Résumé livre : Sécurité informatique et réseaux

Les principes de sécurité

Disponibilité

- Accessibilité, temps de réponse acceptables, capacité => dimensionnement approprié
- tests de montée en charge
- SLA continuité de service,
- politique de sauvegarde (coût entre de sauvegarde vs risque d'indisponibilité supportable par l'organisation)

Intégrité

- Certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle.
- N'ont pas été modifiées lors de leur stockage ou de leur transfert.
- Sont protégées des écoutes actives qui peuvent modifier les données interccceptées

Confidentialité

- Protection des données contre une divulgation non autorisée
- Limiter leurs accès par un mécanisme de contrôle d'accès
- Transformer les données par des procédures de chiffrement

Authentification et Identification

Mises en œuvre pour contribuer à réaliser les mesures de sécurité assurant :

- Confidentialité et intégrité : seuls les ayant droit peuvent accéder aux ressources
- non-répudiation et imputabilité : preuve de l'origine d'un message, d'une transaction, preuve de la destination.

Non-répudiation / imputabilité / traçabilité

- Auditabilité : capacité d'un système à garantir la présence des informations nécessaires à une analyse ultérieure d'un événement.
- Log / journal => durée de rétention ?

Domaines d'application de la sécurité

Sécurité physique et environnementale

Sécurité logique

- Contrôle d'accès
- Classification des données pour qualifier leur degré de sensibilité

Sécurité applicative

Sécurité de l'exploitation

- Maintenance doit être préventive et régulière
- Risque d'exploitation : remplacement des équipements, interruption de service, perte de données
- Adéquation du niveau de service offert, par rapport à celui spécifié dans le contract

Sécurité des télécommunications

- Offrir à l'utilisateur, une connectivité fiable et de qualité de « bout en bout »
- Un environnement de communication sécurisé implique la sécurisation de tous les éléments de la chaîne informatique.
- Un système sécurisé, mobilisant d'importants moyens sécuritaires, aussi pertinents soient-ils, ne pourra être efficace que s'il s'appuie sur un code d'utilisation des ressources informatique formalisé par une charte (page 12)
- Enjeux économique et politiques

Facettes de la sécurité

- Maîtrise de la sécurité informatique, procédures qui régissent leurs utilisations et configuration.
- La sécurité repose sur des axes complémentaires managériaux, techniques et juridiques qui doivent être abordés en parallèle. Elle n'est jamais acquise définitivement.
- Veille juridique
- Actions d'information et de formation, mesures préventives et dissuasives
- SCHEMA p13

Attaques

1) Collecte d'informations, Recherche de vulnérabilités
2) Savoir-faire et exploitation des informations recueillies et des failles (0day exploit)
3) Création d'une attaque
4) Exfiltration (ne pas être détecté, effacer traces)

Active (D I A) / passives (C)

Brut force, dictionnaire, cheval de troie, faiblesse des mots de passé

=> mot de passe à usage unique

Déni / Refus de service

La criminalité informatique

Classiques ou brèches ouvertes par les technologies de traitement de l'information

Internet comme facteur de performance pour le monde criminel

Problème de poursuite, car les tarces sont immatérielles

Les solutions de sécurité sont des réponses statiques à un problèmes dynamique mais surtout des réponses d'ordre technologique à des problèmes humains, managériaux et légaux.

Le niveau de sécurité des infrastructures résulte donc d'un compromis entre ces facteurs :

- Coût
- Niveau de service de sécurité
- Temps de livraison

Dimension humaine difficilement contrôlable

Atteritorialité d'Internet

Maîtrise des risques par l'intégration dans leur management, de la notion de gouvernance de la sécurité

Dématérialisation

Usurpation d'identité, leurre, accès indus, exploitation frauduleuse de ressources, infection, détérioration, destruction modification, divulgation, déni de service, vol

Notion de donnée d'origine n'a plus de sens puisque les copies à l'identique et à l'infinie sont possibles.

Disponibilité d'outils

Information immatérielle, support physique => vulnérabilités

Universalisation et dépendance

SCHEMA p27

Liste p35

Intimité numérique

- La sécurité passe par la surveillance, le contrôle et le filtrage des communications.
- Garde-fous pour éviter les abus
- Intimité, confidentialité de données à caractère personnel
- Protection de la vie privé / respect des droits fondamentaux

Types

- Virus, spam, phising => e-mails
- Intrustion de systems => détecter/ plans d'action, réaction=> limiter la propagation d'une attque, réduire les impacts, réparer les atteintes ou dégâts engendrés.
- Chantage => souvant pas annoncé

La stratégie de sécurité

Connaître les risques pour les maîtriser

- Aucune préjudice ne doit mettre en péril la pérennité de l'entreprise

- Protection, organisation de la défense (démarche proactive), plans de réaction (démarche réactive)
- Prévention, protection, réaction

1) Identifier les valeurs => de la pertinence de l'analyse des risques dépendera l'identification correcte des moyens et des mesures de sécruité à mettre en œuvre pour protéger efficacement les ressources du sytème d'information.
2) Mettre en place les outils et les procédures nécessaires à la gestion des risques et à la sécurité des systèmes, services et données
3) Contrôler l'adéquation, pertinence, évaluation périodique voire constante, optimisation

Stratégie de sécurité

- Critères fondamentaux, DIC A NR, pérennité, intimité numérique
- Sont déterminées, gérées et validées par des procédures de gestion => acte de management
- Réduire la sécurité à sa dimension technologique est assurer son échec
- Page 57 PRINCIPES
- La stratégie relève du domaine de la direction générale
- La sécurité un facteur de compétitivité contribuant à une meilleure rentabilité, facteur de qualité
- La sécurité ne permet pas directement de gagner de l'argent, mais évite d'en perdre.
- Problème : il n'existe pas de critère objectivement mesurable du rendement du capital investi et du retour sur investissement en sécurité.
- La diversité et le nombre de solutions peuvent créer un problème de cohérence globale de l'approche sécuritaire. En conséquence, la technologie ne suffit pas, elle doit être intégrée dans une démarche de gestion.

La politique de sécurité

La gestion des risques constitue le point de départ de l'analyse des besoins sécuritaires.

Bonne politique : complète et cohérente, afin de répondre précisément aux besoins de sécurité de l'organisation dans un contexte donné.

La définition de la politique de sécruité :

- Simple et compréhensible
- Adoptable par un personnel préalablement sensibilisé voire formé
- Aisément réalisable
- Maintenance facile
- Vérifiable et contrôlable
- Évolutive
- Configurable / personnalisable

Normes voir slides :

- Les normes ou méthodes n'évoluent pas au même rythme que les besoins ou les technologies.

Classement de l'information : publique, financier, privée, secrète

Mesures de sécruité

Avant le sinistre

- Mesures préventives
- Mesures structurelles
- Mesures de dissuasion

Après le sinistre

- Mesures palliatives et correctives
- Mesures de récupération

Plan de secours

1) Analyse stratégique
2) Choix des solutions
3) Réalisation (mise en œuvre opérationnelle)
4) Validation et suivi
   Audit

Critères communs

Acteurs

- Utilisateurs : connaît niveau de sécurité offert par un produit
- Développeurs : identification des exigences de sécurité
- Évaluateurs : label standardisé, confiance accorder à l'organisation de certification ?

Toutefois le champ d'application et l'intérêt du label restent faibles au regard de la lourdeur de la démarche de certification.

Label statique attribué à un instant donné pour une version spécifique d'un produit.

La sécurité par le chiffrement

Cryptographie : écrire l'information (son, images, textes) en la rendant inintelligible à ceux ne possédant pas les capacités de la déchiffrer.

Garder un algorithme secret ne renforce pas sa sécurité

Chiffrement symétrique

Autant de paires différentes de clés qu'il y a de paires de correspondant !

Reste voire slides

La sécurité des infrastructures de télécommunication

On ne peut assurer la sécurité que dans un mode connecté

L'association de sécurité est unidirectionnelle, deux associations de sécurité sont alors nécessaires pour supporter un échange bidirectionnel.

Mode transport vs mode tunnel (nouveau paquet IP dans le paquet IP)

Il est impératif de pouvoir distinguer ces deux types de données « données de contrôle du protocole » et « données de l'utilisateur » pour pouvoir chiffrer ces dernières et les rendre confidentielles, sans pour autant chiffrer les premières afin que le protocole puisse effectuer sa tâche et que les données soient effectivement transférées.

La sécurité par les systèmes pare-feu et de détection d'intrusions

Le premier stade de la sécurité d'un intranet passe donc par un bon dimensionnement et un bonne gestion du réseau de l'entreprise.

Ne pas introduire des vulnérabilités supplémentaires en autorisant l'interconnexion de son intranet à l'Internet.

L'intranet facilite et banalise l'accès aux sources de données => contrôler et autoriser l'accès

Firewall

Le firewall constitue un des outils de réalisation de la politique de sécurité et n'est qu'un des composants matériel ou logiciel de sa mise en œuvre. En effet, un firewall ne suffit pas à bien protéger le réseau et les systèmes d'une organisation. Il doit être également accompagné d'outils, de mesures et de procédures répondant à des objectifs de sécurité préalablement déterminés par la politique de sécurité. L'efficacité d'un firewall dépend essentiellement de son positionnement par rapport aux systèmes qu'il doit protéger, de sa configuration et de sa gestion.

Principes : filtrage, masquage, relais

Système de détection d'intrusions (IDS)

- Collecte des informations
- Analyse des informations récupérées
- Détection des intrusions et les réponses à donner suite détection

Méthode basées sur les signatures => doit déjà connaître

Méthode basées sur les profils => basées sur la comparaison d'événement collectés par rapport à des profils de comportement normaux associés à des utilisateurs ou à des applications

- Filtre trop grand =>faux négatif
- Filtre trop restrictif => faux positif

Réponses

Actives :

- entreprendre une action agressive contre l'intrus (illégale)
- restructurer l'architecture du réseau (isoler)
- surveiller le système attaqué

Passives : collection d'information

La sécurité des applications et des contenus

Il faut que les informations sensibles le soient tout au long de la chaîne de traitement et de leur durée de vie. En effet, le vendeur doit assurer leur confidentialité lors de leurs stockages et durant les demandes d'autorisation de paiement (paiement par carte sur internet).

DRM => grands problèmes d'interopérabilité, mais donne du contrôle des médias aux organisations.

La sécurité par la gestion de réseaux

Les administrateurs réseaux comme le personnel technique interviennent comme des pompiers pour parer au plus pressé par des actions de patch & fix. Dans ce contexte, on a donc tout à gagner à travailler avec des produits dont on connaît l'avance le niveau de sécurité qu'ils offrent lorsqu'ils sont certifiés critères communs par exemple.

Cohérence globale des services et la non-redondance excessive => proportionnelle aux risques encourus

Authentification :

- Ce que l'on connait (code)
- Ce que l'on possède (carte)
- Ce que l'on est (biométrie)

Les solutions de sécurité ont aussi besoin d'être protégées et sécurisées => récursivité des solutions de sécurité et leur problème.

Serveurs de nom (login) : backup, testé pour une haute charge,…

Biométrie : problèmes du stockage de l'enregistrement, ainsi que du besoin d'approximation

Mise en place du contrôle d'accès

1) Identification des besoins
2) Recherche et analyse de scénarios possibles
3) Proposition et validation d'un scénario
4) Plan d'action et élaboration d'un cahier des charges
5) Mise en œuvre de la solution

Gestion du parc informatique

One ne gère bien et on ne sécurise bien que ce que l'on connaît bien => recensement le plus exhaustif possible des actifs informatiques de l'entreprise.

Indicateur de qualité

Disponibilité, capacité, accessibilité, temps de réponse, fiabilité

La non-documentation crée ou maintient une dépendance très forte entre l'entreprise et ses administrateurs réseau => estimation du dégrée de détail