Cybersécurité

Faire de la cybersécurité une priorité pour 2018

Le contexte

Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ; l'actualité récente a entrainé un accroissement significatif du nombre d'attaques informatiques visant des sites Internet français.
La très grande majorité de ces attaques sont des défigurations de sites Internet (ou défacement), ou des dénis de service (DDoS)

Trop souvent sous estimées par les PME les cyber attaques engendrent des pertes importantes (financières directs, data, image)

Actusnews considère qu'il est aujourd'hui obligatoire de disposer d'une stratégie concourant à la Sécurité & Confidentialité des données (outils et moyens préventifs et curatifs).

Les attaques possibles contre votre site internet

Les attaques par réseau

- Attaques de type DDoS,
- Man-in-the-middle (MITM), Balayage de port

Les attaques au niveau applicatif

Malveillance au site web

- Défacement ,
- Exploit

Base de données :

- Injection SQL

Tentatives d'accès à l'administration du site :

- Attaque par force brute
- Dictionnaire

Nos champs d'interventions

Couche Infrastructure : Hébergement et Infogérance

- Données hébergées sur des serveurs Européens
- Gestion automatique des attaques de type DDoS, MITM, IP Spoofing, Balayage des ports et reni-flage par les technologies propriétaires AWS
- Protection de l'enceinte AWS
- Protection des instances par « Security Group »
- Firewall mutualisé AWS

- Surveillance technique 24h/24, 7J/7
- Infogéreur disposant de certifications (ITIL, ISO 20000 et ISO 27000) (norme internationale concernant la sécurité de l'information)

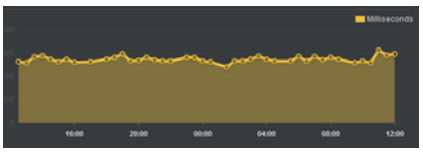
Cybersécurité

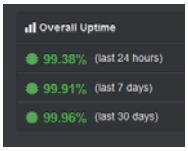
Faire de la cybersécurité une priorité pour 2018

Nos champs d'interventions

Couche applicative

- Mise en place d'un CMS mature, leader sans être le plus exposé (utilisation de Joomla)
- Limitation des composants, plugins ou modules non natifs
- Base de données hébergée sur un serveur distant
- Sécurisation de l'accès à l'interface de gestion
- Renommage de l'url d'administration par défaut
- Achat et mise en place d'un certificat de sécurité (HTTPS)
- Mise en place et suivi d'une sonde externe de monitoring sur les serveurs





- Bridage à l'IP (lorsque seul Actusnews s'occupe de la maintenance)
- Gestion des tickets d'incidents avec l'infogéreur
- Veille / correctif et upgrade
- Application de patch de sécurité ou update des extensions
- Mises à jour du CMS et de ses extensions

<u>Suivi des alertes de sécurité</u>

- De la communauté Joomla
- Du Centre Gouvernemental de veille, d'alerte et de réponse aux attaques informatique) CERT-FR

4 recommandations importantes

1/ Achat et la mise en place d'un certificat https délivré par une Autorité de Certification

2/ Faire les upgrade de version du CMS dès que nécessaire

3/ Ne pas autoriser l'accès à l'administration de votre site à d'autres personnes que celles spécifiquement désignées (**ne pas prêter ses codes**)

4/ **Éviter de stocker ses mots de passe** dans un fichier ou lieu proche de l'ordinateur si celui ci est accessible par d'autres personnes