Jean-François PILLOU
Jean-Philippe BAY

Comment ça marche .net

Tout sur la Sécurité informatique

5e édition

DUNOD

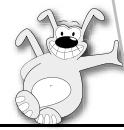
- DNS blockchain
- Sim swap
- Meltdown et Spectre
- Chiffrement homomorphe
- Phone scamming
- Port knocking
- ANSSI
- MÉHARI
- Ransomware
- DNS rebinding
- WPA3
- Cryptomineur
- ASLR
- NIS/RPGD, etc.

Directeur de collection : Jean-François Pillou

Illustration de couverture : Rachid Maraï

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-081347-6

Table des matières



Avant-propos

Nul ne peut aujourd'hui ignorer les dangers liés à l'utilisation d'Internet : virus, spam et pirates informatiques sont les maîtres mots utilisés par les médias. Mais que connaissez-vous exactement de ces risques ?

De plus en plus de sociétés ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs et donnent l'accès à Internet à leurs employés. Quelles menaces les guettent ?

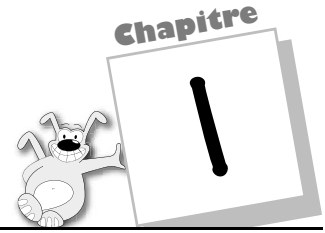
Avec le nomadisme et la multiplication des réseaux sans fil, les individus peuvent aujourd'hui se connecter à Internet à partir de n'importe quel endroit. Tout le monde s'accorde à dire qu'il existe un risque, mais quel est-il pour les particuliers et quelles peuvent en être les conséquences ?

Sur le plan professionnel, les employés sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisée de l'entreprise. Comment protéger les informations vitales de l'entreprise ?

Pour toutes ces raisons, à domicile comme au bureau, il est nécessaire de connaître les risques liés à l'utilisation d'Internet et les principales parades. Cet ouvrage se veut ainsi un concentré d'informations et de définitions sur tout ce qui touche à la sécurité informatique.

Remerciements

Jean-François Pillou remercie Cyrille Larrieu pour l'article sur les systèmes de détection d'intrusion et Sébastien Delsirie pour l'article concernant Enigma.



Les menaces informatiques

Une **menace** (*threat*) représente une action susceptible de nuire, tandis qu'une **vulnérabilité** (*vulnerability*, appelée parfois faille ou brèche) représente le niveau d'exposition face à la menace dans un contexte particulier. La **contre-mesure** (ou parade), elle, représente l'ensemble des actions mises en œuvre en prévention de la menace.

Les contre-mesures ne sont généralement pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'attention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l' « ennemi ». Le but de cet ouvrage est ainsi de donner un aperçu des menaces, des motivations éventuelles des pirates, de leur façon de procéder, afin de mieux comprendre comment il est possible de limiter les risques.

Introduction aux attaques informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.