ISDRANG

BTS INFORMATIQUE DE GESTION

Option « Développeur d'applications »
Option « Administrateur de réseaux locaux d'entreprise »

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

Session 2006

Durée : 2 heures **Coefficient : 2**

Matériel autorisé :

DICTIONNAIRE BILINGUE.

L'USAGE DES CALCULATRICES N'EST PAS AUTORISÉ POUR CETTE ÉPREUVE

Dès que le sujet vous est remis, assurez-vous qu'il est complet.
Le sujet comporte 2 pages, numérotées de 1/2 à 2/2.

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.

IN FOCUS : PHISHING AND PHARMING

by Mark Joseph Edwards, News Editor, mark at ntsecurity/net

"Security : Phishing and Pharming," *Windows IT Pro Magazine*, June 22, 2005

You've undoubtedly heard of "phishing," luring users (typically through email messages) to phony Web sites that imitate legitimate Web sites to try to trick users into divulging private information such as logon IDs, passwords, and account numbers. Phishing can lead to unauthorized monetary charges against your merchant accounts, unauthorized use of your services, and more.

Tools such as CoreStreet's SpoofStick and the Netcraft Toolbar can help in some cases. Both tools are add-ons for Microsoft Internet Explorer (IE) and Mozilla Firefox that try to determine and display the real domain of the site you're visiting.

Recently, hackers are combining phishing with DNS poisoning or DNS hijacking-also known as "pharming." In a pharming attack, the attacker changes DNS records of the servers at an ISP or at the company that's the target of the attack or modifies a client system's HOSTS file or DNS settings. Obviously, protecting against such attacks means devising some method of establishing trust in DNS query results. The two tools I mentioned above don't help much against pharming.

I know of three ways to help prevent pharming attacks. The first method is for a company to use a service, such as one recently announced by MarkMonitor, to monitor the company's DNS servers for unauthorized changes. When unauthorized changes are detected, MarkMonitor alerts the company so that it can begin working to correct the situation.

A second method, which is also new, is to use Next Generation Security's (NGSEC's) AntiPharming tool, which works at the client level (rather than the server level) to prevent unauthorized changes to a system's HOSTS file and local DNS settings. It also listens on the system's network interfaces to capture DNS query responses and then doublechecks those responses against "three secure DNS servers". The tool comes with three DNS servers preconfigured, and you can modify those server addresses as you see fit. The tool is available free for personal use and requires a fee for commercial use.

Another new solution, Identity Cues from Green Armor Solutions, works at the Web site level. The first time a user logs on to an Identity Cues-protected Web site, the product generates colored visual cues that will then appear each time the user logs on to the site. A spoofed Web site won't be able to generate the same cues, so a user sent to a spoofed site will immediately know that he or she isn't visiting the legitimate Web site. Identity Cues is definitely a novel concept.

All three approaches sound like good ideas and would go a long way towards thwarting phishing and pharming. I suspect that there are other ways to help prevent pharming, but at this point I'm unaware of any other solutions. If you know of any, please send me an email message that fills me in on the details.

QUESTIONS

Indiquez le nombre de mots contenus dans vos réponses pour chacune des deux parties.

PREMIÈRE PARTIE ***(12 points)***

Résumez ce texte en français en 150 mots (+/- 10 %).

DEUXIÈME PARTIE ***(8 points)***

EXPRESSION ECRITE. Vous traiterez en anglais les deux sujets ci-dessous.

A- You meet the German teenager who hijacked eBay.de Domain Name in 2004. Write a conversation relating the event. You will insist on the following clues :

1. Explaining the process
2. Goal of the hijacking

(5 points)
150 mots (+/- 10 %).

B- Write a notice from a bank to clients warning against the dangers of phishing. (3 points)

50 mots (+/- 10 %).