



# INFORMATIQUE BUREAUTIQUE COMMUNICATION

**IBC, votre partenaire de service d'ingénierie réseaux  
informatiques, vous informe :**

**ASSISTANCE**

**CONSEIL**

**AUDIT**

**VENTE  
MATERIELS  
&  
CONSOMMABLES**

**CENTRE DE  
FORMATION  
AGREE**

**Un savoir faire**

**Une solution adaptée**

**Une équipe  
expérimentée  
à votre écoute**

**Service Clients :**

service.clients.ibc@orange.fr  
ibc83@wanadoo.fr

**Service Technique :**

service.technique.ibc@orange.fr

**Au moment où le gouvernement revoit sa politique en matière de défense dans le but de s'adapter aux nouvelles menaces dont le catalogue s'est enrichi notamment en matière de sécurité, il nous paraît intéressant de faire un zoom sur :**

## Les Cyber Attaques

L'environnement a changé du fait de la protection renforcée de la plupart des systèmes informatiques et de l'alourdissement des sanctions. On assiste aujourd'hui à l'apparition d'escrocs organisés, déterminés et tenaces et à une diminution d'attaques diffuses au profit d'attaques ciblées et potentiellement plus dangereuses.

Les organisations des secteurs publics et privés doivent agir rapidement et coopérer pour faire face à cette nouvelle tendance.

Si les virus, spams, logiciels malveillants (malware) représentent des menaces évidentes sur les équipements informatiques, il existe bien d'autres menaces dont nous vous signifierons leur définition afin de protéger votre information :

**Attaques de l'intérieur** – Avec la sécurisation croissante des logiciels, les utilisateurs resteront le maillon faible des entreprises et des organisations. Au lieu de perdre leur temps à rechercher des failles difficiles à trouver dans les logiciels, les délinquants s'efforceront de convaincre des utilisateurs finaux de réaliser l'attaque. Délocalisations, restructurations, fusions-acquisitions – toutes ces opérations compliqueront la tâche des entreprises et des organisations qui tentent de sensibiliser leurs utilisateurs à de telles menaces.

**Marchés émergents** – Profitant du manque de coopération internationale contre la cybercriminalité, les cyberdélinquants lancent des attaques transfrontalières avec l'assurance de prendre très peu de risques. Les menaces en direction et en provenance des pays émergents et en voie de développement sont ainsi en augmentation. Et il devient beaucoup plus difficile de remonter à la source des attaques, d'autant que, comme l'indiquent les tendances, les attaques proviennent de plus en plus de régions comme l'Europe de l'Est et l'Asie où les sanctions sont plus légères et où l'application de la loi est limitée.

**Blogging** – L'utilisation croissante d'outils collaboratifs comme les blogs accroît également les risques de fuite de données commerciales confidentielles.

**Messagerie instantanée** – Les « botnets », des réseaux d'ordinateurs « zombies » contrôlés à l'insu de leurs propriétaires, continueront à représenter l'une des plus grandes menaces sur Internet. De nouveaux botnets, s'appuyant sur de plus petites cellules pour être plus difficiles à détecter, se rabattront probablement sur la messagerie instantanée et sur d'autres réseaux d'égal à égal pour contrôler les systèmes infectés.

**Équipements mobiles** – Les logiciels malveillants affectant les téléphones portables, les PC de poche et d'autres équipements sans fil ont sensiblement augmenté l'an dernier, sans toutefois donner lieu à des attaques diffuses de grande ampleur, car ils ne peuvent pas proliférer tout seuls – pour le moment. Cette tendance restera donc sous surveillance.

**Attaques e-mail ciblées** – On note un changement dans la nature et l'intention de ces attaques. Poursuivant fréquemment des objectifs financiers, concurrentiels, politiques ou sociaux, ces attaques ont souvent été dirigées contre des administrations, des organisations militaires et d'autres grandes organisations, en particulier dans les domaines de l'aérospatiale, du pétrole, de la justice et des droits de l'homme. Une série de cas spectaculaires ont fait les unes des journaux en 2005, mais on estime que le nombre des attaques non détectées par les entreprises est très supérieur.

**Spear phishing** – Le « spear phishing », ou pêche au harpon, s'inscrit dans le développement des attaques plus ciblées : des escrocs bombardent des entreprises par un spam très ciblé qui a toutes les apparences d'un courrier interne émanant par exemple du service informatique ou des RH. Souvent, le cyberdélinquant offre une petite récompense en échange d'informations, et les victimes s'exécutent, trompées par l'aspect officiel des e-mails. Elles révèlent alors des informations qui permettront aux escrocs d'accéder à des domaines réservés du réseau de l'entreprise à des fins de vol de propriété intellectuelle et d'autres données commerciales sensibles. Le spear phishing – qui constitue aussi en soi une technique de « socio-ingénierie » – a également été employé pour inciter des gens à ouvrir des logiciels malveillants.

**Phishing** – Le **phishing** (contraction des mots anglais « fishing », en français pêche, et « phreaking », désignant le piratage de lignes téléphoniques), traduit parfois en « hameçonnage », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes. La technique du phishing est une technique d'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.

Z.I. Toulon Est - BP 56 – 799, Avenue Docteur Calmette - 83087 TOULON CEDEX 09  
(LA FARLEDE)

**TEL : 04.94.143.621 - FAX : 04.94.143.552**

S.A.R.L. au Capital de 7 622 Euros - RCS TOULON B 400 956 439 - SIRET 400 956 439 00014 - APE 4651Z

Centre de Formation agréé sous le numéro 93830185583