Architecture réseau sécurisé pour une ouverture à l'Internet et processus qualité

Félix Guy ANOMA-KANIE

Sciences
Internet et systèmes d'exploitation

EDILIVRE.com
universitaire
collection


EDILIVRE.com
universitaire
COLLECTION

Félix Guy ANOMA-KANIE

Architecture réseau sécurisé pour une ouverture à l'Internet et processus qualité

Editions EDILIVRE APARIS
Collection Universitaire
75008 Paris – 2010

Tous nos livres sont imprimés dans les règles
environnementales les plus strictes

ISBN : 978-2-8121-3408-1

Dépôt légal : Juin 2010

REMERCIEMENTS

Je souhaite remercier Monsieur Michel GONIAU, Madame Marie Pierre JARRIGE et Monsieur Xavier BENTES, respectivement Directeur Général, Directeur des Développement et la Directeur Commercial d'Albiran pour m'avoir fait confiance pour la conduite de ce projet dont le mémoire fait l'objet.

Je remercie également Monsieur Didier JACQUEMIN Directeur Informatique de Gan Euro courtage sans qui ce stage ne se serait pas fait.

Je remercie Le Dr. Joëlle GERINIER, Directeur – Adjoint, Hôpital Avicenne, Docteur en Droit, Maître de conférences associé ;
Le Pr. Luc MARCO, Directeur du DRT, Professeur des Universités ;
Le Pr. Jan STEPNIESWKI, Maître de conférences, HDR ;
Le Pr. Ali SMIDA, Maître de conférences, HDR ;
Le Dr. Louise SHRIVEUR, Professeur Honoraire, Animateur ;
Pour l'honneur qu'ils me font de prendre pars au jury.

Je remercie les professeurs de l'Université Paris 13 Nord, de Villetaneuse, de Bobigny, de l'IUT Saint Denis, de l'Hôpital Avicenne et tous les intervenants extérieur, ainsi que les services administratif, pour les enseignements qu'ils m'ont apportés et leur aide.
Je remercie particulièrement le Pr. Gilbert SOL, Directeur du DESS ART et du Visio P7, ainsi que tous les enseignants du DESS ART de l'Université Paris 7, pour la qualité de la formation dispensée et du temps passé à mon écoute.
Je remercie également les équipes de développement, Technique et commerciale pour l'accueil qu'ils m'ont témoigné et l'aide qu'ils m'ont apporté et Monsieur Eric BRUNETON Administrateur Système et Réseau pour sa patience et la confiance qu'il m'a témoigné.

Je souhaite aussi remercier ma famille et tous mes collègues et ami(e)s pour leur soutien et leur patience.

SOMMAIRE

INTRODUCTION

Un réseau qui présente une vulnérabilité ne peut être considéré comme sécurisé. Si personne n'en sait rien, c'est-à-dire si, concrètement, cette vulnérabilité n'a pas encore été découverte, alors le réseau est sûr. Si une seule personne est au courant, elle considèrera que le réseau n'est pas sûr, mais pour toutes les autres personnes, n'ayant aucune idée de cette vulnérabilité, le réseau semblera sécurisé. Si le fabricant de l'équipement de réseau est au courant, si des acheteurs en matière de sécurité sont au courant, si la communauté des pirates est au courant, on peut dire que l'insécurité du réseau s'accroît à mesure que la nouvelle de cette vulnérabilité se répand.

La situation du marché : les réseaux e-business d'aujourd'hui exigent un niveau élevé de sécurité tout en se devant d'offrir une navigation transparente entre des ressources hétérogènes. Selon une estimation de Internet Week, l'entreprise moyenne perdra 1,6 milliards de dollars cette année en raison de violations de la sécurité. Le défi consiste non seulement à empêcher les accès utilisateurs non autorisés aux ressources, mais également à améliorer le confort de l'utilisateur.

Le problème : le déploiement des solutions trop complexes d'aujourd'hui peut prendre des mois et monopoliser de précieuses ressources informatiques. Ces solutions exigent également de modifier les systèmes cibles, ce qui représente un véritable défi sur le plan organisationnel dans un environnement extranet/internet.

Les places de marché électroniques et les portails d'entreprise représentent la nouvelle frontière de l'e-business d'aujourd'hui. Ils donnent accès à tout et ce, où que vous soyez sur le Web. Mais comment relier des sources de données hétérogènes multiples afin de permettre un flux d'informations homogène au sein de l'entreprise virtuelle, tout en appliquant une stratégie de contrôle d'accès forte et personnalisée ?

1 PRESENTATION DE L'ENTREPRISE

Albiran est une Société Anonyme au capital de 338.880 €. Son Siège social est situé au 1, rue de Craiova 92024 Nanterre cedex. Email : albiran@albiran.com

1.1 La société

La société a été créée en 1999 par une équipe de professionnels de l'assurance, de l'informatique et de l'édition de logiciel

La solution développée par ALBIRAN répond parfaitement aux exigences du marché et aux besoins des acteurs de l'assurance ce qui a permis à la société d'acquérir rapidement un bon portefeuille de clients et d'assurer son autonomie et son auto-financement.

La société poursuit son développement pour faire évoluer toujours plus les solutions qu'elle propose et apporter ses compétences et son savoir-faire à ses clients.

Ce point décrit les éléments d'architecture détaillée « système » des serveurs de la plate forme de production dans le cadre de la première phase du projet Albiran.

1.1.1 L'équipe

L'équipe d'ALBIRAN est composée de collaborateurs expérimentés, issus du monde de l'assurance, des nouvelles technologies, de l'informatique grand système et de l'édition de logiciel.

Ce passé d'éditeur de logiciel d'une partie de l'équipe garantit aux clients la pérennité de leur investissement en termes de qualité et d'évolutivité.

De même, la parfaite connaissance des systèmes de gestion des compagnies d'assurance a permis de définir des normes et standards facilitant la connectivité avec les systèmes existants chez les assureurs.

1.1.2 Les dirigeants

- Francis Moise, président du conseil d'administration, a assumé pendant 11 ans les fonctions de directeur des systèmes d'information du groupe AGF (fmoise@albiran.com).
- Michel Gognau, directeur général, était précédemment fondateur et président directeur général de l'éditeur CIRCEA (VIVEO Assurance) (mgognau@albiran.com).
- Joël Berne, directeur des opérations, était précédemment directeur général de l'éditeur IBIS (logiciels de gestion assurance) (jberne@albiran.com).
- Marie-Pierre Jarrige, directeur recherche et développement, était précédemment en charge de la R&D de l'éditeur CIRCEA (VIVEO Assurance) (mpjarrige@albiran.com).
- Xavier Bentes, directeur commercial, possède un parcours commercial d'une quinzaine d'années dont cinq dans les Grands Comptes et l'Internet. Il était auparavant chez l'éditeur international REEF France (xbentes@albiran.com).

1.2 La solutions EBIZA

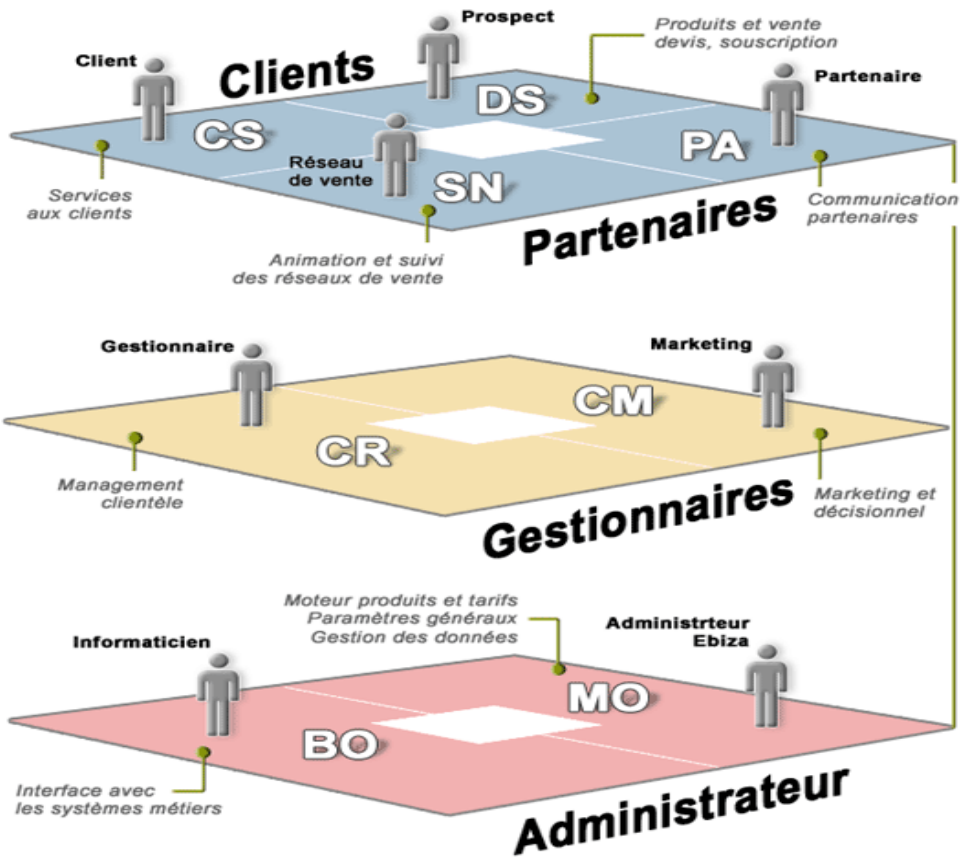
1.2.1 Description générale de la solution

La solution EBIZA 4.0 permet de déployer, de manière simple et rapide, des offres et des fonctionnalités d'assurance via Internet, Extranet ou Intranet.

Elle permet de gérer la communication avec l'ensemble des acteurs pour tous les processus d'assurance : devis, souscription, gestion des contrats, sinistres, informations clients… tout en assurant le lien avec les systèmes de gestion des compagnies ou des courtiers.

La solution est parfaitement modulaire. Il est donc possible de déployer de manière progressive des produits et des fonctions d'assurance auprès de tous types de réseaux de distribution ou des clients finaux.

1.2.2 la solution EBIZA 4.0 est composé de huits modules



EBIZA DS

Produits et ventes : devis, souscription

Description générale :

Module dédié à la vente directe, il comprend une série de fonctions de devis, cotation et souscription en auto, moto, habitation, santé, prévoyance, épargne mono ou multi fonds…

Il incorpore également toutes les pages présentant la société, ses produits, ses objectifs et, de manière générale, toutes les informations que l'assureur souhaite mettre à disposition du public.

Ce module peut être déployé via Internet pour la vente directe ou via Extranet à destination de réseaux de vente : agents, courtiers, apporteurs d'affaires en conjonction avec le module EBIZA-SN.

Pour les produits et leur tarification le module fait appel au moteur « Produits et tarifs » d'EBIZA-MO.

En fonction de la situation et du souhait du client, ces fonctions et pages sont livrables totalement ou partiellement.

Principales fonctionnalités :

- Accueil du prospect
- Gestion de ses données de base
- Devis et souscription habitation
- Devis et souscription automobile
- Devis et souscription moto
- Devis et souscription prévoyance
- Devis et souscription santé
- Proposition et souscription épargne

Sauvegarde, consultation et reprise des devis

EBIZA CS
Services aux clients

Description générale :
Ce module, conçu pour les services au client final, comprend toutes les fonctions d'aide, les informations sur l'avancement de ses dossiers et la possibilité de communiquer avec la compagnie : que faire en cas de problème ou de sinistre, situation de l'indemnisation en cours, qui contacter, pièces attendues par l'assureur, consultation des contrats, valorisation de l'épargne, avenants… EBIZA-CS apporte également des fonctions permettant d'accélérer et d'optimiser la qualité de gestion de l'indemnisation (voir également EBIZA-PA et EBIZA-CR). EBIZA-CS donne enfin l'accès à toutes les fonctions de vente de EBIZA-DS avec les particularités que confère le statut de client : tarif préférentiel, informations privilégiées…

Ce module peut être déployé via Internet pour la relation directe avec le client final ou via Extranet à destination de réseaux de vente : agents, courtiers, apporteurs d'affaires en conjonction avec le module EBIZA-SN pour gérer leurs comptes clients.

Principales fonctionnalités :

- Accueil du client,
- Gestion de ses données de base et de son mot de passe.

Consultation et suivi :

- Suivi synthétique du portefeuille contrats et indemnisations,
- Consultation des devis en cours,
- Consultation des contrats,

Consultation de son solde ; Valorisation de contrat d'épargne :

- Indemnisation,
- Déclaration de sinistre,
- Rendez-vous expertise,
- Suivi du traitement du sinistre,
- Suivi de l'indemnisation et des décomptes santé.

Avenants IARD :

- Modification d'immatriculation Projet d'avenant

Avenants Vie :

- Versement libre,
- Demande d'arbitrage,
- Demande de rachat partiel ou total,
- Demande d'avance.

EBIZA SN

Animation et suivi des réseaux de vente

Spécifique aux réseaux de vente, qu'ils soient constitués de vendeurs permanents ou occasionnels, salariés ou non, ses fonctions sont donc des fonctions d'aide à la vente (Devis, souscription et autorisation compagnie en ligne) et des fonctions d'animation de réseau : objectifs, résultats, suivi de portefeuille…

EBIZA-SN donne également l'accès aux fonctions de gestion du client (EBIZA-CS) pour permettre au distributeur de conseiller et d'aider le prospect et le client.

Principales fonctionnalités :
Accueil du distributeur

Description générale :

- Gestion de ses données de base et de son mot de passe,
- Informations et marketing,
- Suivi du portefeuille clients,
- Reprise d'un devis,
- Statistiques de production,
- Statistiques d'indemnisation,
- Vente en ligne.

EBIZA PA
Communication partenaires

Description générale :

Ce module gère en tout premier lieu les fonctions de communication avec les experts et prestataires dans les secteurs de la cotation et de l'indemnisation : expertises avant souscription ou après sinistre, appels d'offres, ordres de travaux, prises en charge…

Il permettra également la communication avec toutes les catégories d'interlocuteurs de la compagnie d'assurance : informations vers les réassureurs et co-assureurs, déclarations à l'administration fiscale, collecte d'informations de succursales et filiales lointaines…

Comme c'est le cas de l'ensemble des solutions EBIZA les livraisons des fonctions sont adaptées aux besoins du client.

Principales fonctionnalités :

- Accueil du partenaire,
- Modification de ses données de base et de son mot de passe,
- Informations partenaires,
- Consultation des missions d'expertises,
- Saisie des rapports d'expertises,
- Consultation des rapports d'expertises.

EBIZA CR
Relations clientèle

Description générale :

Ce module permet aux gestionnaires d'intervenir soit en support téléphonique du prospect, client ou vendeur, soit d'intervenir en gestion et décision : assistance ou validation d'une proposition faite par le vendeur, décision de nomination d'un expert, décision d'indemnisation immédiate…

Principales fonctionnalités :

- Accueil du gestionnaire,
- Gestion de ses données de base et de son mot de passe,
- Consultation de ses dossiers,
- Prise en charge d'un dossier,
- Transfert d'un dossier ou portefeuille à un autre gestionnaire,
- Attribution d'un dossier à un expert,
- Gestion des règlements d'indemnisation,
- Demande de complément d'information,
- Clôture d'un dossier d'indemnisation,
- Gestion des mouvements d'épargne.

EBIZA CM

Marketing et décisionnel

Description générale :

- Tous les événements significatifs de la vie du site sont enregistrés dans la base de données, qu'il s'agisse de devis, de souscriptions, d'interrogations, de mises à jour…

- Ce module permet d'élaborer des compléments d'analyse de l'activité du site, des statistiques pertinentes et, le cas échéant, de fournir les informations nécessaires à la mise en œuvre d'outils généralistes de marketing d'e-commerce.

Principales fonctionnalités :

- Accueil du suivi des ventes,
- Statistiques globales des ventes du portefeuille,
- Consultation détaillée des devis ou contrats par période,
- Relances des prospects,
- Export de données vers outils de CRM ou autre,

EBIZA BO

Interfaces vers le système de l'assureur

Description générale :

Ce module permet d'assurer la cohésion du site et du back office ;
Réplication réduite des données du back office pour alimenter le site (informations clients, contrats, indemnisations…).

Transfert des données acquises par le site (devis, souscriptions, déclarations de sinistres, messages…) vers ce back office.

La communication peut se faire selon le besoin en mode synchrone ou asynchrone par utilisation des grands standards du marché. Le format des fichiers et messages échangés sera adapté

à chacun des hosts cibles, soit par paramétrage, soit, si besoin, par adaptation des couches externes de communication.
Principales fonctionnalités :

- Principaux modes de communication, synchrone ou asynchrone, gérés :

XML
FTP
Scort intranet connector
MQSeries

- Vers les principaux systèmes :

Systèmes MVS
AS/400
Unix
Windows NT

EBIZA MO
Moteur produits et tarifs, paramètres généraux, gestion des données

Description générale :

Principales fonctionnalités, Paramétrage :

- Gestion des sociétés, devises, langues et paramètres généraux,
- Gestion des produits classiques (création, modification, consultation, duplication, versioning),
- Gestion des tarifs (paramétrage, simulation, versioning),
- Gestion des produits d'épargne (création, modification et valorisation des produits et supports),
- Gestion des habilitations (filtre événement, profil),
- Gestion des partenaires (distributeur, expert, gestionnaire) et des rôles,
- Visualisation et gestion des données du site avec filtrage des données par type d'interlocuteur.

Exploitation :

- Gestion des habilitations système,

- Consultation de l'historique des connexions,

Attribution d'un nouveau mot de passe.

1.2.3 Architecture technique EBIZA

Une attention toute particulière a été apportée aux standards de développement et au choix des composants techniques pour assurer une très grande portabilité de l'offre EBIZA sur l'ensemble des plates-formes d'exploitation courantes développée intégralement en Java, la solution ne contient aucune implémentation spécifique à l'une ou l'autre solution propriétaire. Il en est de même pour les modules d'accès aux bases de données.

- Principaux systèmes d'exploitation supportés :

NT

Windows 2000

UNIX

LINUX

- Principaux systèmes serveurs et moteurs de servlets supportés :

IIS

Apache

Web sphere

WebLogic

Resin

…

- Principaux systèmes de bases de données supportés :

Microsoft SQL 7

Microsoft SQL 2000

Oracle

…

1.3 L'activité de l'entreprise

1.3.1 Les assurances

Le point commun des assurances est qu'elles vendent toutes les mêmes produits.

- Clients (simple/particulier : Automobile, santé…),
- Entreprises (couverture risque : contre une prime, contrat d'entreprise type, exemple : 100 à 1000 véhicules d'une entreprise).

Par contre leur gestion différent :
(Macif, Maïf….), vente sans agents, sans courtiers, sans intermédiaires,
Sociétés anonymes classique : AGF, GENERALY, AXA, GAN, fonctionnent avec des intermédiaires (Mandataires =/= courtiers).
Ce qui entraîne un impact sur l'informatique.

Avant l'Internet :

Les courtiers travaillaient sur papier,

Mode de vente :

50% fait par les agents,
20 à 30% fait par les courtiers,
Le reste se faisait par vente directe.

Avec l'informatique apparaissent une nouvelle méthode de gestion et de nouveaux canaux de distribution.

L'extranet permet une gestion simultanée de différents statuts, ce qui implique pour les ressources de développement, un seul développement et une minimisation des erreurs.
Cela à aussi un impact sur la vente et sur la structure juridique.

Exemple pour un accident il faut :

- Une déclaration,
- Un expert,
- Un réparateur,
- Une responsabilité.

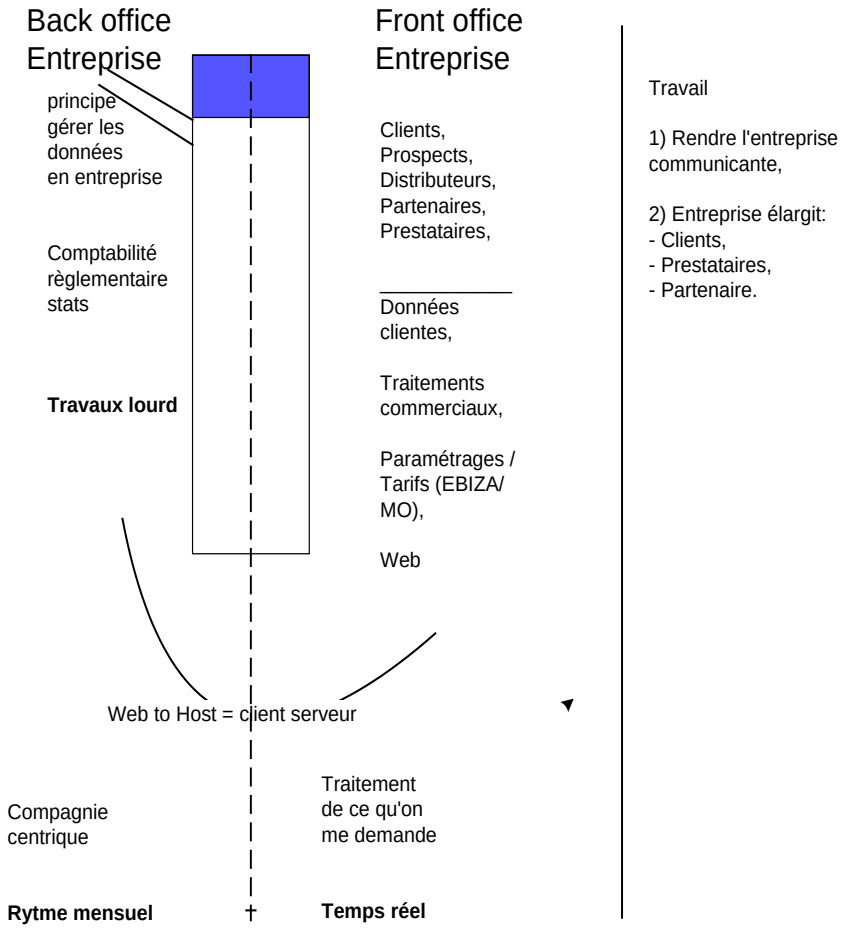
Si il y a un procès :

Un intervenant (l'huissier),
Si il y a un blessé :
Un intervenant (le médecin).

Ce qui nécessite un travail de communication.

Travail :

- Rendre l'entreprise communicante,
- Elargissement de l'entreprise aux clients, aux prestataires et aux partenaires.



Principe de fonctionnement informatique d'une structure d'assurance.

1.4 Exemple de Mise en œuvre d'une Architecture

1.4.1 Présentation

L'architecture technique à mettre en œuvre pour l'installation de la solution EBIZA est la suivante :

L'application EBIZA doit être installée sur un serveur d'application exemple WebLogic (BEA) avec une connexion à une base de donnée Oracle 8.0 sous environnement UNIX.
Le serveur d'application WebLogic peut être mis dans un environnement UNIX ou Windows.

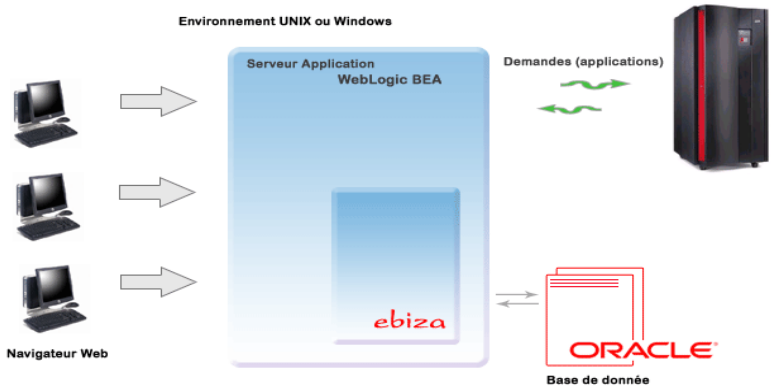


Schéma architecture technique

Il existe dans WebLogic Server 7.0, un module appelé WebLogic JAM (Java Adapter for Mainframe). Ce module est composé de deux parties :

- La partie Gateway installée sur le serveur d'application,
- La partie CRM (Communication Ressource Manager) sur le Mainframe.

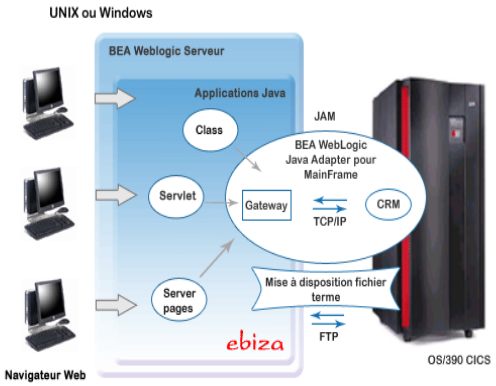


Schéma implantation JAM

Le protocole de communication utilisé entre le serveur d'application et la machine MVS est le protocole TCP/IP.
Des modules d'échantillonnage seront créés pour la traduction entre les deux plates-formes.

1.5 Exemple d'Architecture des machines pendant les différentes phases de projet

1.5.1 Phase de dévelloppement

Durant cette phase une seule machine sous un environnement Windows. Machine sera installé :

- Application EBIZA (pages, modules java),
- Serveur Web (serveur http et serveur d'application),
- Serveur Oracle (serveur de base de donnée).

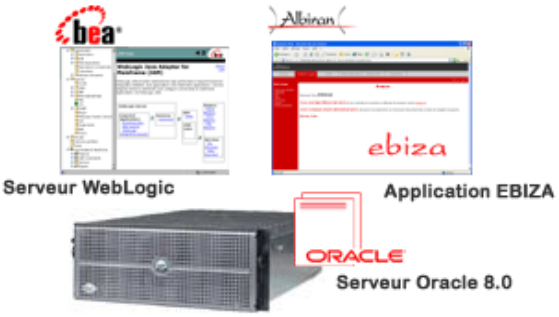


Schéma représentant l'organisation
des différents logiciels et application en phase de développement

1.5.2 Phase d'homologation et de recette

Durant ces phases une seule machine sous un environnement UNIX. Sur cette machine sera installé :

- Application EBIZA (pages, modules java),
- Serveur Web (serveur http et serveur d'application),
- Serveur Oracle (serveur de base de donnée).

Schéma représentant l'organisation
des différents logiciels et application en phase de développement

1.5.3 Phase de production

Durant cette phase trois machines sous un environnement UNIX.

- Une machine pour le serveur http,
- Une machine pour le serveur d'application et l'application EBiza,
- Une machine pour la base de donnée Oracle.

Le serveur http et le serveur d'application WebLogic Server 7.0, peuvent être fusionnés sur la même machine, deux machines peuvent donc suffirent.

Schéma représentant l'organisation
des différents logiciels et application en phase de production

1.6 Références

La société Albiran travaille avec un certain nombre de références qui sont :

gan	**GAN Eurocourtage** Société de courtage en assurance
AGF	AGF ESPACE COURTAGE **AGF Espace Courtage** est une structure entièrement dédiée aux courtiers, qui propose une large gamme de produits et services (IARD, Transport) et des produits innovants (auto malussés, plaisance…) tant dans les secteurs des risques d'Entreprises que de Particuliers. AGF SANTÉ **AGF Santé distribue ses produits santé auprès de nombreux courtiers en France.**

MARSH	**Ce grand courtier, leader mondial, s'est positionné sur plusieurs opérations comme concepteur du produit et apporteur de l'ensemble de la solution, incluant le site Web.**
CNP ASSURANCES	**CNP Assurances**
	Gras Savoye
FIRSTREAM	FIRSTREAM est une compagnie qui distribue des produits et services multiples au niveau européen. Son portail Assuronline propose des produits **d'assurance auprès des étudiants, particuliers et professionnels**. Mais FIRSTREAM souhaite également proposer certains produits au travers de sites partenaires.

2 L'OUVERTURE VERS L'INTERNET : LES RISQUES ET LES SOLUTIONS.

L'Internet permet aux entreprises d'établir des connexions avec leurs clients, partenaires et employés. Cette technologie, bien qu'offrant de nouvelles opportunités, peut aussi poser des problèmes en matière de sécurité, de performances et de gestion. Pour répondre aux besoins des entreprises d'aujourd'hui qui disposent d'un accès à Internet ; Des fonctionnalités de mise en cache permettent aux entreprises d'économiser de la bande passante réseau et fournissent aux utilisateurs un accès plus rapide au Web.

Les services de pare-feu qui protègent les ressources réseau des accès non autorisés provenant de l'extérieur du réseau de l'entreprise, tout en permettant des accès autorisés efficaces. Des fonctionnalités de gestion et d'administration grâce auxquelles les entreprises peuvent contrôler et gérer l'utilisation et l'accès à Internet d'une manière centralisée.

Un pare-feu d'entreprise et un serveur de cache qui s'exécute sur le système d'exploitation, lequel propose un contrôle d'accès basé sur des stratégies, l'accélération des performances et la gestion de la mise en réseau. Conçues pour répondre aux besoins de l'entreprise en termes d'organisation et de réseau. Qu'il soit déployé comme composant distinct ou comme serveur de pare-feu et de mise en cache intégré, fournit aux entreprises une console de gestion unifiée, conçue pour simplifier la gestion de la sécurité et des accès.

2.1 Cerner l'organisation

Afin de cerner l'organisation nous suivrons la méthodologie d'attaque de base de l'intrus qui se décompose de la façon suivante :

- Acquisition de la cible et collecte d'informations,
- Premier accès,
- Remontée des droits d'accès,
- Masquage des traces.

Ce qui permet d'avoir une vue globale des vulnérabilités, des failles et des informations sensibles dont pourrait se saisir un intrus, interne ou externe à l'entreprise.

2.1.1 La prise d'empreinte

La prise d'empreinte est l'art de rassembler des informations sur une cible.

2.1.1.1 Définition de la notion de prise d'empreinte

La prise d'empreinte systématique d'une organisation permet aux pirates de créer un profil complet de l'état de sécurité de celle-ci. En exploitant une combinaison d'outils et de techniques, les pirates peuvent prendre une grandeur inconnue (connexion Internet d'une entreprise fictive.) et la réduire en une plage donnée de noms de domaine, de blocs de réseau et d'adresses IP individuelles de systèmes directement connectés à Internet.
La prise d'empreinte est nécessaire pour s'assurer de la manière systématique et méthodologique que toutes les informations associées aux technologies suivantes :

- Internet,
- Intranet,
- Accès à distance et extranet.

Les cibles sont identifiées. La prise d'empreinte est la tache la plus ardue et la plus importante dans la détermination de l'état de sécurité d'une entité.

2.1.1.2 Prise d'empreinte Internet

Un guide pas à pas de prise d'empreinte n'existe pas car c'est une tâche qui peut mener dans diverses directions, cependant les opérations élémentaires permettant de mener à bien une analyse approfondie de prise d'empreinte sont les suivantes.

Technologie	Identifie
Internet	Noms de domaine Blocs de réseau Adresse IP spécifiques de systèmes accessibles par Internet Service TCP et UDP exécutés sur chaque système identifié Architecture système (exemple SPARC ou X86) Mécanisme de contrôle d'accès associé (listes ACL) Système de détection d'intrusion Recensement du système (noms des utilisateurs et des groupes, bannières système, tables de routage, information SNMP)
Intranet	Protocoles de réseaux utilisés (par exemple IP, Ipx, DecNET, etc.) Noms de domaines internes Blocs de réseau Adresses IP spécifiques de systèmes accessibles par Internet Service TCP et UDP exécutés sur chaque système identifié Architecture système (exemple SPARC ou X86) Mécanismes de contrôle d'accès et listes de com-mande d'accès associées (ACL) Système de détection d'intrusion Recensement du système (noms des utilisateurs et des groupes, bannières système, tables de routage, informations SNMP)
Accès à distance	Numéros de téléphone analogiques /numériques Type de système d'accès à distance Mécanisme d'authentification
Extranet	Origine et destination de la connexion Type de connexion Mécanisme de contrôle d'accès

Tableau 1 :

2.1.1.3 Détermination du champ d'activité de prise d'empreinte

La détermination du champ d'activité de prise d'empreinte commence par une recherche dans les sources ouvertes ; recherche d'informations susceptibles d'aider les pirates, par un parcours du site Web de l'organisation cible, voir les aspects suivants :

- Implantation ;
- Les sociétés et entités associées ;
- Les informations concernant les fusions ou des acquisitions ;
- Les numéros de téléphone ;
- Les noms de contacts et adresses électroniques ;
- Les politiques de sécurité et d'anonymat appliquées qui donnent des indications sur les types de mécanismes de sécurité mis en place ;
- Liens vers d'autres serveurs Web liés à l'organisation.

Examiner les pages Web à l'aide d'outils (Wget pour Unix ou téléport pour Windows)[1]
Recherche d'informations relatives à l'organisation cible dans les sources ouvertes (moteur de recherche) http://www.ferretsoft.com/ Exploitation simultanée de plusieurs moteurs de recherche.
Recherche dans EDGAR http://www.sec.gov/edgarhp.htm/[2] ; pour les objectifs qui sont des sociétés cotées en bourse (gestions des connexions Internet).
La sécurité des bases de données publiques reste la parade car bon nombre de ces informations sont destinées au publique d'où l'importance de déterminer les informations confidentielles. Manuel Site Security Hand book RFC 2196

2.1.1.4 Recensement des éléments de réseau

Les noms de domaine concrétisent la présence d'une société sur Internet ainsi il est important de recenser les domaines et d'identifier les réseaux auxquels ils sont reliés. "Whois". Tableau 3.

Mécanisme	Ressources	Plate-forme
Interface Web	http://www.networksolutions.com/ http://arin.net	Toute plate-forme équipée d'un client Web

[1] http://www.tenmax.com/teleport/pro/download.htm (prise d'empreinte "Windows") ftp://gnjlux.cc.fer.hr/pub/unix/util/wget (prise d'empreinte "Unix").
[2] La base de données EDGAR permet d'interroger des documents publics qui contiennent des informations importantes concernant le champ d'activités d'une organisation en identifiant des entités associées.

Client whois (annuaire)	Whois est fournis avec la plupart des versions d'UNIX. Fwhois a été créé par Chris Cappuccio ccappuc@santafe.edu	UNIX
WS Ping ProPack	http://ipswitch.com	Windows 95/NT
Sam Spade	http://www.blighty.com/products	Windows 95/NT
Interface Web Sam Spade	http://www.samspade.org	Toute plate-forme équipée d'un client Web
Outils Netscam	http://www.nwpsw.com	Windows 95/NT
Xwhois	http://www.goatnet.ml.org/software.html	UNIX avec X et boite à outils GTK+GUI

Tableau2 : Technique de recherches Whois et sources de données

Serveur Whois	Adresses
Attribution des adresses IP pour l'Europe	http://whois.ripe.net
Attribution des adresses IP pour l'Asie	http://whois.apnic.net
Organismes militaires américains	http://whois.nic.mil
Gouvernement Américain	http://whois.nic.gov

Tableau3 : Serveur Whois

La majorité des informations utilisées par les pirates pour amorcer leurs attaques sont fournies par les requêtes suivantes :

- Requête de registraire de nom de domaine (affiche des informations spécifiques relatives au registraire de nom de domaine et aux serveurs whois associés) Tableau 3.
- Requête d'organisation (Affiche toutes les informations relatives à une organisation donnée)
- Requête de domaine (Affiche toutes les informations relatives à un domaine donné)
- Requête de réseau (Affiche toutes les informations relatives à un réseau donné ou une adresse IP unique)[3]

[3] http://www.arin.net/whois/arinwhois.html

- Requête de point de contact. (Affiche toutes les informations relatives à une personne donnée)

Ainsi la sécurité des bases de données publiques est la parade. Mais il existe des mesures de sécurité qu'il convient d'appliquer pour rendre plus difficile la tâche des pirates.

- S'assurer que les renseignements fournis par la base de donnée sont exacts ;
- Mettre à jour les informations de contact d'ordre administratif, technique et comptable ;
- Examiner les numéros de téléphone et adresses fournis (départ d'attaque par voie téléphonique ou à des fin d'ingénierie sociale) « utilisation de numéro vert ou de numéro ne dépendant pas d'un central téléphonique ».

L'InterNIC authentifie l'identité de l'inscrit à l'aide de trois méthodes différentes :
Le champ DE (expéditeur) d'un courrier électronique, un mot de passe ou une clé PGP (Pretty Good Privacy). La méthode d'authentification par défaut est le champ DE d'un courrier électronique. Les conséquences en matière de sécurité de ce mécanisme d'authentification sont considérables. Car n'importe qui peut aisément falsifier une adresse électronique et modifier les informations associées à notre domaine. Cas d'AOL le 16 octobre 1998 rapporté par le Washington Post, où un imposteur s'est fait passer pour un représentant officiel d'AOL et a modifié les informations de domaine de façon à rediriger tous le trafic vers autonete.net. Il faut choisir une authentification plus sûre (mot de passe) ou une authentification PGP pour pouvoir modifier les informations de domaine.

2.1.1.5 Interrogation de serveurs DNS

Une fois les domaines associés identifiés, on peut commencer à interroger le serveur DNS.
Le serveur DNS est une base de données répartie utilisée pour mettre en correspondance des adresses IP avec des noms d'hôtes et vice versa. S'il est configuré sans les mesures de sécurités appropriées, l'obtention d'informations intéressante concernant l'organisation est possible.

2.1.1.6 Transfert de zone

Ne pas autoriser les utilisateurs Internet non validés à exécuter un transfert de zone DNS (un transfert de zone permet à un serveur maître de mettre à jour sa base de donnée de zone à partir du serveur maître principal (opération permettant d'exploiter des DNS redondants en cas

de panne du serveur de noms principal)). Lorsqu'une entreprise n'utilise pas de mécanisme DNS public/privé pour séparer les informations DNS externes de ses informations DNS privées, internes, les noms d'hôtes et les adresses IP internes sont dévoilés à l'assaillant. Ainsi fournir des informations d'adresses IP internes à un utilisateur non validé par Internet revient à fournir une copie, ou une carte, complète du réseau interne de l'entreprise.

Les informations DNS fournissent de nombreux renseignements aux pirates. Pour cela on réduit la quantité d'informations disponibles sur Internet ; au niveau de la configuration des hôtes on limite les transferts de zone uniquement vers les serveurs autorisés. Dans les versions moderne de BIND utilisation de xfernets du fichier named.boot pour l'application de ces restrictions.

Sur le plan réseau on configure un pare feu ou un routeur filtreur de paquets pour rejeter toutes les connexions entrantes non autorisées vers le port TCP 53. On configure les serveurs de nom externes de façon qu'ils fournissent uniquement les informations concernant les systèmes directement connectés à Internet.

2.1.2 Balayage systématique

Le balayage systématique consiste à frapper contre les murs de l'entreprise pour trouver toutes les portes et fenêtres, contrairement à la prise d'empreinte qui est la recherche d'information.

2.1.2.1 Sondages réseau de type ping

Il est important de détecter cette activité lorsqu'elle se produit. On peut aussi opter pour le blocage des sondages ping en fonction de la politique de sécurité de l'entreprise.

Effectuer une cartographie de réseau au moyen de sondages ping est une méthode éprouvée pour effectuer une reconnaissance de réseau avant de mettre en œuvre une attaque décisive. Dès lors, la détection d'une opération de sondage par ping est cruciale pour savoir si une attaque peut se produire et qui peut en être l'auteur. Les principales méthodes de détection

d'attaque par sondages ping sont des programmes IDS[4] de type réseau comme (NFR) Network Flight Recorder et snort[5] ou des mécanismes de type hôte.

Plusieurs utilitaires UNIX sont capables de détecter et d'enregistrer ces attaques. Généralement on les détecte par des paquets de type ICMP ECHO provenant d'un système ou d'un réseau de données. Il faut alors suivre de près cette activité, car il peut s'agir d'une reconnaissance du réseau et indiquer une attaque imminente.
Il existe sur Windows un produit gratuit ou diffusé en shareware "Genius 3.1"[6]. Genius ne détecte pas les balayages ICMP ECHO vers un système, il détecte les sondages ping TCP sur un port donné. Le produit commercial de détection de sondage de ports TCP est Black ICE de Network ICE www.networice.com.

Il est important d'étudier attentivement le trafic ICMP que l'on autorise. L'une des méthodes de prévention les plus efficaces est de bloquer les types ICMP qui fournissent des informations au niveau des routeurs frontières. On doit au moins empêcher les requêtes de paquets TIMESTAMP (ICMP type 13) et ADRESS MASK (ICMP type 17) d'accéder au réseau.

2.1.2.2 Balayage systématique de ports

Le balayage systématique des ports est une opération qui consiste à se connecter aux ports TCP et UDP du système cible pour déterminer les services qui sont en cours d'exécution ou en état de veille (LISTENING). L'identification des ports en Veille est importante pour déterminer le type de système d'exploitation et les applications utilisées.

Détecter des activités de balayage de ports est essentiel pour savoir à quel moment une attaque peut être lancée et par qui. Les principales méthodes de détection de balayages systématique de ports sont des programmes IDS de type réseau comme NFR ou un mécanisme basé sur l'hôte. Tableau 4

Outil de balayage	TCP	UDP	Furtif	Ressource
UNIX				
Strobe	×			ftp://ftp.freeBSD.org/pub/FreeBSD/ports/distfiles/strobe-1.06.tgz

[4] http://www.securite.org/db/securite/ids
[5] http://www.snort.org/ et http://www.indiesoft.com
[6]