Sécurité et espionnage informatique: Connaissance de la menace APT (Advanced Persistent Threat) et du cyberespionnage

- **Author : Cédric Pernet**
- **Publisher : Eyrolles, 2015**
- **pages : 240 pages**
- **N° Class : 621/1118**

Les attaques informatiques ciblées d'entreprises dans un but d'espionnage industriel, plus connues dans le milieu de la sécurité informatique sous le nom d'APT (Advanced Persistent Threat) sont fortement médiatisées outre-Atlantique. Qui les organisent ? Comment fonctionnent-elles ? Comment les détecter ?

APT : des attaques toujours plus difficiles à détecter

Les attaques APT sont des attaques informatiques menées contre des entreprises afin de dérober des informations sensibles et/ou concurrentielles. Elles suivent un modus operandi qui varie peu mais qui s'avère d'une efficacité redoutable : investigation sur la cible potentielle, infection de postes de travail et de serveurs au moyen de chevaux de Troie, rebond à l'intérieur du réseau de l'entreprise ciblée jusqu'à atteindre les données souhaitées, maintien de portes dérobées opérationnelles sur le réseau de la victime afin de conserver un accès constant sur plusieurs mois et s'emparer à loisir des informations sensibles de l'entreprise. Ces attaques sont orchestrées par des groupes de taille variable, dotés généralement de moyens considérables, souvent plus conséquents que ceux dont disposent les professionnels de la sécurité protégeant les entreprises ciblées. Certains de ces groupes sont financés par des États, alors que d'autres sont privés et opportunistes. Ces attaques peuvent néanmoins être combattues, sur un plan préventif par une prise de conscience globale de chaque utilisateur, et sur un plan opérationnel par une surveillance du parc informatique plus appropriée.

Un livre de référence sur les attaques APT et le cyberespionnage

Un ouvrage de fond en sécurité informatique, destiné à devenir une référence, écrit par l'un des pionniers français de la lutte contre le cyberespionnage. S'opposant aux idées reçues en la matière, l'ouvrage présentera les points de vue des experts du domaine et les cas les plus intéressants médiatisés ces dernières années. Il guidera le professionnel dans l'amélioration de la protection de son entreprise face à ces attaques

.

À qui s'adresse cet ouvrage ?

- Aux directeurs des systèmes d'information qui cherchent à optimiser leurs stratégies de sécurité
- Aux responsables de la sécurité des systèmes d'information (RSSI) qui souhaitent améliorer la sensibilisation aux attaques APT en entreprise ainsi que le niveau de sécurité global de leur parc informatique
- Aux administrateurs système, architectes réseau, développeurs d'outils de sécurité et particuliers curieux de se cultiver sur le sujet