Les Bonnes Pratiques RGPD

La **sécurité informatique** est l'ensemble des moyens **techniques, organisationnels, juridiques et humains** nécessaires et mis en place pour **conserver, rétablir et garantir la sécurité des systèmes informatiques**.

Elle est intrinsèquement liée à la **sécurité de l'information et des systèmes d'information**.

Afin de mettre en place la sécurité informatique dans une structure, il est important de **suivre à minima les étapes suivantes** :

Sensibilisation à la sécurité informatique

Les équipes opérationnelles et les utilisateurs doivent, dans la mesure du possible, être **sensibilisés ou formés** sur ces différents points :

- La **législation en vigueur** : Loi Informatique et Libertés, RGPD…
- Les **principaux risques et menaces potentiels** : piratage, virus, phishing…
- Les **objectifs et enjeux de la sécurité informatique** : maîtrise, confidentialité…
- Les **informations considérées comme sensibles** : mots de passe, données bancaires…
- Les **règles de sécurité** régissant l'activité quotidienne et le respect de la politique de sécurité : charte informatique…

Connaissance du système d'information

Chaque entité possède des **données sensibles**. Afin de les protéger efficacement, il est indispensable de les **identifier** et de **localiser leur emplacement**.

Il faut donc **créer et maintenir à jour** un **schéma simplifié du réseau** (**cartographie**) représentant les **différents équipements** (postes, pare-feu, routeurs, serveurs…) et préciser où les **données sensibles** se trouvent.

Choix judicieux des mots de passe

Pour bien **protéger vos informations**, choisissez des **mots de passe difficiles à retrouver** à l'aide d'outils automatisés ou à deviner par une tierce personne.

Choisissez des mots de passe composés si possible de 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance…) et ne figurant pas dans le dictionnaire.

Authentification et définition des accès

Accès informatique

Afin de faciliter l'attribution d'une action sur le système d'information en cas d'incident ou d'identifier d'éventuels comptes compromis, les **comptes d'accès** doivent être **nominatifs**.

L'utilisation des comptes génériques (user, admin) doit être marginale et gérée selon une politique aussi stricte que celle des comptes nominatifs.

La **journalisation** liée aux comptes (relevé de connexions réussies/échouées) doit si possible être **activée**.

Ensuite, il est primordial de **définir qui a accès à quelles ressources en fonction des besoins**. On évite ainsi la dispersion et l'utilisation non maitrisée des documents.

Accès physique

Les **mécanismes de sécurité physique** doivent faire partie intégrante de la **sécurité des systèmes d'information** et être à l'état de l'art afin de s'assurer qu'ils ne puissent pas être contournés aisément par un attaquant.

Il convient donc d'**identifier les mesures de sécurité physique** adéquates et de **sensibiliser continuellement** les utilisateurs aux **risques** engendrés par le contournement des règles.

Les **accès aux salles serveurs** et aux **locaux** techniques doivent être **contrôlés** à l'aide de **serrures** ou de mécanismes de contrôle d'accès par **badge**.

Les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont à proscrire, sauf s'il est possible de tracer strictement les accès et de limiter ces derniers en fonction des plages horaires.

Une revue des droits d'accès doit être réalisée régulièrement afin d'**identifier les accès non autorisés**.

Lors du **départ** d'un collaborateur ou d'un changement de prestataire, il est nécessaire de procéder au **retrait des droits d'accès** ou au changement des codes d'accès.

Enfin, les **prises réseau** se trouvant dans des zones ouvertes au public (salle de réunion, hall d'accueil, couloirs, placards, etc.) doivent être **restreintes ou désactivées** afin d'empêcher un attaquant de gagner facilement l'accès au réseau de la structure.

Mise à jour des logiciels

Dans chaque **système d'exploitation** (Android, IOS, MacOS, Linux, Windows,...), logiciel ou application, des **vulnérabilités** existent. Une fois **découvertes**, elles sont **corrigées** par les éditeurs qui proposent alors aux utilisateurs des **mises à jour de sécurité**. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les **attaquants exploitent ces vulnérabilités** pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction.

Il convient donc, au sein de l'organisme, de mettre en place une **politique de mises à jour régulières**.

S'il existe un **service informatique** au sein de l'entité, il est **chargé de la mise à jour du système d'exploitation** et des **logiciels**.

S'il n'en existe pas, il appartient aux utilisateurs de faire cette démarche, sous l'autorité du directeur.

Enfin il faut **configurer les logiciels** pour que les **mises à jour de sécurité** s'installent **automatiquement** chaque fois que cela est possible. Sinon, il est conseillé de **télécharger les correctifs de sécurité** disponibles.

Sauvegardes régulières

Pour veiller à la **sécurité informatique** il est vivement conseillé d'effectuer des **sauvegardes régulières** afin de pouvoir **récupérer les données** après un dysfonctionnement du système d'exploitation ou à la suite d'une attaque.

Il est possible de sauvegarder sur des **supports externes** (Disque dur externe, DVD) qui seront à ranger dans un **lieu distant** pour éviter que la destruction ou le vol des données d'origine ne s'accompagne des données de sauvegarde.

Avant d'utiliser le **Cloud**, il faut être conscient que ces sites de stockage peuvent être **cibles d'attaques informatiques** entrainant ainsi des risques spécifiques :

- **Risques pour la confidentialité** des données
- **Risques juridiques** liés à l'incertitude de la localisation des données
- **Risques pour la disponibilité et l'intégrité** des données
- **Risques liés à l'irréversibilité** des contrats

Si cette solution est choisie il faut donc :

- **Être vigilant** sur les conditions générales d'utilisation
- **Recourir à des spécialistes** techniques et juridiques pour la rédaction des contrats
- **Chiffrer les données** avant de les copier dans le Cloud

Sécurisation des postes, du réseau et de la Wi-Fi

Sécurisation des postes

Afin de **protéger le système**, il est fondamental de mettre en place un **niveau de sécurité minimal** sur l'**ensemble du parc informatique** de l'entité (Postes utilisateurs, serveurs, imprimantes, téléphones, périphériques USB, etc…) en implémentant les **mesures** suivantes :

- **Limiter** au maximum le nombre d'**applications installées** et **modules optionnels** des navigateurs web
- Doter les **postes** d'un **pare-feu local** et d'un **anti-virus**
- Si possible **chiffrer les partitions** où sont stockées les données à caractère personnel et les **fichiers transmis par voir Internet**
- **Ne pas brancher des clés USB inconnues** ou dont l'**intégrité n'est pas maitrisée**.

Sécurisation du réseau

Il est donc important, dès la conception de l'architecture réseau, de **raisonner par segmentation en zones** composées de systèmes ayant des besoins de sécurité homogènes.

On pourra par exemple **regrouper** distinctement des serveurs d'infrastructure, des serveurs métiers, des postes de travail utilisateurs, des postes de travail administrateurs, des postes de téléphonie sur IP, etc.

Une **zone** se caractérise alors par des VLAN et des sous-réseaux IP dédiés voire par des **infrastructures dédiées selon sa criticité**.

Ainsi, des **mesures de cloisonnement** telles qu'un filtrage IP à l'aide d'un pare-feu peuvent être mises en place entre les différentes zones. On veillera en particulier à **cloisonner** autant que possible les **équipements et flux associés aux tâches d'administration**.

Il est recommandé de mettre en œuvre une **passerelle sécurisée d'accès à Internet** comprenant au minimum un **pare-feu** au plus près de l'accès Internet pour **filtrer les connexions** et un serveur mandataire (**proxy**) embarquant différents mécanismes de sécurité. Celui-ci **assure** notamment l'**authentification** des utilisateurs et la **journalisation** des requêtes.

Sécurisation de la Wi-Fi

L'usage du Wi-Fi en milieu professionnel est aujourd'hui démocratisé mais il ne faut cependant pas oublier qu'un **Wi-Fi mal sécurisé** peut permettre à des personnes d'**intercepter les données** et d'utiliser la connexion Wi-Fi à votre insu pour réaliser des **opérations malveillantes**. Il convient donc en cas d'utilisation de la Wi-Fi de suivre à minima ces **mesures** :

- **Modifier la clé de connexion par défaut**
- **Ne divulguer la clé de connexion qu'à des tiers de confiance** et la **changer régulièrement**
- **Activer le mode de chiffrement** WPA2
- **Activer la fonction pare-feu** de la box

Gestion du nomadisme et des supports amovibles

Bien que proposant des services innovants, les **terminaux nomades** (ordinateurs portables, tablettes, Smartphones,...) sont, par nature, **exposés à la perte et au vol**. Il convient donc de prendre certaines **mesures** :

- N'**installer** que les **applications nécessaires** et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…).

  Certaines applications demandent l'**accès à des données qui ne sont pas nécessaires** à leur fonctionnement, il faut **éviter de les installer**

- **Sécuriser l'accès au terminal** et le **configurer** pour qu'il se **verrouille automatiquement**
- Effectuer des **sauvegardes**
- Ne **pas préenregistrer les mots de passe**
- **Informer** son organisme en **cas de perte ou de vol**

Dans la mesure du possible, il est conseillé de **chiffrer les données** sur le matériel nomade, notamment les **clés USB** et certaines **partitions d'un disque dur**, afin de **préserver leur confidentialité**.

En cas de vol, il faudrait un **code secret** pour accéder au contenu.

Prudence lors de l'utilisation de la messagerie (Phishing…)

Les **courriels** et leurs **pièces jointes** sont souvent **sources d'attaques informatiques** (courriels frauduleux, pièces jointes piégées, etc.). Lorsque vous recevez des courriels, prenez les **précautions suivantes** :

- L'**identité** de l'expéditeur n'est **pas garantie**, il faut donc **vérifier la cohérence entre l'expéditeur présumé et le contenu** du message.
- **Ne pas ouvrir les pièces jointes** et **ne pas cliquer sur les liens** des **mails** provenant d'**expéditeurs inconnus**
- **Ne pas répondre** aux **mails demandant des informations personnelles** tels que des mots de passe ou code confidentiels pour accéder à un contenu, une offre ou une mise à jour, il s'agira dans de nombreux cas d'une **tentative d'hameçonnage** ou « **Phishing** »
- **Ne pas relayer les messages de type chaines**

Téléchargement des logiciels sur les sites officiels

Utilisez exclusivement les **sites Internet officiels** des éditeurs.

Si vous téléchargez du contenu numérique sur des **sites Internet dont la confiance n'est pas assurée**, vous prenez le risque d'enregistrer sur votre ordinateur des **programmes** pouvant contenir des **virus ou malwares**.

Cela peut permettre à des **personnes malveillantes** de **prendre le contrôle à distance de votre machine pour espionner** les actions réalisées sur votre ordinateur, **voler vos données personnelles**, **lancer des attaques**, etc.

Prenez également ces **précautions supplémentaires** :

- Pensez à **désactiver ou décocher** les **cases** proposant d'**installer** des **logiciels complémentaires**
- **Évitez** de **cliquer** sur **les liens sponsorisés**
- **Désactivez l'ouverture automatique des documents téléchargés** et lancez une **analyse anti-virus** avant de les ouvrir.

Pour plus de détails veuillez consulter le site de L'Agence nationale de la sécurité des systèmes d'information (ANSSI) : https://www.ssi.gouv.fr/