SECURITE DU SYSTEME D'INFORMATION

Enjeu :

Dans 80 % des cas, ce sont les maladresses internes, (volontaires ou non) ou l'absence de sauvegardes fiables qui sont à l'origine de la perte ou de la destruction d'informations sensibles. Les 20 % restants sont imputables à des actes externes mal intentionnés. Au cours de ces dernières années, le risque sur le système d'information s'est accru avec le développement du travail à distance et des nouvelles technologies.

L'entreprise doit concilier la nécessité de communiquer des informations et de préserver certaines d'entre elles en mettant en place une politique de sécurité de son système d'information (SSI).

Pour être efficace, la politique de sécurisation du système d'information doit s'appuyer sur la mise en place de moyens techniques mais son efficacité reposera également fortement sur l'organisation du processus dans l'entreprise et sur les comportements individuels.

Comment ?

Que protéger ?

- Le système d'information comprend :
  - le ou les serveurs réseau et des postes de travail informatique (fixes et nomades) ;
  - les applications (systèmes d'exploitation, suites bureautiques, logiciels métiers …) ;
  - les infrastructures de communication et de télécommunication (réseaux locaux, liaisons inter-sites, réseau téléphonique, accès Internet, liaison radio …).
- Les informations sensibles détenues par l'entreprise (Les informations dont la divulgation procurerait un avantage à la concurrence ou aux partenaires ou réduirait l'avantage dont dispose l'entreprise telles que la *R&D, les travaux d'innovation*, le *savoir-faire technologique, le contenu d'offres commerciales, la structure des comptes financiers, les fichiers clients, les projets de développement, le fonctionnement de l'entreprise…)*. Les informations les plus sensibles devront faire l'objet de procédures renforcées.

Quels sont les risques pesant sur le système d'information ? vols, destruction de données ou de matériel, captations d'information, indisponibilité du système, etc. avec une origine qui peut être externe mais souvent interne (malveillance ou négligence).

Quelles sont les vulnérabilités du système d'information ? (modes d'accès au réseau de l'entreprise – protection insuffisante des serveurs et postes de travail, équipements nomades, messagerie non protégée…)

Formalisation d'une politique de protection du Système d'Information

Désignation et formation d'un **responsable de la sécurité du Système d'Information**

Formation et sensibilisation permanentes de l'ensemble des salariés à la protection des informations sensibles

(Voir fiche sur la sensibilisation du personnel à la protection des informations sensibles)

Etablir une charte avec les **règles de bonnes pratiques quant à l'utilisation du Système Informatique**

- Confidentialité et renouvellement des mots de passe
- Verrouillage de l'ordinateur
- Gestion des courriers électroniques
- Déclaration de tout incident
- Sauvegarde et suppression des données les plus anciennes
- Installation de tout nouveau logiciel interdite sans autorisation
- règles d'utilisation d'internet (téléchargement – participation à des forums…)
- etc.

Engagement de la responsabilité des utilisateurs (charte d'utilisation annexée au règlement intérieur ou document qui renvoie au règlement intérieur pour les sanctions – attention aux conditions de mise en place).

Implication forte de la direction

Quelles procédures de sécurisation du système d'information ?

Authentification :

➢ Déterminer des droits d'accès au système d'information différenciés selon les responsabilités des salariés et les statuts des autres personnes pouvant avoir accès au système d'information (stagiaires, personnels temporaires, prestataires extérieurs) : qui a le droit de faire quoi ? de savoir quoi ?

➢ Gestion des codes d'accès et des mots de passe (attribuer des mots de passe suffisamment sécurisés (agrégat de caractères alphabétiques et numériques), les renouveler régulièrement (tous les 3 mois par exemple), les supprimer lors du départ des individus) ;

➢ Configuration des postes par le responsable de la sécurité du système d'information …

Sécuriser les informations et le système :

➢ Utilisation des logiciels et matériels de sécurité (antivirus, anti-spyware, pare-feu, anti-spam, etc.) pour les serveurs et postes informatiques (fixes et nomades) ;

➢ Sécurisation des échanges (Internet - extranet – Wifi ...) par le chiffrement des données les plus sensibles ;

➢ Pour les données très sensibles, utilisation de matériel non connecté au réseau ;

➢ Application des mises à jour et correctifs des logiciels ;

➢ Contrôler régulièrement la configuration des pare-feu ;

➢Veille sur les nouveaux virus, logiciels espions (www.certa.ssi.gouv.fr - www.cert-ist.com).

Sauvegarde :

➢ Définir le type de données à sauvegarder, selon quelle périodicité, pour quelle durée (obligations légales pour certaines données) – Revoir périodiquement le périmètre de sauvegarde

➢ Dupliquer les sauvegardes - Répartir les informations confidentielles sur plusieurs supports

➢ Sécurisation des lieux de sauvegardes, conservation des supports mensuels et annuels en dehors de l'entreprise

➢ Contrôle du bon fonctionnement des sauvegardes

➢ Sous-traitance à un prestataire : s'assurer du cryptage des données sauvegardées chez le prestataire …

Contrôle de la bonne utilisation du système d'information par les salariés *(Cf. www.cnil.fr pour les conditions d'application)* – Le contrôle est nécessaire, l'entreprise étant responsable de la protection de son système d'information. – Ces mesures doivent notamment être transparentes, connues de tous, faire l'objet d'une discussion collective, faire preuve de précision et mesure, définir clairement les procédures concernant les messages privés.

Gestion des incidents :

➢ Détection des vulnérabilités et anomalies le plus en amont possible

➢ Les instances à alerter en cas d'attaque informatique :

La Gendarmerie – La DCRI (Direction Centrale du Renseignement Intérieur) – L'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'information et de la Communication) – le BEFTI (Brigades d'Enquêtes sur les Fraudes aux Technologies de l'Information) - Pour plus d'informations : www.clusif.fr (Portail Cybervictime) ;

➢ Prévoir des solutions de secours en cas d'indisponibilité du système informatique (assistance dépannage – mise à disposition de matériel de secours).

Recours à la sous-traitance

Les 10 points clés du contrat de sous-traitance (*source : Guide SSI – Medef 2005*)

➢ S'assurer de la santé financière du prestataire

➢ Veiller au respect de la confidentialité des informations (clauses de confidentialité)

Le contrat de sous-traitance

1. Mention dans le document contractuel de l'ensemble des documents (cahier des charges, propositions du prestataire…) **- 2.** Description précise des prestations **- 3.** Régime de l'obligation du prestataire (moyens ou résultats) **- 4.** Prix des prestations (critères d'évolution des prix) **- 5.** Etablissement du montant des pénalités **- 6.** Définition du statut et la propriété des matériels et logiciels **- 7.** Etendue de la responsabilité **- 8.** Limitation du préjudice réparable **- 9.** Cession de droits (développement de logiciels par le prestataire) **- 10.** Juridiction compétente en cas de litige

Quels enjeux juridiques ?

(les principaux)

Risque de mise en cause civile ou pénale de l'entreprise induite par le comportement de ses salariés :

- L'utilisation malveillante des moyens informatiques et de communications électroniques (messagerie, forums) (contenus diffamatoires à l'égard de tiers par exemple) ;
- Le téléchargement de documents ouvrant droit à des poursuites pénales (pédophiles, incitation à la haine raciale …) ;
- La contrefaçon : utilisation de copies illicites de logiciels ou d'œuvres protégées sans autorisation des ayants droits ;
- Traitement de données nominatives sans autorisation (cf. www.cnil.fr et fiche sur la collecte d'information) ;
- Le non respect du secret des correspondances privées.

En cas de défaut de protection de son système d'information, la responsabilité de l'entreprise peut également être engagée :

- Par ses partenaires extérieurs (atteinte à leur système d'information, non respect des engagements de livraison, de confidentialité …) ;
- Par ses actionnaires et ses salariés (mise en cause du dirigeant pour faute de gestion).

La responsabilité du chef d'entreprise peut être également mise en cause en cas de non respect des procédures dans la mise en place d'un processus de cybersurveillance des salariés (cf. www.cnil.fr)

L'entreprise est soumise à la nécessite de veiller à **l'intégrité,** la **confidentialité,** la **disponibilité,** et la **traçabilité** de ses informations et de mettre en place les moyens adaptés tant d'un point de vue technique qu'organisationnel (procédures – encadrement du comportement humain).

Sites et documents de référence : « Guide sécurité, fiches pratiques », Haut fonctionnaire de défense et de sécurité, ministères de l'Économie et du Budget, 2009 // www.ssi.gouv.fr // Passeport « Protégez votre information stratégique », Préfecture de la région Basse-Normandie, 2010 // Guide pratique du chef d'entreprise face au risque numérique, 3e Forum international sur la Cybercriminalité, 2009 // www.afnor.org (norme ISO 27001 : référentiel pour le management de la certification de la sécurité des systèmes d'information – stratégies – mise en œuvre et bonnes pratiques ; Référentiel de bonnes pratiques « Sécurité des informations stratégiques », 2002) // CLUSIF : Menaces Informatiques et Pratiques de Sécurité en France, 2010 – Maîtrise et Protection de l'Information, juin 2006 (www.clusif.fr) // Sécurité économique : Les bonnes pratiques pour votre entreprise, Comité Opérationnel Défensif à l'Intelligence Economique de Lorraine // Dispositif de Sécurité Economique, Comité Opérationnel de Sécurité Economique de Basse-Normandie // Guide méthodologique de Sécurité économique dans les pôles de compétitivité, INHES // Guide SSI, Medef, 2005 // www.securite-informatique.gouv.fr // Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&categorieLien=id)