sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce dernier.
On sait que les firewalls matériels, du fait de leur intégration directe dans la machine, font office de "boite noire". De ce fait, leur configuration est souvent relativement ardue, mais en contrepartie leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau. Ce sont des éléments relativement peu flexibles en terme de configuration, mais aussi peu vulnérables aux attaques de par leur présence dans la "boite noire" qu'est le routeur. Cette intégration matérielle rend aussi l'accès à leur code assez difficile.
Nous retiendrons donc :

- **Avantages** :
  - Intégré au matériel réseau ;
  - Administration relativement simple ;
  - Bon niveau de sécurité ;
- **Inconvénients** :
  - Dépendant du constructeur pour les mises à jour ;
  - Souvent peu flexibles.

D'autre part, les firewalls tournant sous linux sont réputés pour leur sérieux car cet OS offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les firewalls matériels des routeurs, à ceci près qu'ils sont configurables à la main.
Nous retiendrons donc :

- **Avantages** :
  - Personnalisables ;
  - Niveau de sécurité très bon.
- **Inconvénients** :
  - Nécessitent une administration système supplémentaire.

La grande faille de ces firewalls logiciels est leur non utilisation de la couche réseau. Il suffit donc d'utiliser une librairie spéciale, pour récupérer les paquets qui auraient été normalement « droppés »

par le firewall. Néanmoins, cette faille induit de s'introduire sur l'ordinateur en question pour y faire des modifications... chose qui induit déjà une intrusion dans le réseau, ou une prise de contrôle physique de l'ordinateur, ce qui est déjà synonyme d'inefficacité de la part du firewall.
Nous avons choisi d'utiliser une machine sous FreeBSD avec le logiciel PacketFilter comme firewall de tête alors qu'une solution matérielle s'offrait à nous (routeur propriétaire de marque Cisco).
Il aurait pu être intéressant d'utiliser les fonctionnalités du routeur pour assurer cette fonction ce qui aurait permis d'attribuer un autre usage à notre machine et de verrouiller un peu plus les accès au réseau.
Cependant, connaissant les différences entre les deux solutions et au vu du contexte du projet qui ne nécessitait pas d'interpréter les protocoles, la solution open-source que nous avons choisi a répondu à notre besoin tout en étant aisément configurable et en sécurisant de manière fiable le réseau.

2. Mise en œuvre d'une politique de défense

Nous avons axé notre politique de défense selon cinq axes :

1. **Se prémunir des attaques (proactif)** en évitant, dans un premier temps, la présence ou l'apparition de failles dans les constituants du système d'information. Afin de respecter ce premier point, nous avons opté pour des versions stables des divers éléments mis sur le réseau. Versions dont nous avons d'ailleurs dû baisser le niveau afin *d'ouvrir* des failles permettant ainsi à l'équipe Attaque d'atteindre le réseau.

2. **Bloquer** les attaques en leur empêchant de parvenir jusqu'aux composants sensibles et potentiellement vulnérables du système d'information, ou plus généralement réduire les chances de succès des attaques même si elles ciblent des composants vulnérables. Une fonction de filtrage des adresses IP des attaquants s'est mise en place de façon manuelle lors de la première confrontation. L'automatisation de celle-ci s'est avérée utile pour la suite du projet (ban d'une adresse après un certain nombre de tentatives pour inonder le réseau).

3. **Renforcer** la défense (rétroactif) afin de limiter les conséquences d'une compromission de l'un ou l'autre des composants du système d'information. Ce point est le plus difficile à mettre en œuvre du fait de l'accessibilité de la salle à l'ensemble de la promotion et donc aux équipes Attaque et Analyse. Malgré cela, un système de chiffrement du disque avec accès par *passphrase* s'est avéré être une protection suffisante jusqu'à ce que les périphériques (claviers) soient modifiés par l'équipe Analyse afin d'y greffer des *keyloggers*.

4. **Détecter et identifier** les incidents ou compromissions survenant sur le système d'information afin d'y faire face.

5. **Réparer** le système d'information suite à un incident ou à une compromission. Ceci a été rendu possible par le système de reprise sur activité qui a été mis en place très tôt. Toutes les configurations réalisées sur les machines étaient sauvegardées sur la machine de sauvegarde mais aussi, et ce de façon manuelle et périodique, sur un disque amovible.

3. Cloisonnement inter-projets

Cette section aborde une thématique récurrente du contexte d'entreprise, à savoir les relations d'interdépendance et de décloisonnement qui se créent au sein d'un ou plusieurs SI, et qui impactent la sécurité globale des systèmes et des données. Cette situation est classique dans ces contextes :

- au sein d'une même entreprise, par l'externalisation d'un ou plusieurs de ses services ;
- au sein d'une même entreprise, par la refonte de son organisation métiers/projets (processus d'urbanisation des SI, exemple typique à l'origine de bouleversements importants) ;
- par le biais de prestataires mettant en œuvre des solutions "clé en main" dont les failles deviennent exploitables entres SI de différentes natures.

L'exemple propre au contexte "projet" est **le pillage d'informations de l'infrastructure *externe*** constituée par candidesa.org, placée sur des équipements **à priori** non-attenants au projet, par les auditeurs de Candide S.A.
Ici, cette infrastructure à priori indépendante a peu à peu contribué à l'architecture de l'entreprise. Cette indépendance a été rompue dès lors que la machine :

- a été utilisée comme passerelle VPN ;
- a servi à centraliser de l'information propre au projet et a supporter l'ensemble des communications électroniques des collaborateurs (fréquemment accédée par les membres du groupe depuis l'infrastructure de projet, source de convoitise pour les attaquants du SI, ... et ses auditeurs).

Conclusion

La sécurité des systèmes d'informations prend tout son sens dans un contexte tel que celui proposé. En effet, une agence de sous-traitants telle que Candide S.A. peut devenir par son activité une cible potentielle d'actions "d'intelligence économique" de natures à compromettre principalement :

- la disponibilité de son infrastructure ;
- l'intégrité de ses données ;
- la confidentialité nécessaire vis-à-vis de l'activité ;
- et de façon indirecte, la crédibilité et l'image publique de l'entreprise.

Ces composantes sont connues sous le nom de "CIA Triad".
Pour ceci, la mise en oeuvre de **politiques de sécurité**, de **plans de reprise et de continuité d'activité**, ou encore d'une **méthodologie d'analyse** préalable telle que MEHARI ou EBIOS peut s'avérer bénéfique dans le sens où elle **structurent les actions et les méthodes en processus**. Par ailleurs, un impératif propre à l'ingénierie sécurité s'avère être la connaissance précise des coûts, risques et menaces encourus par une action ou un contexte spécifique.
Même si la plus-value technique et professionnelle du projet n'est plus à démontrer, la collaboration intra et inter-équipes permet de mesurer en sus :

- les difficultés inhérentes aux **facteurs humains** dans une organisation ;
- la nécessité de disposer de **visibilité sur les systèmes et les applications**, l'obscurité ou la mauvaise connaissance d'une solution s'avérant difficilement surmontable ;
- le **niveau de sécurité à appliquer aux différentes couches** composant une infrastructure de SI.

La connaissance des principes de base de la sécurité ainsi que la mise en place d'une bonne politique de défense a contribué, dans ce contexte, à instaurer un réseau sécurisé même si l'activité de ce dernier n'était pas significative par rapport à la durée du projet. Même si les exigences fonctionnelles ont été globalement satisfaites, ce manque aurait pu être comblé par une capacité étendue de **virtualisation** du parc, offrant une continuité de service à ce dernier mais aussi une **scénarisation propre à l'activité d'un utilisateur** réel (téléchargement en ligne, consultation et mise à jour d'un blog, accès à des infrastructure de type "Web 2.0", etc.). Cette fonctionnalité nous aurait permis de mieux appréhender les failles créées par les utilisateurs majoritairement du fait de leur ignorance que du fait de leur malveillance.
Les enseignements acquis par le biais de notre autonomie, des confrontations proposées et de la démarche de recherche ont incontestablement participé à la sensibilisation des participants ainsi qu'à l'acquisition de méthodes valorisantes pour l'avenir professionnel se dessinant à court terme.

Annexes

Ressources

Pour consulter l'ensemble de nos travaux en détail, suivre les évolutions séance par séance et inspecter la configuration de chacun des équipements, notre Wiki Candidesa.org est désormais accessible à tout le monde en lecture seule à l'adresse suivante : https://secure.candidesa.org/wiki/index.php/Accueil (certificat cacert.org)

Logiciels utilisés

- Distributions : Gentoo, Debian, MS XP SP2, MS XP SP0 & MS Server 2003
- Web : Apache 2
- FTP : ProFTPd
- Reverse Proxy : HAProxy
- DNS : bind9
- Firewalling : OpenBSD PF + ALTQ, Linux NetFilter
- Routage : Quagga
- Chiffrement : OpenSSH, GnuPG
- Monitoring : Nagios + NRPE
- Chiffrement partitions : LVM2 + Luks
- Gestion des logs : Syslog-ng
- Mail (SMTP) : Postfix
- Mail (POP & IMAP) : Dovecot
- Virtualisation : QEMU-KVM & VDE2
- Sauvegardes distantes : RSync
- Base de données : MySQL
- Moteur de Wiki : DokuWiki
- Moteur de blog : WordPress