RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

SE PROTÉGER DES FUITES DE DONNÉES

Retrouvez, en onze bonnes pratiques, les ressources essentielles de l'ANSSI pour protéger son organisation des fuites de données.

- **Sensibiliser la direction et les salariés** au rôle qu'ils jouent dans la protection des données manipulées et aux impacts d'une compromission.
- **Évaluer les risques liés au partage de données avec des sous-traitants et fournisseurs de services, et contractualiser la sécurisation des données.**
- **Développer, faire développer, ou choisir des applications en respectant le principe de protection des données dès la conception et par défaut** (cf. RGPD), par exemple en appliquant des règles restrictives quant à l'export massif de données. Pour aller plus loin, voir le retour d'expérience du CERT-FR (applicable au-delà du secteur social).
- **Appliquer une politique de gestion des données** en lien avec les métiers :
  - identifier les données sensibles (données personnelles ou régulées, propriété intellectuelle etc.) et celles facilement révocables (mots de passe utilisateur, tokens, etc.), et ne stocker que les données nécessaires au bon fonctionnement des métiers et du SI ;
  - archiver ou effacer les données obsolètes de manière sécurisée ;
  - définir une politique de sauvegarde sécurisée - voir les publications « Les Fondamentaux » et « Les Essentiels » de l'ANSSI sur le sujet.
- **Se préparer à la crise :**
  - créer et mettre à jour des procédures de gestion de crise ;
  - identifier les contacts pertinents à prévenir (CNIL, ANSSI, gendarmerie, cybermalveillance, prestataires, clients, DPO, etc.) ;
  - établir, en amont, une communication de crise – se référer au guide Anticiper et gérer sa communication de crise cyber.
- **Assurer la sécurité et la confidentialité des données et des traitements réalisés directement ou par un sous-traitant**, en mettant notamment en œuvre :
  - des mesures de sécurité physique : sécurité des accès aux locaux, etc. ;
  - des mesures de sécurité informatique : défense en profondeur, chiffrement des données stockées et en transit, antivirus, EDR, etc. ;
  - des accès d'administration sécurisés, et dédiés pour les sous-traitants ;
  - le maintien en condition opérationnelle (MCO) et le maintien en condition de sécurité (MCS) du système d'information.
- **Concevoir une politique forte de gestion des accès et des privilèges :**
  - appliquer les Recommandations relatives à l'authentification multifacteur et aux mots de passe ;
  - éviter le cumul des rôles ;
  - minimiser systématiquement les accès aux données par rôle, par zone du SI (développement/production/préproduction) et par créneaux horaires ;
  - superviser et journaliser. Les journaux doivent être protégés, comme expliqué dans les Recommandations d'architecture pour la sécurité d'un système de journalisation et en environnement Active Directory.

V1.0 (01/25)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

→ **Mettre en pratique les Recommandations sur le nomadisme numérique**, et tout particulièrement l'adoption de filtres écran de confidentialité (R7) et le verrouillage automatique des sessions (R16).

→ **Déployer et superviser des outils spécialisés adaptés aux besoins de l'organisation**, tels que des logiciels DLP (*Data Loss Protection*) ou un coffre-fort numérique.

→ **Mettre en place des outils de veille automatique en réaction** (ex : *haveibeenpwned.com*) **et, si possible, en anticipation** (veille sectorielle, renseignement sur la menace cyber (CTI)). La veille peut être réalisée en interne ou via un prestataire.

→ **Comprendre, en cas de fuite de données avérée, sa source** pour adopter une remédiation adéquate et éviter une nouvelle compromission par le même vecteur (ex : *infostealer*).