Sécurité des Systèmes d'Information
Le processus d'audit et le facteur humain

Martin Peres

Doctorant de Francine Krief au LaBRI

April 23, 2012

Sommaire

Système d'information (SI)

- donne accès à des informations
- uniquement aux personnes à qui elles sont destinées
- n'est pas pas limité à l'informatique (courrier classique, dépôt physique, etc...)!

Les différentes composantes du système d'information

En suivant la théorie du contrôle d'accès:

- Sujet: Humains
- Objet: information (informatiques ou physiques)
- Opération: Lire(confidentialité) ou écrire(intégrité)

Chaîne d'acquisition d'une information

- humain
- interface (terminal informatique ou un autre humain)
- application/base de donnée

Conclusion

Un système d'information rend service à un humain et est attaqué par un autre pour profiter de privilièges qui ne lui étaient pas accordés :
$--> $ On doit prendre le facteur humain en compte lors de la conception et la sécurisation d'un SI.

Problèmes d'un système d'information inadapté

- sous-optimalité de la productivité
- système inadapté = système contourné
- perte de contrôle sur les flux d'information(vous laissez les utilisateurs faire)
- $--> $ vous n'êtes plus RSSI car vous ne comprenez plus le SI

Exemple de perte de contrôle sur les flux d'information

- pas de procédure d'échange de fichiers:
  - transfert par clés USB
  - perte de la-dite clé: confidentialité compromise
  - Solution: serveur de partage de fichier
- pas de procédure de sécurité physique
  - les visiteurs rentrent dans l'entreprise
  - vol (im-/)matériel de données
  - Solution: politique de compartimentation et d'accréditation

Qui a accès à toute l'entreprise?

- Les patrons
- Les gardiens de nuit
- Les femmes de ménage

Qui est le plus susceptible de "fuiter"?

- Tous: Fuite par négligence/incompréhension (social engineering)
- Les femmes de ménage: Revente d'informations (salaire faible = forte motivation)

Conclusion

- Loggez tout sur un serveur dédié pas accessible en lecture!

Audit d'un système d'information

- avoir une vue complète du système
  - centraliser les besoins utilisateur
  - centraliser les ressources disponibles
  - centraliser les services rendus
- mesurer l'adéquation des besoins à la demande
- proposer des modifications (concertation avec les utilisateurs impactés)
- appliquer les modifications
- recommencer (processus itératif)

Implications pratiques pour un DSI

- Être avant tout à l'écoute de ses utilisateurs
- Savoir identifier les vulnérabilités d'un système par rapport aux menaces pesant sur l'entreprise
- Proposer des améliorations au SI pour s'adapter aux besoins et mitiger les risques
- Tenir à jour un guide de bonnes pratiques (doit être simple)

Se tenir à jour

- Suivre des mailing lists et des sites webs concernant l'administration et la sécurité des SI
- Parler avec d'autres DSI
- Aller à des conférences pour suivre les tendances (RMLL, FOSDEM, autres...)

Approche normalisée à la sécurité

- Apporte un cadre au processus d'audit
- Permet d'obtenir des certifications
- Aide à convaincre la direction de l'entreprise
- Facilite la reprise d'un audit

Normes existantes

- Suite ISO 9000: Démarche qualité, trop général
- Suite ISO 20000 (ITIL): axé qualité des SI
- Suite ISO 27000 et EBIOS: axé sécurité

ISO 20000

Qualité des systèmes d'information. Découpé en 2 parties:

- définition précise du fonctionnement de l'entreprise
- procédure pour atteindre les résultats attendus

Cycle de Deming (PDCA)

- Plan : l'entreprise va planifier
- Do : Faire
- Check : Contrôler et vérifier
- Act : Rechercher des points d'amélioration

ISO 27000

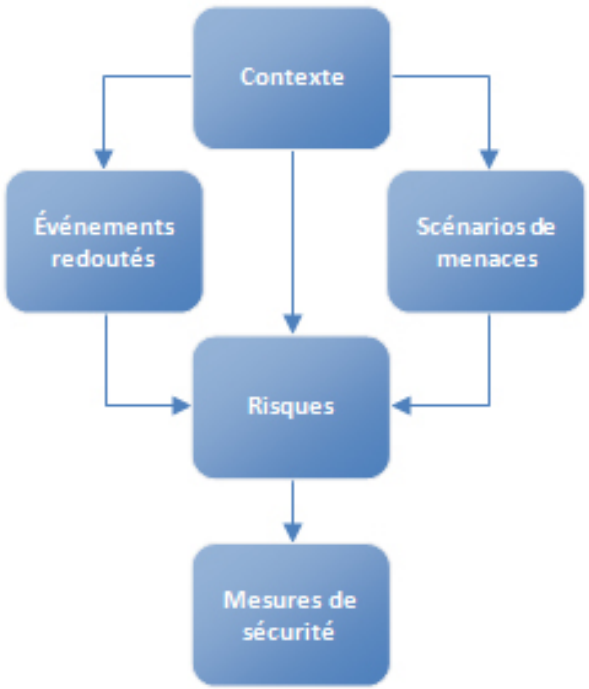
Sécurité des systèmes d'information

- suite de recommandation pour la sécurité
- améliore le processus de démarrage
- d'amélioration
- et de maintient de la sécurité

EBIOS

Sécurité des systèmes d'information

- Expression des besoins et identification des objectifs de sécurité
- défini par l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information)



Sommaire

Les Humains

Motivation: Attaquer le maillon le plus faible d'un SI. C'est généralement l'humain:

- Animal social (fait confiance)
- Rationalité limitée (premier choix acceptable)
- Se croit supérieur aux autres, effet Dunning–Kruger:
  - Above average effect
  - Worse-than-average effect
- Principe de Peter: Un employé s'élève à son niveau d'incompétence
- Fort coût de synchronisation (Le mythe du mois-homme)

Les sauvegardes

Motivation: Répliquer pour éviter de perdre des données. Les risques sont qu'un humain:

- 1) N'en fasse pas du tout (se croire supérieur)
- 2) Écrase une valide par une invalide (erreur d'inattention)

Les sauvegardes: Exemple de solutions

- 1) Montage des répertoire home en NFS ou Samba pour centraliser les données
- 2) Versionnement des sauvegardes pour revenir dans le temps
  - Chaque modification est loggée: GIT/SVN/...
  - Snapshot périodique: Filesystem (ZFS, BTRFS) ou réseau

Le Social Engineering

L'ingénierie sociale (ou social engineering en anglais) est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations clefs. Cette pratique exploite les failles humaines et sociales de la structure cible, à laquelle est lié le système informatique visé. Utilisant ses connaissances, son charisme, l'imposture ou le culot, le hacker abuse de la confiance, de l'ignorance ou de la crédulité des personnes possédant ce qu'il tente d'obtenir.
Source: Wikipedia
À lire: L'art de la supercherie, Kevin Mitnick

Exemple d'attaque numéro 0: Le pishing

Plusieurs formes exploitant la rationalité limitée et l'animal social:

- Imitation de site de confiance: Vol d'identité / coordonnées bancaires
- Rendre un service: Installation d'un trojan

Exemple: `http://downloadyoutubevideo.org/`

TD: Étude de cas

Pour les 4 cas suivant, vous devez :

- identifier les menaces pensant sur l'organisation
- identifier les vulnérabilités
- détailler l'attaque

Le mac do

Voir: `https://www.youtube.com/watch?v=27NX_MMIkLY`

- Motivation: Manger gratuitement
- Menace pour macdo: travailler à perte
- Vulnérabilité: Pas d'association entre une personne et sa commande
- Vulnérabilité de fond: Animal Social

Hacker

Voir: `https://www.youtube.com/watch?v=_G3NT91AWUE`

- Motivation: Accéder à des informations
- Moyen: Se renseigner sur l'entreprise et faire du name-dropping, jouer sur les peurs
- Menace: Violation de confidentialité/intégrité de fichiers vitaux
- Vulnérabilité: Pas de formation au gardien de nuit (pas de tentative d'authentification)
- Vulnérabilité de fond: Animal Social

Attaque interne

Voir: `https://www.youtube.com/watch?v=Y6tbUNjL0No`

- Motivation: Vol d'informations (im)matérielles
- Moyen: Se faire passer pour un collègue de Bureau
- Menace: Violation de confidentialité/intégrité de fichiers vitaux
- Vulnérabilité: Pas de contrôle des badges à l'entrée
- Vulnérabilité de fond: Animal Social

Exemple d'attaque numéro 4: Attaque interne 2

Voir: `https://www.youtube.com/watch?v=DCOm4osfWn8`

- Motivation: Vol d'informations
- Moyen: Exploiter les émotions humaines
- Menace: Perdre de l'argent à cause du SI
- Vulnérabilité: Divulgation d'information qui pourraient exploiter les failles du système
- Vulnérabilité de fond: Animal Social