

Les principes de la sécurité

Critères fondamentaux

Introduction

- ▶ La sécurité informatique est un domaine vaste qui peut appréhender dans plusieurs domaines
 - ▶ Les systèmes d'informations
 - ▶ Les réseaux informatiques
 - ▶ Les accès physiques à des salles machines
- ▶ Nous nous concentrerons sur les aspects relatifs aux systèmes informatiques et réseaux

Les critères fondamentaux

- ▶ Les solutions de sécurité doivent contribuer à satisfaire au moins les critères suivant:
 - ▶ la disponibilité: la probabilité de pouvoir mener correctement à terme une session de travail
 - ▶ l'intégrité
 - ▶ la confidentialité

La disponibilité

- ▶ La disponibilité est de pair avec son accessibilité
 - ▶ Une ressource doit être accessible, avec un temps de réponse acceptable
- ▶ La disponibilité des services, systèmes et données est obtenue
 - ▶ par un dimensionnement approprié
 - ▶ par une gestion opérationnelle des ressources et des services
- ▶ Ce paramètre est mesuré par une montée en charge du système afin de s'assurer de la totale disponibilité du service
- ▶ Un service doit aussi être assuré avec le minimum d'interruption en respect avec l'engagement établi
- ▶ De plus des pertes de données sont possibles si l'enregistrement et le stockage ne sont pas gérés correctement, d'où l'importance d'une haute disponibilité d'un système et de la mise en place d'une politique de sauvegarde

L'intégrité

- ▶ L'intégrité permet de certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle
- ▶ L'altération est principalement occasionnée par le média de transmission mais peut provenir du système d'informations
- ▶ Il faut également veiller à garantir la protection des données d'une écoutes actives sur le réseau

La confidentialité

« **La confidentialité est le maintien du secret des informations** » (Le Petit Robert)

- ▶ Dans le cadre d'un système d'information, cela peut être vu comme une protection des données contre une divulgation non autorisée
- ▶ 2 actions complémentaires permettant d'assurer la confidentialité des données
 - ▶ Limiter leur accès par un mécanisme de contrôle d'accès
 - ▶ Transformer les données par des procédures de chiffrement

L'identification et l'authentification

- ▶ L'identification de l'auteur d'un document peut être aisée par contre être en mesure d'assurer l'authenticité du document est chose plus délicate
- ▶ Ces mesures doivent être mises en place afin d'assurer
 - ▶ La confidentialité et l'intégrité des données d'une personne
 - ▶ La non répudiation, c'est à dire qu'une personne identifiée et authentifiée ne peut nier une action
- ▶ L'identification peut être vu comme un simple login de connexion sur un système
- ▶ L'authentification peut être un mot de passe connu seulement par l'utilisateur

La non-répudiation

- ▶ La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu
- ▶ A cette notion sont associées
 - ▶ L'imputabilité: une action a eu lieu et automatiquement un enregistrement, preuve de l'action, est effectué
 - ▶ La tracabilité: mémorisation de l'origine du message
 - ▶ L'auditabilité: capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement.
- ▶ L'existence de fichiers journal permet de garantir l'imputation et l'auditabilité

Les principes de la sécurité

Domaines d'applications

Les domaines de la sécurité

- ▶ Tous les domaines de l'informatique sont concernés par la sécurité d'un système d'information
- ▶ En fonction de son domaine d'application, la sécurité informatique se décline en
 - ▶ Sécurité physique
 - ▶ Sécurité de l'exploitation
 - ▶ Sécurité logique
 - ▶ Sécurité applicative
 - ▶ Sécurité des télécommunications

La sécurité physique

- ▶ Concerne tous les aspects liés de l'environnement dans lequel les systèmes se trouvent
- ▶ La sécurité physique passe donc par
 - ▶ Des normes de sécurité
 - ▶ Protection de l'environnement (incendie, température, humidité, ...)
 - ▶ Protection des accès
 - ▶ Redondance physique
 - ▶ Plan de maintenance préventive (test, ...) et corrective (pièce de rechange, ...)
 - ▶ ...

Sécurité de l'exploitation

- ▶ Rapport à tous ce qui touche au bon fonctionnement des systèmes
- ▶ Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic et de mise à jour
- ▶ La sécurité de l'exploitation dépend fortement de son degré d'industrialisation qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches
- ▶ Quelques points clés de cette sécurité
 - ▶ Plan de sauvegarde, de secours, de continuité, de tests
 - ▶ Inventaire réguliers et si possible dynamique
 - ▶ Gestion du parc informatique, des configurations et des mises à jour
 - ▶ Contrôle et suivi de l'exploitation
 - ▶ ...

La sécurité logique

- ▶ La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel
- ▶ Elle repose sur la mise en oeuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation
- ▶ Elle repose également sur
 - ▶ les dispositifs mis en place pour garantir la confidentialité dont la cryptographie
 - ▶ une gestion efficace des mots de passe et des procédures d'authentification
 - ▶ Des mesures antivirus et de sauvegarde des informations sensibles
- ▶ Pour déterminer le niveau de protection nécessaire aux informations manipulées, une classification des données est à réaliser pour qualifier leur degré de sensibilité (normale, confidentielle, top secrète, ...)

La sécurité applicative

- ▶ Faire un développement pertinent et l'intégrer harmonieusement dans les applications existantes
- ▶ Cette sécurité repose essentiellement sur
 - ▶ Une méthodologie de développement
 - ▶ La robustesse des applications
 - ▶ Des contrôles programmés
 - ▶ Des jeux de tests
 - ▶ Un plan de migration des applications critiques
 - ▶ La validation et l'audit des programmes
 - ▶ Un plan d'assurance sécurité
 - ▶ ...

La sécurité des télécommunications

- ▶ Offrir à l'utilisateur final une connectivité fiable et de qualité de « bout en bout »
- ▶ Il faut donc mettre un canal de communication fiable entre les correspondants, quels que soient le nombre et la nature des éléments intermédiaires
- ▶ Cela implique la réalisation d'une infrastructure réseau sécurisée au niveau des accès, des protocoles de communication, des systèmes d'exploitation et des équipements

Les principes de la sécurité

Les facettes de la sécurité

Diriger la sécurité

- ▶ La sécurité informatique passe par la définition d'une politique de sécurité et la formation du personnel
- ▶ Elle est en constante évolution et se traduit par un problème de gestion de la qualité constante lié pour l'essentiel à la maintenabilité et à l'évolution des systèmes, des enjeux et des risques
- ▶ Dans de nombreuses entreprises, l'outil informatique est essentiel dans son développement, le moindre dysfonctionnement constitue donc un risque majeur

Le juridique

- ▶ La responsabilité des acteurs (responsable sécurité, ...) est de plus en plus invoquée lors de sinistre où les ressources informatiques qu'ils gèrent sont l'objet ou le moyen d'une fraude
- ▶ Il est donc nécessaire de pouvoir prouver que des mesures sont pourtant prise pour sécuriser le système afin de se protéger contre un délit de manquement à la sécurité
 - ▶ A défaut d'une obligation de résultat, les responsables de systèmes informatiques ou sécurité ont une obligation de moyens
- ▶ Les responsables d'entreprises doivent également être extrêmement attentifs à l'égard du droit des nouvelles technologies

Architecture de sécurité

- ▶ Elle permet de visualiser toutes les dimensions de la sécurité
 - ▶ Dimension technique et opérationnelle
 - ▶ Sécurité matérielle
 - ▶ Sécurité environnementale
 - ▶ Sécurité des télécommunications ...
 - ▶ Dimension organisationnelle et économique
 - ▶ Méthodologie
 - ▶ Budget
 - ▶ Evaluation ...
 - ▶ Dimension humaine
 - ▶ Surveillance
 - ▶ Ethique
 - ▶ Formation ...
 - ▶ Dimension juridique et réglementaire

Architecture de sécurité

- ▶ Cette architecture est indispensable si l'on veut prendre en compte l'ensemble des problèmes de sécurité d'une entreprise
- ▶ Elle permet d'identifier les critères minima de sécurité pour chacun des éléments
- ▶ Permet également d'harmoniser le niveau de sécurité dans toutes les dimensions

Les principes de la sécurité

Les attaques via internet

Réalisation d'une attaque

- ▶ La première phase est la collecte d'information et la recherche de vulnérabilité
- ▶ Phase 2: savoir-faire et exploitation des informations recueillies et des failles
- ▶ Phase 3: création de l'attaque
 - ▶ débouche sur l'intrusion
- ▶ Phase 4: exfiltration
 - ▶ rester anonyme et donc ne pas laisser de trace sur le système
 - ▶ utiliser l'identité d'une autre personne connu du système

Typologie des attaques

- ▶ Les attaques sont le plus souvent basées sur l'usurpation de paramètres de connexion, de mots de passe, sur le leurre et l'exploitation de failles et de vulnérabilités
- ▶ Les attaques qui modifient les données sont dites actives, tandis que les autres, relevant de l'écoute de données sans altération sont qualifiés de passives

Appropriation de mots de passe

- ▶ Tout simplement par l'utilisateur qui lui révèle son mot de passe ou parce ce mot de passe est beaucoup trop évident
- ▶ Utilisation d'une complicité
- ▶ Il peut leurrer les utilisateurs, par téléphone ou email, en se faisant passer pour l'administrateur du réseau (domaine du *social engineering*)
- ▶ Par écoute passive du réseau, d'où l'utilité de chiffrer les mots de passe pendant les transferts ou de ne pas les transmettre
- ▶ En cas de découverte de mots de passe cryptés, le pirate va tenter de les découvrir par brute force ou par dictionnaire
- ▶ Utilisation de cheval de Troie
 - ▶ programme qui substitue au programme de connexion pour la première connexion uniquement, ensuite il redonne la main de bon programme de connexion. Cette technique évite d'attirer l'attention sur un éventuel dysfonctionnement
- ▶ Activation d'un périphérique comme un micro ou une webcam à l'insu de l'utilisateur

Attaques fondées sur le leurre

- ▶ Basé sur les sources de vulnérabilités des environnements Internet
- ▶ Les leurre permettent
 - ▶ d'usurper les identités des utilisateurs ou des adresses IP
 - ▶ de voler des sessions TCP
- ▶ Elles exploitent les propriétés de certains protocoles de communication

Le détournement des technologies

- ▶ Une attaque conduisant à un déni ou refus de service peut être réalisée en sollicitant excessivement des ressources
- ▶ Les attaques occasionnant un déni de service sont considérées par la loi comme un acte criminel
- ▶ Il existe les inondations de messages (e-mail bombing) qui consiste à submerger la boîte aux lettres électronique d'un utilisateur par un grand nombre de messages

Manipulation d'information

- ▶ Cela consiste à modifier la page d'accueil d'un site web
- ▶ Pour l'entreprise victime de ces attaques, les répercussions peuvent être nombreuses
 - ▶ réputation et confiance mises en cause
- ▶ Modification du contenu d'un article de presse sur un site d'information
 - ▶ ces actions de désinformation relèvent de l'infoguerre (*infowar*) et permettent de mener des attaques sémantiques (touchent le sens des informations)