



La cybersécurité

Nicolas ARPAGIAN

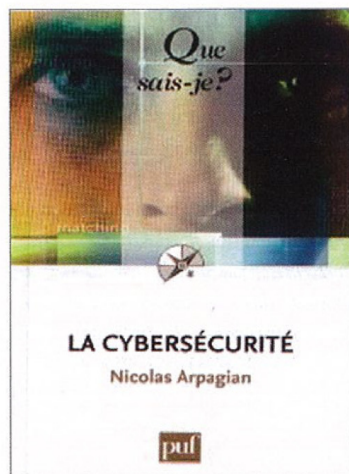
L'entrée dans la société de l'information a engendré de profondes mutations pour les collectivités modernes.

Nicolas Arpagian résume parfaitement la situation actuelle : « *Ce nouveau théâtre d'ombres consacre le principe de la guerre asymétrique, où les parties prenantes n'ont plus nécessairement la même nature juridique, ni a priori la même puissance : des États peuvent être attaqués par des militants isolés, des sociétés commerciales peuvent être visées par des services de renseignements gouvernementaux ou être la cible de compétiteurs indélégitimes, des particuliers peuvent être mis en cause par d'autres personnes privées.* »

La protection des systèmes d'information est devenue un enjeu primordial.

En effet, nous sommes aujourd'hui bien loin de la philosophie des premiers « hackers » (pirates) qui infiltraient les réseaux pour mettre en lumière les failles des systèmes de sécurité mis en place dans les administrations ou les entreprises. Leur démarche était fondée sur le goût de la prouesse technique. On observe depuis plusieurs années un basculement de l'intérêt des cybercriminels vers des motivations purement financières. Aujourd'hui, les hackers travaillent aussi bien pour des organisations criminelles et des mafias, que pour des États, des entreprises ou encore pour leur propre compte.

L'élaboration de logiciels malveillants, la détection de failles permettant le vol de données ou l'infiltration de système, le piratage de milliers de postes (botnets) vont servir aux hackers



2010, PUF, Col. *Que sais-je ?*
128 p., 9 €

à atteindre des fins économiques ou politico-militaires.

Plusieurs exemples sont repris dans cet ouvrage afin de mieux mesurer les risques liés à ces offensives menées, dans le secteur public comme dans la sphère privée, contre les systèmes d'informations.

La cyberattaque contre l'Estonie en 2007 a montré les limites des réponses techniques apportées. La prise de contrôle de sites gouvernementaux et de certains médias nationaux avait semé la panique à Tallin : de nombreux sites institutionnels étaient inaccessibles du fait d'une saturation des demandes d'accès et leur contenu avait été remplacé par des portraits nazis... Les médias diffusaient des images d'entrée de chars russes dans la capitale ce qui rappela immédiatement les tensions politiques existantes entre les deux pays. Les autorités n'ont techniquement pas pu contrer ces attaques simultanées et ont observé un retour à la normale quelques jours plus tard.

De la même façon, les entreprises ne sont pas à l'abri : des sociétés telles que Yahoo ont fait face à des attaques par déni de service, des sites internet de certains groupes du secteur du luxe ont vu leur contenu modifié. Ces cyberattaques nuisent au développement stratégique des firmes tout en entachant parfois leur image de marque (incapacité à sécuriser les données des clients, mise en lumière des pratiques peu éthiques de certaines entreprises à l'aide de guerres informationnelles...).

Ces attaques de grande ampleur ont ravivé les questions de sécurisation des systèmes d'information du fait de la présence grandissante des technologies de l'information et de la communication dans notre environnement.

Le dernier chapitre souligne la disparité des dispositifs étatiques existants. Le vide juridique vient de surcroît compliquer la mise en place de solutions efficaces et nuit aux processus d'identification de l'origine des attaques et des cybercriminels.

La capacité de nuisance des cybercriminels est considérable : ils peuvent paralyser des villes entières si ils dirigent leur attaque vers des structures administratives, médicales, militaires, industrielles (réseaux électriques, usines nucléaires, systèmes d'information militaire...).

En conclusion, Nicolas Arpagian éclaire de façon décisive une problématique chaque jour plus capitale.

Anaïs BÉRANGER
INHESJ, Chargée d'Études
et de Recherches
Département Sécurité Économique