Sécurité des Systèmes d'Information

TD1: Principes Fondamentaux

Sommaire

« Le système d'information représente un patrimoine essentiel de l'organisation , qu'il convient de protéger .

La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. »

JF Pillou

1. Définir le concept de sécurité des systèmes d'information.

2. Citer au moins 3 notions fondamentales de la sécurité des systèmes.

3. Pourquoi dit-on souvent que les problèmes de sécurité sont des problèmes de gestion d'architectures et de management de personnes?

4. Citer des domaines qui ne peuvent se passer d'une politique de sécurité.

5.Dans quelle mesure la sécurité est-elle le résultat d'un compromis?

Définir le concept de sécurité des systèmes d'information.

La sécurité informatique est un défi d'ensemble qui concerne une chaîne d'éléments :

1. les infrastructures de traitement / communication ;

2. les logiciels ;

3. les données ;

4. le comportement des utilisateurs.

Le niveau global de sécurité est défini par le niveau de sécurité du maillon le plus faible.

Citer au moins 3 notions fondamentales de la sécurité des systèmes :

1. L'intégrité ;
2. La confidentialité ;
3. La disponibilité ;
4. La non-répudiation et l'imputation ;
5. L'authentification.

Définissez ces notions.

L'intégrité :

Les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire.

La confidentialité :

Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

La disponibilité :

Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

La non-répudiation et l'imputation :

Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

L'authentification :

L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

Pourquoi dit-on souvent que les problèmes de sécurité sont des problèmes de gestion d'architectures et de management de personnes?

- Connexions « sauvages » ;
- Mot de passe sur des post-it ;
- …

Citer des domaines qui ne peuvent se passer d'une politique de sécurité.

- L'énergie (Fukushima) ;
- La défense (Dassault)
- Les communications (Angela Merkel) ;
- ...

Dans quelle mesure la sécurité est-elle le résultat d'un compromis?

« The tester entered bogus credit card information with his order, which triggered a phone call from an employee whose job it was to manually enter all payment information from the seller's online orders. The tester offered to send the correct information to the business in an e-mail with an attached document. The phone conversation was designed to lower the guard of the employee, who might not have opened the e-mail had it come from a complete stranger. In the end, the employee opened the e-mail and attachment, Patterson says, and welcomed in the Trojan, allowing the tester to break through the firewall and gain access to 25,000 credit card accounts. »

1. Lire.
2. Résumer brièvement le problème soulevé dans ce paragraphe.
3. Quel logiciel malicieux a été utilisé? Citez-en au moins 2 autres.
4. Qu'est ce qu'un *firewall*? Pourquoi a-t-il échoué dans sa mission.

« La NSA a soumis au NIST (National institute of standards and technologies) un algorithme de génération de nombres aléatoires avec une porte dérobée. Il y a un terme pour ce genre de vulnérabilités : la kleptographie, qui est l'utilisation d'attaques implémentées au sein d'un système de chiffrement, comme une porte dérobée dans un système de chiffrement. L'algorithme était connu comme étant une création de la NSA. En effet, la NSA est impliquée depuis longtemps dans la standardisation d'outils de chiffrement. En 2007, la porte dérobée a été trouvée et rapportée par les ingénieurs de Microsoft. Ceux qui étaient dans le milieu ont rapidement deviné que la NSA avait tenté d'implémenter une porte dérobée dans l'algorithme… »

1. Lire l'article
2. Définir la notion et l'utilité de la *porte dérobée*.
3. Que reproche-t-on à la NSA?
4. Lier cet article avec l'actualité (projet PRISM)

“Don’t rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You’ll usually find that vulnerability lies in your people.”

Kevin D. Mitnick – “The Art of Deception”

Lire l' article puis répondre aux questions suivantes:

1. Récapituler les risques mentionnés dans l'article ;

2. Quel est la thèse soutenue par l'article ?

L'article manque malheureusement de détails… en prenant en compte la citation suivante (issue de l'article source), expliquez pourquoi l'Homme restera le point le plus vulnérable d'un SSI.

« The report observes that while organizations have made progress preventing repeat attacks arising from viruses/worms, they have been less successful in dealing with e-mail attacks and phishing/pharming. The reason is because e-mail attacks are more varied and because e-mail can't just be shut down. »

« Delta Search est un moteur de recherche. Delta Toolbar est son équivalent, présenté sous la forme d'une barre d'outils. Mais dans 99,9% des cas, les utilisateurs n'ont pas souhaité que Delta Search remplace Google…

Google domine tous ses concurrents. Une domination telle, que certains moteurs de recherche n'hésitent plus à s'imposer sur les ordinateurs des particuliers. On parle alors de PUP (***Potentially Unwanted Program***) ou LPI (***Logiciel Potentiellement Indésirable***). Lorsque vous installez une nouvelle application sur votre ordinateur, vous devez généralement décocher certaines cases pour que ces programmes ne s'installent pas dans la foulée. »

1. Lire l' article ;

2. Récapituler les risques mentionnés dans l'article ;

3. Ces programmes sont-ils bénéfiques pour l'utilisateur ?

Internet Sans Frontières reproche ainsi à Facebook une ***« collecte déloyale et frauduleuse »*** de données personnelles, collecte effectuée sans le consentement des utilisateurs, notamment par le biais ***de cookies***, dont certains qualifiés de cookies zombies.
« Ces cookies peuvent être installés sur un navigateur web qui a choisi de ne pas recevoir de cookie car ils ne sont pas entièrement configurés comme des cookies traditionnels » décrit l'association dans sa plainte.

D'autres techniques de collecte sont également pointées du doigt, dont l'exploitation du bouton ***«J'aime»*** et la ***reconnaissance faciale***, qui pourrait d'ailleurs valoir à la firme un procès en Allemagne, faute d'une conciliation avec les autorités allemandes de protection des données personnelles. Autre accusation portée contre Facebook, une infraction aux articles 6, 7, 32 et suivants de la loi Informatique et Libertés. Une nouvelle fois, c'est « le non respect du droit de suppression des données et la conservation pendant une durée excessive des données personnelles » qui est épinglé.

Article original

1. Qu’est-ce qu’un « cookie zombie »?

2. Quel rôle joue-t-il dans la collecte d’informations personnelles?

3. Que reproche cet article à Facebook?

4. Quels sont les risques d’une défaillance du système de sécurité de Facebook?