Dispositif VIGIPIRATE
Volet Sécurité des Systèmes d'Information

Attaques des sites internet :

- Les deux principaux types d'attaques « voyantes » de sites internet sont :

    - le défaçage : l'attaquant modifie le site pour y afficher ses revendications.
    - le déni de service : l'attaquant inonde le site de requêtes afin de le faire tomber.

    Ces attaques peuvent être accompagnées d'un vol de données et/ou dépôt d'une charge utile (« payload ») en vue d'une attaque ultérieure.

- Les sites internet et intranet des administrations sont en général hébergés sur des plate-formes ministérielles. La sécurité est assurée par les centres techniques des ministères.

- Les autres sites internet sont en général hébergés par des prestataires privés. La SSI est plus ou moins prise en compte par ces prestataires. Il peut être conseillé :

    - de bien vérifier les clauses contractuelles liant le propriétaire du site au prestataire. La SSI est-elle bien prise en compte ?
    - de vérifier avec le prestataire qu'il a appliqué l'ensemble des correctifs de sécurité (« patch ») connus pour sa plate-forme,
    - de vérifier les droits d'accès à l'administration du site (qui a le droit de le gérer ?),
    - d'utiliser des mots de passe robustes et de les changer régulièrement.

- En cas d'attaque constatée : prévenir l'hébergeur, porter plainte et le cas échéant en informer l'Agence Nationale SSI.

Vigilance sur les systèmes d'information

- Les équipes informatiques doivent mettre à jour les logiciels en appliquant les correctifs des éditeurs de logiciels et en suivant les alertes du CERT-FR (Computer Emergency Response Team, le centre gouvernemental français de veille, d'alerte et de réponse aux attaques informatiques).
- La surveillance des journaux d'événements des serveurs doit être renforcée.
- Les droits d'accès aux systèmes doivent être vérifiés.
- Les équipes doivent se préparer à appliquer le Plan de Continuité d'Activité informatique.

Vigilance comportementale

- Le respect d'un certain nombre de règles de bon sens contribue à limiter la surface d'attaque des systèmes d'information (mots de passe, protection des machines et de leurs informations, accès à internet, utilisation de la messagerie, ingénierie sociale etc).
- Afin de préserver le secret, être vigilant sur les informations délivrées sur les réseaux sociaux pour les personnels « sensibles » (forces de l'ordre, autorités …).
- Vérifier l'information provenant des réseaux sociaux même s'il s'agit d'une source considérée comme fiable (le compte peut avoir été piraté).