CORRIGE

Ces éléments de correction n'ont qu'une valeur indicative. Ils ne peuvent en aucun cas engager la responsabilité des autorités académiques, chaque jury est souverain.

ISDRANG

BTS INFORMATIQUE DE GESTION **Session 2006**

E1.2 : LANGUE ANGLAISE APPLIQUÉE À L'INFORMATIQUE ET À LA GESTION

(partie écrite)

Durée : 2 heures **Coefficient : 2**

L'usage d'un dictionnaire bilingue est autorisé.
Les calculatrices sont interdites.

PROPOSITION DE CORRIGÉ

I- Pour le résumé : faire apparaître les idées suivantes.

- La technique du phishing (hameçonnage) comme système d'attaque en vue d'obtenir des crédentiales (autorisation) d'accès, tels que mots de passe et noms d'utilisateurs.
- Il existe des outils pour navigateurs Internet (IE ou Mozilla) qui aident à déterminer le domaine réel du site visité.
- Les pirates viennent d'inventer le « pharming » qui exploite la vulnérabilité des serveurs DNS en permettant à un pirate d'acquérir le Nom de domaine pour un site donné, et de rediriger les flux de ce site vers un autre site.
- 3 méthodes nouvelles pour lutter contre ce procédé.

  1- Pour une entreprise, permettre l'utilisation d'un service de surveillance des serveurs DNS pour traquer les échanges illicites. (MarkMonitor)

  - Un service qui est aussi un service d'alerte.

  2- l'utilisation d'un système anti-pharming (NGSEC's) qui fonctionne à deux niveaux :

  - au niveau du client : pour empêcher les modifications des configurations locales.

  - au niveau des interfaces réseau, en capturant et comparant les requêtes DNS avec trois autres serveurs DNS sécurisés.

  - Le système est gratuit pour des particuliers mais nécessite un droit financier pour un usage commercial.

3- Le tout nouveau système ICues qui fonctionne au niveau du site web.

- à la première connexion avec un site web protégé par ICues, le système envoie des signaux en couleur qui réapparaîtront aux utilisations suivantes.

- un site falsifié ne pouvant pas reproduire ces signaux, vous savez immédiatement ce à quoi vous avez affaire.

- Ce sont les trois dernières approches à ce jour pour enrayer l'empoisonnement que sont le phishing et le pharming.

Evaluation des points : 1 point par idée.

- **Remarques** : à redécouper en petites unités pour permettre d'affiner et de bien filtrer la production des étudiants.

II. Productions écrites :

A. Tableau des points d'évaluation à donner en fonction des critères suivants :

Respect des consignes 0 1

Richesse de vocabulaire 0 1 2

Correction grammaticale 0 1 (questionnement et utilisation des temps)

Prise de risque et structures 0 1

Idées possibles à développer dans ce sujet :

Q : How did you hijack the system ?

- As you know, servers are vulnerable. Every web site on the net has a so-called IP address which consists of 4 numbers.
- These addresses are comparable to the telephone number.
- As it's difficult to remember these numbers, websites also have a Domain Name (ex: www.google.com).
- The domain name server acts as a phone book to associate the Domain name of a website with its IP address.
- I used a copy of the site which is also SSL protected and I stole the user's information : identification and password.

Q : Why did you organise the hijacking ?

* Wanted to see if I was able to access a DNS server.

* Wanted to do it for fun.

B. <u>Tableau des points sujet B</u>.

Vocabulaire 0 1

Correction grammaticale 0 1

Pertinence 0 1

Advice to counter phishing.

The bank would like to recommend these pieces of advice to customers concerning phishing as a result of a series of problems affecting customers.

1. Never divulge details of account numbers and codes via e-mail. The bank would never ask for such information.

2. Always take care to keep code and account numbers confidential.

49 words