Sécurité des systèmes d'information

Introduction

Plan de la présentation

- Présentation d'un SI et de son bon fonctionnement
- Pourquoi un besoin spécifique en sécurité

Théorie de l'information

- Les différents stades de l'information
  - Données
  - Information
  - Connaissance
- Le patrimoine d'une entreprise est l'ensemble des processus permettant le passage de données à connaissances

Les systèmes d'information (SI)

- Un système d'information: l'ensemble des moyens de traitement de l'information d'une organisation
  - Du modem aux PC
  - Réseau téléphonique
  - ...
- Permettant l'optimisation des processus de passage de données brutes à connaissances

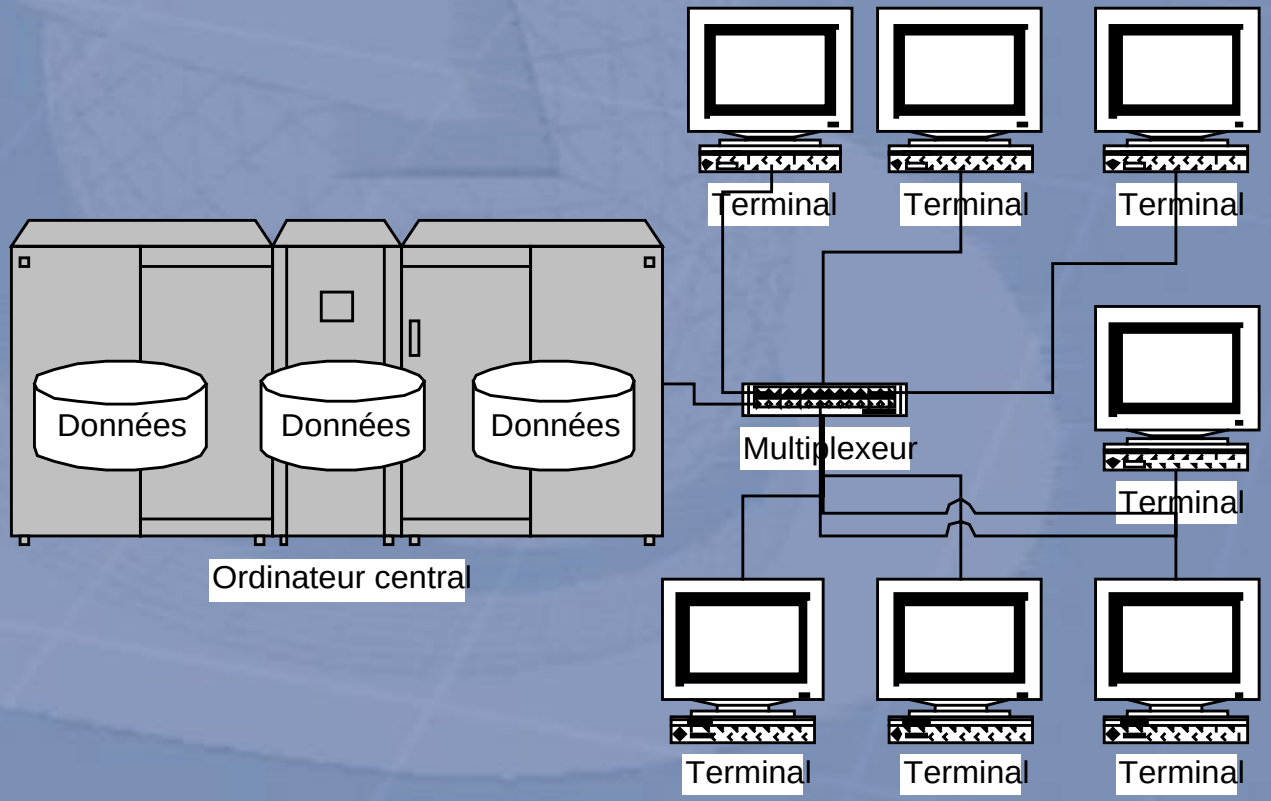
Historique des SI (1)

- Années 70 et 80: systèmes d'information centralisés
  - Autour de calculateurs
  - Le système est conçu par l'informaticien pour l'informaticien
  - Les postes des utilisateurs du système sont des terminaux passifs vers les calculateurs

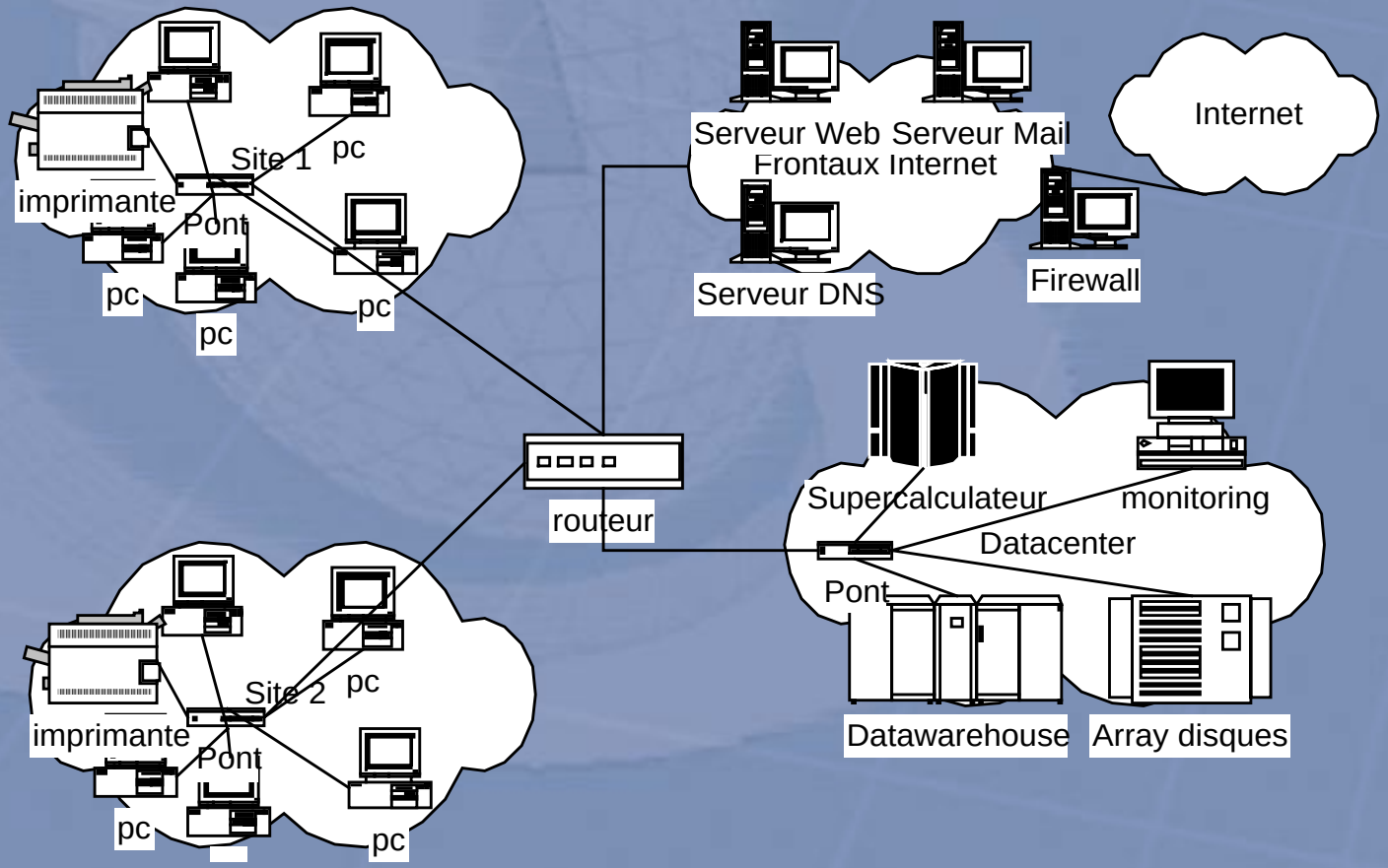
Historique des SI (2)

- Années 90 à ???: systèmes d'information étendus
  - Tout le monde est (sur)équipé!
  - Environnement hétérogène: du PC au datawarehouse
  - Le réseau est omniprésent: privé (LAN/WAN) et publique (Internet)

Historique des SI (3)



Historique des SI (4)



Historique des SI (5)

- Raisons de cette évolution
  - De + en + d'utilisateurs du SI, demandant de + en + de ressources
  - Utilisateurs avides de fonctionnalités gourmandes (interfaces graphiques)
  - Modèle centralisé non adapté à cette demande croissante
    - Augmentation des performances difficile et chère pour des machines simples
    - Apparition d'alternatives économiques: les postes de travail PC

Constatations actuelles

- Complexité grandissante des logiciels
- Course à la puissance et aux fonctionnalités entretenues par l'industrie hard et software
- Interconnexion totale grâce aux réseaux
- SI actuels déséquilibrés:
  - Ressources (humaines, matérielles, ...) éparpillées
  - Forts héritages historiques (notamment, absence de sécurité)

Bon fonctionnement

- La sécurité s'inscrit dans le bon fonctionnement du SI
- Elle fait partie des propriétés à assurer pour contenter les utilisateurs
- La sécurité est souvent vue *(par erreur)* comme une contrainte

Fiabilité

- Fiabilité des matériels et logiciels
  - Le matériel/logiciel fait ce qu'on lui demande, et uniquement ce qu'on lui demande
  - Il le fait bien

Performance et disponibilité

- Au minimum gênant lorsque le SI est un outil, critique lorsque le SI est le moyen de production
  - *Poste de la secrétaire* : on ressort le papier
  - *Startups* : avant la crise, certaines sociétés n'auraient pas survécu à une interruption de service de 6 heures...

Protection des informations

- Informations stockées ou échangées
  - ➔ Assurer leur *confidentialité*
  - ➔ Et leur *intégrité*

Protection des accès

- Seules les personnes autorisées peuvent accéder au système
- Seules les personnes habilitées à faire une action peuvent la réaliser
  - ➔ *Autorisation*

Confiance entre acteurs

- Confiance en l'identité du correspondant
- Assurance de non compromission de cette identité

  ➔ *Authentification*

Concepts de base de la sécurité

- Assurer:
  - La fiabilité
  - La disponibilité
  - L'authentification
  - L'autorisation
  - L'intégrité
  - La confidentialité

Dans la suite du cours, nous nous occuperons d'étudier les caractéristiques de ces 4 derniers (authentification, autorisation, intégrité, confidentialité)

Pourquoi un besoin spécifique en sécurité ? (1)

- Logiciels / matériels non pensés sécurité
  - Nombreuses failles publiques ou non
  - Systèmes historiquement et par défaut ouverts
- Nécessité de diagnostiquer et parer ces failles
  - Rôle de l'industrie de la sécurité: fournir des moyens pour minimiser l'impact des failles des autres (!!!)

Pourquoi un besoin spécifique en sécurité (2)

- À des fins de préservation des avantages concurrentiels
  - Préserver l'outil informatique
  - Préserver ses données confidentielles (secrets de fabrication, délits d'initiés, ...)

Mais aussi ...

- Obligation légale de protection des données
  - Données nominatives ou privées (CNIL)
  - Atteinte aux droits d'autrui: droits d'auteurs, protection des mineurs, racisme, provocation, ...
- Autres contraintes légales
  - Surveillance des employés
  - Implication involontaire dans des affaires de piratage (rebonds)

L’affaire de tous

- La sécurité est l’affaire de tous
  - Des RSSI, administrateurs systèmes, développeurs aux utilisateurs
- Dans un objectif de minimisation des risques sécurité