15 minutes d'avance

Fiche conseil. 07

Captcha or not captcha ?

Pour protéger les sites web et les applications mobiles des usages frauduleux, il est devenu courant d'insérer un CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) sur la page de collecte. Inspiré du test de Turing, cet outil permet de repérer de manière automatisée si la saisie des données est réalisée par un robot ou par un humain. Quel merveilleux outil pour filtrer le trafic ! Et pourtant ...

Risques

Selon l'outil de captcha choisi, les données collectées peuvent être nombreuses et diverses. Ex. : adresse IP de l'internaute, données de géolocalisation, horodateur, cookie, mouvement de la souris / touches du clavier, durées de pause entre les actions, langue, ...

Ces données sont-elles transférées dans un pays non adéquat ? sont-elles exploitées à d'autres fins ?

Leur usage précis est difficile à connaître précisément à la lecture des conditions générales des éditeurs.

Que dit le RGPD ?

- Principes fondamentaux du RGPD : intégrité et confidentialité
- Art. 6 sur la licéité du traitement
- Art. 32 sur l'obligation d'assurer la sécurité des données personnelles

La sécurité et la licéité sont des fondamentaux de la protection des données à caractère personnel. L'usage d'outils pour protéger les sites web et les applications mobiles des attaques par bourrage d'identifiants sont donc au cœur des mesures techniques et organisationnelles à mettre en œuvre.

Bonnes pratiques

La 1e question à se poser est : le captcha est-il réellement nécessaire ?

Il existe en effet des alternatives apportant de meilleures garanties au regard du RGPD. Par exemple :

- **Technique du Honey Pot** : consiste à cacher des champs dans le formulaire. Seuls les robots les détectent et remplissent ;
- **Confirmation par envoi de sms / mail** (très utilisé dans le cas de données confidentielles) ;
- Mécanisme de **Time Measuring** : il s'agit d'un test basé sur le temps de remplissage ;
- Système de **filtrage anti-spam** côté serveur.

- Ces alternatives seront discutées avec le RSSI pour s'adapter aux technologies engagées.

- A défaut, certains outils de CAPTCHA présentent à ce jour des garanties conformes au RGPD. Par exemple :
  - **Live Identity Captcha**, par Orange (France) : solution managée et hébergée en France qui ne recueille et ne stocke aucune donnée à caractère personnel (les requêtes des utilisateurs du captcha sont traitées et gérées de façon anonyme, conformément au RGPD). Live Identity a été audité par l'ANSSI ;
  - **Friendly Captcha,** par Interlink (Allemagne) : solution « made in Europe », « GDPR compliant » et « « proven accessibility ».

- Concernant les autres outils, préférer les outils avec **version payante paramétrable** (ex. H-Captcha, MTCaptcha) ainsi que les fournisseurs états-uniens inscrits sur le Data Privacy Framework.

- En cas de doute ou de question, se rapprocher de son DSI ou de son DPO.

Pour aller plus loin

CNIL – Guide de la sécurité des données

ANSSI – Recommandations relatives à l'authentification multifacteur et aux mots de passe