«Attaques par déni de service» Information et prévention

DoS – Denial-of-Service

Une attaque DoS ou par déni de service est portée directement à partir de l'ordinateur du hacker et ne met pas d'autres ordinateurs en cause. Le cybercriminel inonde un serveur ou un site Web de demandes au point de ne plus être à même de les traiter. Le service est donc ainsi interrompu.

DDoS – Distributed-Denial-of-Service

L'attaque DDoS ou par déni de service distribué s'articule en deux temps:

1. L'attaquant se rend maître de plusieurs ordinateurs à l'aide d'un cheval de Troie ou d'un autre maliciel pour établir ainsi un botnet ou réseau de bots.
2. Après avoir pris le contrôle de ce botnet, il l'utilise pour attaquer sa cible (un site Web par exemple), comme lors d'une attaque DoS.

Contre-mesures

Il est essentiel de bien respecter les «5 mesures pour votre sécurité» afin d'empêcher que votre ordinateur ne devienne membre d'un réseau de bots et ne participe de ce fait involontairement à une attaque DDoS.

En particulier, il convient de:

- utiliser un programme antivirus parfaitement à jour
- surveiller la connexion avec un pare-feu
- installer régulièrement les mises à jour de votre système d'exploitation et des programmes installés
- faire attention et de se montrer vigilent

Attaque par déni de service

L'objectif d'une attaque par déni de service (attaque DoS) est de bloquer un serveur ou d'empêcher l'accès à un site Web. Pour cela, un hacker doit saturer un service ou le suspendre.

Ce type d'attaque concerne la plupart du temps des sites Web et ne comporte donc en règle générale pas de vol ni de manipulation de données. Pour le hacker, il s'agit tout simplement d'empêcher les utilisateurs légitimes d'accéder à un site Web, si bien qu'il leur sera par exemple impossible d'utiliser pendant un certain temps les services d'e-banking.

Pour en savoir plus: www.ebas.ch/denialofserviceattack

«eBanking – en toute sécurité!» informe les utilisateurs des services de banque en ligne sur les questions de sécurité

eBanking en toute sécurité!

Le site Web **www.ebankingentoutesecurite.ch** vous informe gratuitement sur les mesures nécessaires à mettre en œuvre et les règles de comportement à adopter pour une utilisation sécurisée des applications e-banking.

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz