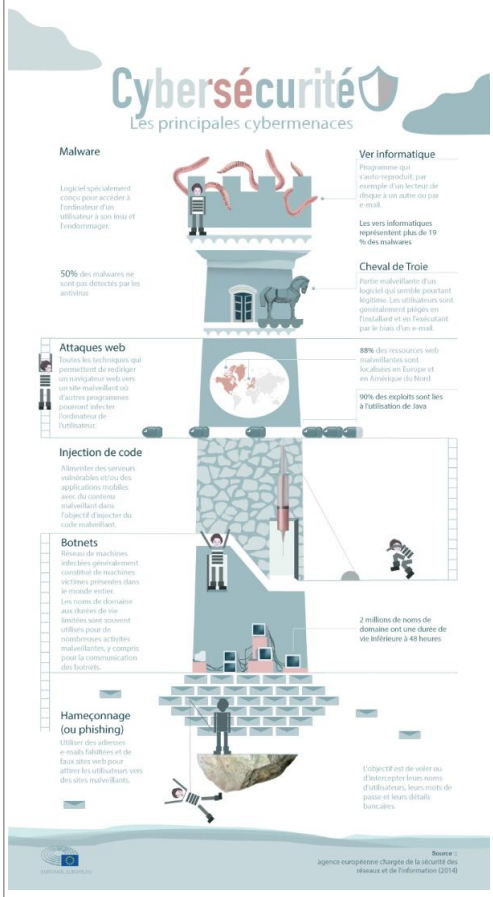
Directive sur la sécurité des réseaux et des systèmes d’information

Directive sur la sécurité des réseaux et des systèmes d’information

Nos sociétés digitalisées reposent de plus en plus sur des réseaux électroniques qui peuvent faire l'objet de cyberattaques aux conséquences importantes. Afin de mieux faire face à ce type de menaces en ligne, le Parlement et le Conseil ont conclu en décembre dernier un accord sur les premières règles européennes en matière de cybersécurité. Celles-ci ont été soutenues par l'ensemble du Parlement réuni en session plénière ce mercredi 6 juillet.



Vols d'identité, faux sites web de banques, espionnage industriel ou inondation de données qui rendent un serveur incapable de répondre : les menaces en ligne sont nombreuses et visent tant les particuliers que les entreprises et les autorités publiques.
Les incidents et les attaques des systèmes d'information des entreprises et des citoyens pourraient représenter un coût de 260 à 340 milliards d'euros par an, selon les estimations de l'Agence européenne chargée de la sécurité des réseaux et de l'information.
Les cyberattaques menées contre certaines infrastructures clés de nos sociétés, comme les services bancaires, les réseaux d'électricité ou le secteur du contrôle aérien, peuvent avoir des conséquences particulièrement importantes sur notre quotidien.
Dans le cadre d'un Eurobaromètre publié en février 2015, les citoyens européens ont exprimé de fortes inquiétudes à propos de la cybersécurité : 89 % des internautes évitent de diffuser des informations personnelles en ligne. Selon 85 % des sondés, le risque d'être victime de cybercriminalité est de plus en plus important.

Vote en plénière
Les députés ont approuvé la directive sur la sécurité des réseaux et de l'information dans l'Union, qui définit une approche commune autour de la question de la cybersécurité.
Le texte prévoit une liste de secteurs dans lesquels les entreprises qui fournissent des services essentiels, liés par exemple à l'énergie, aux transports ou au secteur de la banque, devront être en mesure de résister aux cyberattaques.
La directive les oblige notamment à signaler les incidents de sécurité graves aux autorités nationales. Les fournisseurs de services numériques tels qu'Amazon ou Google devront également notifier les attaques majeures aux autorités nationales.
Ces nouvelles règles sur la cybersécurité visent également à renforcer la coopération entre États membres en cas d'incidents.

Téléchargez la directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil :
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Article original du Parlement Européen

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybersécurité : mieux faire face aux attaques en ligne