Sécurité des Systèmes d'Information

Guide pratique à l'usage des dirigeants

Sommaire

La Sécurité des Système d'Information ne se résume pas à protéger son informatique

Un dégât des eaux, pas de sauvegarde à l'abri et c'est votre entreprise qui est en péril. Vos procédés de fabrication piratés, c'est votre bénéfice qui s'envole.
Que vous utilisiez un peu ou beaucoup l'informatique, votre entreprise en est forcément dépendante.
Et si la survie de votre entreprise tenait à la sécurité de votre système d'Information (SI) ?

Pourquoi protéger son SI ?

Usage d'outils nomades (téléphone, PDA, clés USB), accès distants aux données internes de l'entreprise, connexion sans fil à Internet … : ces nouveaux usages facilitent la dématérialisation et la circulation de l'information mais génèrent de nouveaux risques.
Selon une étude réalisée par l'Espace Numérique Entreprises auprès de 350 PME du Rhône, plus d'un tiers des entreprises **reconnaissent avoir perdu des données dans l'année**. Quelles qu'en soient les causes, ces pertes engendrent des coûts directs (remplacement des équipements, chômage technique des salariés) et indirects (perte d'image) ainsi que des conséquences parfois irréversibles pour l'entreprise.

Sécuriser son système d'information ne se résume pas qu'à prendre de nouvelles mesures techniques, c'est aussi protéger l'information stratégique de l'entreprise (plans, fichiers client, etc.). Le vol ou l'altération de ces données capitales aura certainement des des conséquences parfois irréversibles pour l'entreprise.

Qu'est ce qu'un système d'information ?

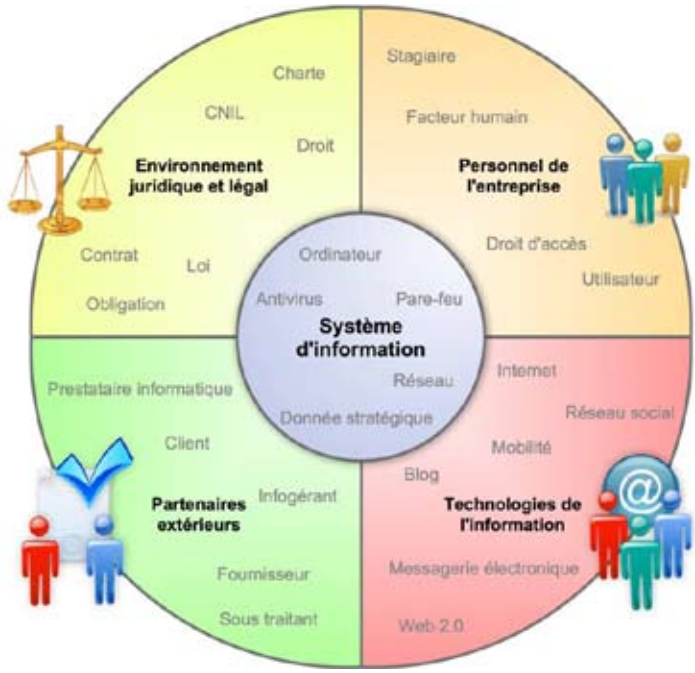
A la base de tout fonctionnement d'entreprise, il y a des informations utilisées par une ou plusieurs personnes. Pour traiter, stocker et transmettre ces informations, les collaborateurs utilisent des outils (informatiques ou pas) et agissent selon des procédures d'utilisation (envoyer un email, créer ou archiver un document …).

Cet ensemble organisé de moyens techniques, administratifs, et humains permettant de gérer l'information dans l'entreprise s'appelle un système d'information (SI).

Par ailleurs, la sécurité des systèmes d'information représente également un avantage concurrentiel car elle offre la garantie aux clients et partenaires que les informations confidentielles, confiées à votre entreprise (cahiers des charges, plans), sont protégées.

Pourquoi ce guide ?

Ce guide est le fruit d'une démarche entreprise par les services de l'Etat pour sensibiliser les dirigeants à la sécurité des systèmes d'information. Il se compose de 10 fiches pratiques traitant de manière synthétique des règles élémentaires de SSI.



Qu'est ce que la sécurité des systèmes d'information ?

L'informatique n'étant finalement qu'un moyen de faciliter la gestion de l'information, il serait donc réducteur de considérer que protéger ses outils, c'est protéger l'information de l'entreprise. La sécurité des systèmes d'information (SSI) prend en compte tous les éléments qui composent le SI : les utilisateurs, les procédures et les outils.

Protéger son SI, c'est donc aussi sensibiliser les utilisateurs à la sécurité ou revoir certaines procédures comportant des risques pour le patrimoine informationnel de l'entreprise.

Evaluer l'importance de ses informations pour mieux les protéger

« Ce n'était qu'un fichier parmi tant d'autres mais mises à disposition d'un concurrent, les données sont devenues des informations stratégiques. »

Tous les éléments d'un système d'information n'ont pas besoin d'être sécurisés de la même manière.
Protéger l'ensemble de son système d'information à un même niveau de sécurité se révèlerait d'ailleurs extrêmement coûteux. Certaines informations stratégiques nécessitent une protection importante mais elles ne représentent pas la majorité des données d'une entreprise.

C'est pourquoi la Sécurité d'un Système d'Information (SSI) implique une réflexion au préalable sur la valeur de l'information avant de mettre en place des outils de protection. Le but est de trouver le meilleur compromis entre les moyens que l'on est prêt à consacrer pour se protéger et la volonté de parer les menaces identifiées.

Cette fiche pratique vous explique comment hiérarchiser les données à protéger en fonction de leur importance stratégique et comment mettre en place une politique de sécurité adéquate.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

Voici les points clés à retenir :

- Réaliser un état des lieux afin d'avoir une vision d'ensemble de son système d'information et élaborer une classification des données.
- Formaliser et faire connaître les règles générales de sécurité à tous les acteurs du système d'information.
- Etre sélectif : il est impossible de protéger toute l'information à un fort niveau de sécurité.

Sommaire

1 - Comment identifier ce qui doit être protégé ?

La première étape est de réaliser un état des lieux afin d'avoir une vision d'ensemble de son système d'information.
Il n'est pas toujours facile pour un dirigeant de mesurer l'étendue de l'information détenue par son entreprise car elle n'est généralement pas stockée dans un lieu unique.

Dans un premier temps, commencez par recenser :

- ➲ les ressources internes de votre entreprise : messagerie électronique (emails, contacts, agenda), données stratégiques, fichier clients, données techniques…
- ➲ les ressources de l'entreprise exploitées ou détenues par un prestataire extérieur ou un tiers.
- ➲ les ressources appartenant à un prestataire extérieur exploitées par lui au profit de votre entreprise.

2 - Hiérarchiser la valeur des informations

Pour définir le degré de valeur ajoutée de chaque type de données, hiérarchisez la valeur des informations selon l'importance de leur disponibilité et de leur intégrité.

Attribuez ensuite des droits d'accès aux documents à l'aide de profils utilisateurs selon leur degré de responsabilité dans l'entreprise. Il est préférable de désigner une personne responsable pour ce type d'activité.

Pour vous aider dans la démarche de classification de vos données, vous pouvez vous inspirer librement du tableau ci-dessous.

En voici la légende :

[1] **Information sensible** : information susceptible de causer des préjudices à l'entreprise si elle est révélée à des personnes mal intentionnées pouvant entraîner la perte d'un avantage compétitif ou une dégradation du niveau de sécurité.

[2] **Information stratégique** : information essentielle et critique contenant la valeur ajoutée de l'entreprise (savoir-faire, procédures, méthodes de fabrication…).

Voici quelques exemples donnés à titre indicatif permettant de remplir le tableau :

- ➲ La divulgation d'une proposition commerciale peut permettre à un concurrent de remporter un appel d'offre en proposant un meilleur prix. (information sensible)

Tableau de classification des informations de l'entreprise selon leur degré d'importance

	Information divulgable (faible valeur ajoutée)	**Information sensible**[1] (moyenne valeur ajoutée)	**Information stratégique**[2] (forte valeur ajoutée)	**Accès autorisé pour les personnes**
Contacts et dossiers du personnel				
Factures clients				
Factures fournisseurs				
Listes fournisseurs				
Données comptables				
Relevés de compte				
Propositions commerciales				
Contrats commerciaux				
Contrats de travail				
Données de production				
Grille tarifaire des produits				
Procédés de fabrication				
Veille concurrentielle				
Autre				

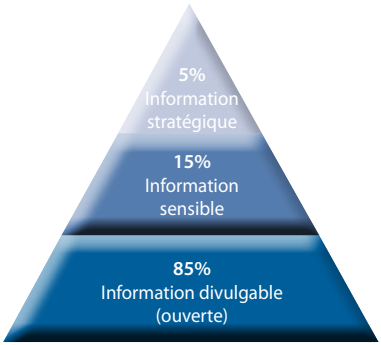
➲ La diffusion d'un catalogue de produits accompagnée des prix permet à des prospects de faire appel aux services de l'entreprise. (information ouverte)

En général, dans les entreprises :

➲ 5% de l'information est stratégique : toute information permettant de mettre à nu la valeur ajoutée de l'entreprise ou divulguant ses avantages compétitifs.

➲ 15 % de l'information est sensible : ensemble des données qui, associées et mises en cohérence, peuvent révéler une partie de l'information stratégique.

➲ 80% de l'information est divulgable (ouverte) : ensemble des données diffusables à l'extérieur de l'entreprise sans pour autant lui être préjudiciable.



Remarque :
Il est courant de dire qu'en matière de SSI, 80% de l'effort en matière de sécurité (budget, ressources) doit être consacré à sécuriser les 20 % de données qui contiennent 80% de l'information stratégique de l'entreprise.

3 - Evaluer les risques

La phase d'évaluation des risques internes et externes permet d'identifier les différentes failles, d'estimer leur probabilité et d'étudier leur impact en estimant le coût des dommages qu'elles causeraient.

3.1. Quelles sont les menaces ?

Une menace est une action susceptible de nuire et de causer des dommages à un système d'information ou à une entreprise.
Elle peut être d'origine humaine (maladresse, attaque) ou technique (panne) et être interne ou externe à l'entreprise.

Le CLUSIF (Club de la Sécurité de l'Information Français) a établi une grille des menaces types et de leurs conséquences dans un document intitulé Plan de continuité d'activité – Stratégie et solutions de secours du SI et publié en 2003[1].

3.2. Quelle est la probabilité qu'une menace se materialise ?

Pour chaque menace, il convient ensuite d'estimer la probabilité qu'elle se concrétise.

Voici, à titre indicatif, un état des causes de perte de données les plus fréquentes chez les entreprises du Rhône :

Source : Observatoire des usages TIC – La sécurité informatique dans les PME rhodaniennes. Espace Numérique Entreprises, 2008.

3.3. Quels impacts pour l'entreprise ?

L'analyse d'impact consiste à mesurer les conséquences d'un risque qui se matérialise.

A titre d'exemple, l'Afnor a établi un système de classification des risques liés aux informations (Tableau ci-après).

[1]Ce dossier est téléchargeable sur le site www.clusif.fr

Tableau de classification des risqueselon le degré d'importance des informations (Afnor)

	3 : secret	2 : confidentiel	1 : diffusion contrôlée
Préjudice potentiel	Préjudice grave Séquelles compromettant l'action à court et moyen terme	Préjudice faible Perturbation ponctuelles	Préjudice faible Perturbation ponctuelles
Risques tolérés	Aucun risque même résiduel n'est acceptable	Des risques très limités peuvent être pris	Des risques sont pris en connaissance de cause
Protection	Recherche d'une protection maximale	Prise en compte de la notion de probabilité d'occurrence	La fréquence et le coût du préjudice potentiel déterminent les mesures prises

Vous pouvez également vous aider de méthodes d'analyse de risques approfondies et reconnues en France telles que :

- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité). Elaborée par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) (renvoi vers le site web ?), cette méthode s'appuie sur une étude du contexte et sur l'expression des besoins de sécurité en vue d'identifier les objectifs de sécurité.

- MEHARI (Méthode Harmonisée d'Analyse de Risques). Elaborée par le CLUSIF (Club de la Sécurité de l'Information Français), cette méthode d'audit permet d'élaborer des scénarios de risques.

4 - Bâtir une politique de sécurité adéquate

4.1. Les grands principes

La SSI repose sur trois finalités :

- **L'intégrité du SI** : s'assurer de son bon fonctionnement, de l'exactitude des données et de leur intégrité.

- **La confidentialité SI** : s'assurer que seules les personnes autorisées ont accès aux données.

- **La disponibilité du SI** : s'assurer que les différentes ressources (ordinateurs, réseaux, périphériques, applications) sont accessibles au moment voulu par les personnes autorisées.

En fonction de ces objectifs, la politique de sécurité de l'entreprise va se décliner de trois manières :

- **Stratégique** : définition des objectifs globaux de sécurité, définition qui découle du travail d'état des lieux, de hiérarchisation des données selon leur importance stratégique et d'analyse des risques.

- **Organisationnel** : plan de secours , charte utilisateur, définition du rôle de chaque membre du personnel, sessions de sensibilisation des collaborateurs à la SSI.

- **Technique** : mise en place des moyens de protection (antivirus, mot de passe…).

4.2. Sécuriser son SI

Il s'agit de mettre en place des mesures préventives et curatives.

Certaines reposent sur des outils et d'autres sur le comportement des utilisateurs.

Mais avant de mettre en place ces mesures, l'entreprise doit d'abord statuer sur 2 questions :

- Quelle est la quantité maximale d'informations qui peut être perdue sans compromettre l'activité de l'entreprise ?

- Quel est le délai maximum de reprise d'activité acceptable sans menacer le fonctionnement de la société ?

La réponse à ces questions va permettre d'évaluer le niveau de sécurité que l'entreprise devra mettre en place et de déterminer les informations qui devront être protégées et rétablies en priorité en cas de sinistre pour générer un minimum de pertes, y compris financières.

◆ **Les mesures préventives**
Elles permettent d'éviter une interruption de l'activité.

Voici les principaux points de vigilance :

➲ **Plan de sauvegarde** : il s'agit de déterminer la fréquence et le type de sauvegarde (complète, différentielle, incrémentale) pour chaque catégorie d'information (basique, sensible, stratégique).

➲ **Sécurité logique** : il convient de mettre en place des outils de protection de base (anti-virus, firewall, anti-spam) et de les mettre à jour. A cela peuvent s'ajouter des contrôles d'accès aux données par mot de passe ou certificat électronique.

➲ **Sécurité physique** : il s'agit de la sécurité des locaux. Une attention particulière doit être portée à la sécurité du serveur de l'entreprise.

➲ **Le facteur humain** : la sécurité des systèmes d'information n'est pas qu'une affaire d'outils mais dépend aussi et surtout d'une information régulière aux utilisateurs de l'informatique dans l'entreprise. Des règles élémentaires (comme ne pas noter son mot de passe sur un papier) doivent être ainsi rappelées.

◆ **Mesures curatives**
Ces mesures sont nécessaires car aucune mesure préventive n'est efficace à 100%. Elles sont mises en œuvre lorsqu'un sinistre survient :

➲ Restauration des dernières sauvegardes
➲ Redémarrage des applications
➲ Redémarrage des machines (ordinateurs…)

5. Pour aller plus loin

◆ **AFNOR : (Association française de normalisation)**
La sécurité des Systèmes d'Information et son management s'appuient sur des normes de la sécurité.
Les plus importantes sont :

➲ ISO 27000 (série de normes dédiées à la sécurité de l'information)
➲ ISO 17799 (code de bonnes pratiques)
➲ ISO TR 13335 (guide d'administration de la sécurité des systèmes d'information « Sécurité informatique : manager et assurer »)

http://www.afnor.fr

◆ **CLUSIF : (Club de la Sécurité de l'Information Français)**
Le Club de la Sécurité de l'Information Français (CLUSIF) est une association œuvrant pour la sécurité de l'information dans les organisations.
Il publie régulièrement des documents techniques et méthodologiques sur le sujet.
http://www.clusif.asso.fr

◆ **ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information**
L'ANSSI représente l'autorité nationale en matière de sécurité des systèmes d'information. A ce titre, elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées.

Dans le domaine de la défense informatique, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. L'agence va créer un centre de détection précoce des attaques informatiques.
http://www.ssi.gouv.fr

◆ **Portail de la sécurité informatique (SGDN)**
Ce portail propose des fiches pratiques et des conseils destinés à tous les publics (particuliers, professionnels, PME). Il comporte également des actualités et avertit de menaces nouvellement rencontrées qui appellent une action rapide des utilisateurs pour en limiter les effets.
http://www.securite-informatique.gouv.fr

Quels outils utiliser pour une protection minimum du SI ?

« Des pirates informatiques entraient régulièrement dans notre système d'information via Internet sans que nous nous en apercevions. Jusqu'au jour où certaines de nos informations stratégiques se sont retrouvées chez notre principal concurrent. »

Une entreprise est exposée quotidiennement aux risques d'attaques informatiques. Il est donc primordial de mettre en œuvre de façon préventive des moyens de protection minimaux adaptés.
En matière de sécurité logique[2], une PME a besoin principalement d'outils permettant de préserver des données importantes et de pouvoir échanger ou faire circuler des informations sensibles.

Cette fiche pratique vous informera sur les antivirus, les pare-feux ainsi que l'usage du certificat numérique.

[2]Sécurité logique : sécurité des données.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

Voici les points clés à retenir :

- Choisir des produits de sécurité adaptés à vos besoins.
- Utiliser plusieurs dispositifs de sécurité informatique complémentaires.
- Effectuer régulièrement des mises à jour des anti-virus et appliquer les correctifs de sécurité et les mises à jour des systèmes d'exploitation.
- Ne pas oublier qu'aucun dispositif de sécurité informatique n'est fiable à 100 %.

Sommaire

1. Les outils de protection de base

Il est impératif qu'au sein de votre entreprise, chaque poste de travail et/ou le serveur soit protégé par un antivirus et un pare-feu (firewall) mis à jour.

1.1. L'antivirus

◆ **Qu'est-ce que c'est ?**
Il s'agit d'un logiciel permettant de protéger son poste informatique ou son système contre les infections informatiques (virus, vers[3] ou spyware[4]). Ce logiciel surveille et analyse régulièrement l'ensemble des fichiers puis filtre les contenus suspects. Une fois l'anomalie détectée, il vous en informe et la détruit.

La plupart des logiciels antivirus intègrent également une protection antispam qui permet d'analyser l'ensemble des messages entrants avant qu'ils ne soient délivrés au destinataire.

◆ **Comment fonctionne t-il ?**
L'antivirus fonctionne à partir d'une base d'empreintes de virus connus ou d'un système d'intelligence artificielle détectant les anomalies. C'est pourquoi, pour une efficacité optimale, il est indispensable de le mettre à jour régulièrement (aussi bien la base d'empreintes que l'application elle-même).

Deux fonctionnements sont envisageables pour l'antivirus :

➲ La réparation des anomalies du ou des fichiers infectés. Dans ce cas, les données du fichier sont récupérées et le virus détruit.

➲ La mise en quarantaine du fichier infecté pour l'isoler de l'environnement informatique et en limiter sa propagation et ses effets. L'utilisateur peut accéder aux fichiers mis en quarantaine via l'interface graphique de l'antivirus d'où il peut les supprimer ou les restaurer à leurs emplacements d'origine.

➲ La quarantaine peut malheureusement isoler des fichiers essentiels au fonctionnement du système et altérer ce dernier.

1.2. Le pare-feu

◆ **Qu'est-ce que c'est ?**
Un pare-feu ou firewall (en anglais) désigne un dispositif capable de bloquer les virus et d'éviter la fuite d'informations vers l'extérieur. Lorsque des données sont transmises entre ordinateurs via Internet, les informations entrent et sortent par des portes virtuelles appelées « ports ». Chaque ordinateur dispose de 65 536 ports.

Ces « entrées » sont autant de possibilités de pénétrer dans le système d'information de l'entreprise. Si bien qu'en l'absence de pare-feu, des pirates informatiques ont tout loisir d'infecter ou de détruire les données d'un ordinateur (virus, vers) ou de récupérer des informations via un cheval de Troie[5].

◆ **Comment fonctionne t-il ?**
Un pare-feu joue un rôle de douanier vis-à-vis des ports. Il contrôle les flux de données entrant et sortant de l'ordinateur ou du réseau de l'entreprise.
Il est très fréquent qu'un logiciel professionnel ait besoin d'accéder à un serveur extérieur à l'entreprise pour effectuer des mises à jour. Il lui faut alors communiquer par un canal spécifique (port de communication), à la fois pour émettre des données (port sortant) mais aussi pour en recevoir (port entrant). Les règles de filtrages doivent donc autoriser ces ports de communication pour permettre au logiciel de télécharger la mise à jour.

Il existe deux catégories de pare-feu :

➲ **Le pare-feu personnel** est un logiciel installé sur les postes informatiques permettant de protéger uniquement le système sur lequel il est installé. Windows, par exemple, en comporte un par défaut.

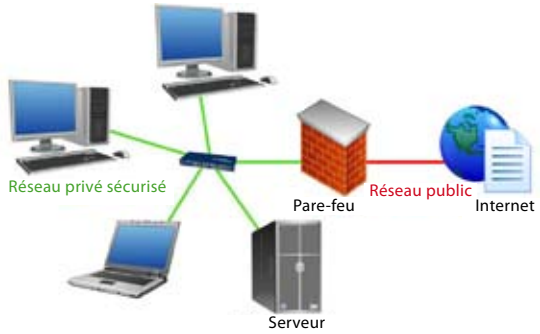
➲ **Le pare-feu réseau** se présente sous forme de boîtier placé entre un accès externe et un réseau d'entreprise.

[3] Vers : virus se propageant de manière autonome dans l'ordinateur et de nouvelles machines.

[4] Spyware : petit programme informatique conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur ou à un tiers via Internet ou tout autre réseau informatique.

[5] Parfois appelés trojans, ces programmes malicieux créent une brèche dans le système d'information de l'entreprise afin de permettre une prise en main à distance d'un ordinateur par un pirate informatique.

Principe de fonctionnement d'un pare-feu réseau



Le mode de fonctionnement reste similaire pour les deux types de pare-feux.

Remarque :

Attention, le pare-feu reste néanmoins insuffisant puisqu'il ne protège pas contre les virus provenant de périphériques amovibles (clé USB).

Certaines offres logicielles proposent des solutions complètes (antivirus, antispam et pare-feu) et parfaitement intégrées à l'environnement informatique des entreprises.

2. Sécuriser les échanges de données

Dès lors que vous souhaitez sécuriser l'envoi d'informations ou l'accès à distance aux données de l'entreprise, il est recommandé de crypter les informations lors de leur transit. Pour ce faire, on utilise couramment un certificat électronique.

2.1. Qu'est ce que c'est ?

Le certificat électronique est une carte d'identité numérique permettant de garantir l'intégrité des informations et documents transmis et de s'assurer de l'identité de l'émetteur et du récepteur de ces données.
Il contient des informations sur :

- L'autorité de certification qui a émis le certificat
- Le certificat électronique (validité, longueur des clefs,…)
- Le titulaire du certificat (nom, prénom, service, fonction) et son entreprise (dénomination, n° Siren).

2.2. Comment s'en procurer ?

Le certificat électronique est délivré pour une durée déterminée par une Autorité de Certification qui joue le rôle de Tiers de confiance. Cet organisme garantit l'identité de la personne et l'usage des clés par une personne qui en est la seule propriétaire.
De plus, elle atteste de l'exactitude des informations contenues dans le certificat.
La liste des autorités de certification référencées par l'Etat est disponible sur le site du ministère de l'Economie, de l'Industrie et de l'Emploi. Aller dans « recherche » et taper « Certificats référencés PRIS v1 »

2.3. Comment ça marche ?

Lorsque les données transitent, elles sont cryptées.
Le certificat électronique fonctionne selon un principe de clé : l'émetteur et le récepteur des données disposent chacun d'une clé publique[6], servant au chiffrement du message, et d'une clé privée[7], servant à déchiffrer le message.
Le certificat numérique consiste à déterminer si une clé publique appartient réellement à son détenteur supposé. Il peut être stocké sur un support logiciel ou matériel (une carte à puce à insérer dans un lecteur de carte ou une clé USB).
Le support matériel reste le plus sûr car le certificat et la clé privée ne sont pas stockés sur un disque dur d'un ordinateur mais sur un support que vous pouvez conserver en lieu sûr.

[6] La clé publique est publiée dans des annuaires publics.
[7] La clé privée est connue uniquement par son propriétaire.

Ceci présente de nombreux avantages:

- Il est impossible de réaliser une copie de la carte ou de la clé USB.
- Ce support est plus économique car il est accepté par toutes les téléprocédures des autorités administratives.
- Il facilite la mobilité car utilisable depuis plusieurs postes de travail.

2.4. Ses usages

Le certificat électronique est de plus en plus utilisé, notamment dans le cadre des téléprocédures administratives (TéléTVA, télécarte grise…).
Voici deux autres types d'usages en entreprise :

◆ **La signature électronique**
Elle possède la même valeur juridique et la même fonction qu'une signature manuscrite. Une différence notable les distingue cependant : alors qu'une signature manuscrite peut être facilement imitée, une signature numérique est pratiquement infalsifiable. La loi accorde d'ailleurs un statut particulier à la signature électronique (cf articles 1316-1 à 1316-4 du code civil).

La clé privée permet de signer et la clé publique de vérifier cette signature. La signature électronique n'est pas visuelle mais est représentée par une suite de nombres.
Plusieurs logiciels (suite bureautique) supportent des outils de signature électronique.

◆ **Le VPN**
Un VPN (Virtual Private Network) permet d'accéder à la totalité des fichiers d'une entreprise en toute sécurité.
Il donne accès au réseau local d'une entreprise à distance via une connexion Internet sécurisée.

Les données qui transitent sont chiffrées grâce à une technique de « tunnel » et donc inaccessibles aux autres internautes. Ce cryptage est rendu possible grâce à un certificat électronique[8].
Celui-ci fonctionne comme un passeport. Il doit être présent à la fois du côté de l'ordinateur distant qui tente d'accéder aux fichiers de l'entreprise et du côté du serveur.

Chaque certificat dispose d'une clef publique et d'une clef privée. Lorsque l'ordinateur distant tente d'accéder aux fichiers, il envoie sa clef publique au serveur. Si celui-ci reconnaît le certificat de l'ordinateur distant, il envoie également sa clef publique.
La connexion VPN est alors établie (le tunnel est créé), les données qui transitent entre les deux parties sont chiffrées et déchiffrées grâce aux certificats.

3. Pour aller plus loin

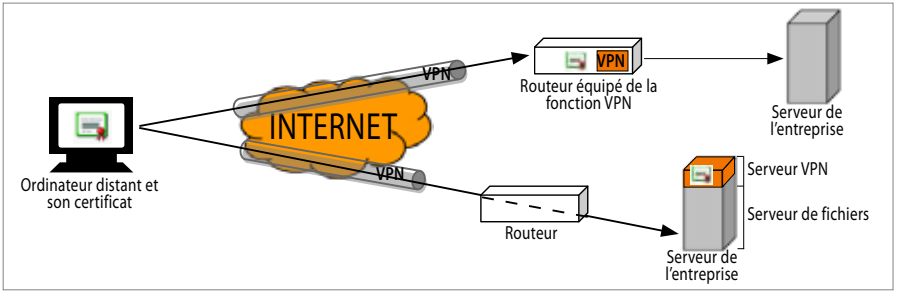
◆ **Guide de vulgarisation « Les virus informatiques démystifiés »**
Il explique les virus, les dommages qu'ils peuvent causer et les méthodes pour les éviter.
http://www.sophos.fr/sophos/docs/fra/comviru/viru_bfr.pdf

◆ **Dématériel.com**
http://www.demateriel.com

◆ **Comment ça marche :** Rubrique Dossiers /Sécurité/Cryptographie
http://www.commentcamarche.net

[8] Il est possible d'utiliser un VPN sans certificat électronique mais ce n'est pas recommandé pour des raisons de sécurité

Accès au serveur de fichiers à distance grâce à un VPN



Sécuriser son SI lors des déplacements professionnels

« Sur un salon, un de nos collaborateurs n'a pas pris garde qu'on lui dérobait sa clé USB pendant qu'il discutait avec un client. Or celle-ci contenait la liste de ses prospects. »

Travailler en dehors de l'entreprise est aujourd'hui facilité par une pléiade d'outils et d'applications. Désormais, il est possible se connecter à Internet presque partout sans fil, de transporter dans sa poche des centaines de documents ou encore d'envoyer un contrat via un téléphone.
Ces « outils de la mobilité » engendrent toutefois de nouveaux risques pour le système d'information de l'entreprise, les plus courants restant le vol et la perte d'un matériel contenant des données importantes (clé USB, smartphone, ordinateur portable). Des règles de sécurité s'imposent donc pour utiliser ces outils sans danger.

Cette fiche pratique fournit des conseils pratiques sur les règles de vigilances pour utiliser les outils de la mobilité au cours de déplacements professionnels.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

Voici les points clés à retenir :

- Eviter de divulguer oralement ou par écrit des informations stratégiques dans les lieux publics (hôtels, salons, congrès, …) et les transports en commun.
- Rester discret sur les projets de l'entreprise envers les prospects, les clients, les fournisseurs et plus généralement dès que l'on se trouve en dehors de l'entreprise.
- Ne pas se déplacer à l'extérieur de l'entreprise avec des documents confidentiels. Au besoin, utiliser une clé USB ou des accès VPN (Virtual Private Network) sécurisés.
- Garder toujours en sa possession les périphériques de stockage amovible (disques durs externes, clés USB).
- Ne jamais laisser sans surveillance du matériel (ordinateur portable, téléphone portable, agenda, carte de visite client et fournisseur) ou des documents professionnels.

Sommaire

1. Une attitude vigilante

Pendant vos déplacements, il convient de rester vigilant et d'observer quelques principes :

- Etre attentif aux personnes qui vous entourent et à leurs actions.
- Se méfier des comportements trop amicaux.
- Rester en permanence en pleine possession de ses capacités d'attention (l'alcool est à proscrire). Vous risquez sinon de dévoiler des informations sensibles malgré vous.
- Se méfier d'une question trop ciblée : les réponses mises en commun peuvent dévoiler des informations stratégiques.
- Savoir répondre habilement aux questions de manière à ne pas fournir d'informations stratégiques sur votre entreprise.
- Sur un salon professionnel, ne jamais être seul sur un stand.
- Ne jamais laisser d'informations confidentielles dans le coffre-fort d'une chambre d'hôtel, une soute à bagages ou encore les vestiaires d'un restaurant.
- Travailler sur des documents non confidentiels pendant vos déplacements.
- Ne pas discuter au téléphone d'informations stratégiques.

2. Protection des accès aux données

Si, malgré votre vigilance, votre matériel est volé ou perdu, veillez à verrouillez l'accès à vos données.

Plusieurs possibilités s'offrent à vous :

- Mettre en place un dispositif d'authentification de l'utilisateur lors de la mise en marche des ordinateurs portables (mot de passe ou système de reconnaissance biométrique comme l'empreinte digitale).
- Crypter les données du disque dur des ordinateurs portables.
- Privilégier l'utilisation de supports amovibles cryptés et facilement transportables (comme une clé USB) pour emporter l'ensemble des documents confidentiels.

Remarque :

Dans certains pays (USA, Israël, Chine…), des informations confidentielles peuvent être demandées et les disques durs contrôlés par le service de sécurité dans le cadre de la politique de défense des services de l'Etat. C'est pourquoi un cryptage des données n'est pas superflu.

3. Utiliser les réseaux sans fil avec prudence

3.1. Pour se connecter à Internet

De plus en plus de lieux publics sont équipés de Wifi via des hotspots. Cette technologie permet de se connecter à Internet facilement mais présente des risques de vols de données.

Voici quelques conseils pour utiliser le Wifi sereinement :

- Utiliser des réseaux Wifi équipés de clés de cryptage (WPA).
- Désactiver par défaut les fonctions de liaison sans fil Wifi si vous n'en avez pas l'utilité.
- S'assurer que les procédures de sécurité intégrées sont activées (méthode d'authentification et de chiffrement) et permettent l'identification des équipements par un certificat.
- Mettre à jour les logiciels des équipements Wifi. Ils peuvent être téléchargés sur le site du constructeur de votre périphérique (ordinateur portable, PDA, …) avant tout déplacement.

D'une manière générale, privilégiez l'utilisation d'une clé 3G+ sécurisée (Internet par le réseau de téléphonie portable) pour accéder à Internet.

3.2. Pour échanger des documents

La technologie Bluetooth est un système de communication radio de faible portée (10 à 15 mètres) qui permet les échanges de voix et de données entre équipements numériques. Pratique et facile d'utilisation, il est très facile de s'y connecter.

C'est pourquoi il mérite une configuration adéquate :

- Ne pas laisser actif le Bluetooth en permanence sur vos appareils.
- Limiter les échanges de données en refusant les fichiers de personnes inconnues.
- Ne pas installer de programmes provenant du réseau Bluetooth (ceux-ci peuvent être un virus ou un programme malveillant).
- Paramétrer l'accessibilité du Bluetooth en mode non détectable (seules les personnes à qui vous avez transmis l'identifiant de votre appareil pourront communiquer avec vous).
- Appliquer les dernières mises à jour de sécurité.

3.3. Pour téléphoner

Le faible niveau de sécurité des téléphones GSM et des PDA ainsi que leur totale traçabilité doivent être pris en compte par les utilisateurs.

Restez vigilant quand vous emportez des documents professionnels accessibles depuis votre téléphone portable car il est beaucoup plus facilement perdu ou volé.

De plus, il existe des systèmes d'interception des appels via des logiciels disponibles sur Internet qui permettent de mettre sur écoute une communication téléphonique à distance.

4. Pour aller plus loin

◆ **Les guides des Conseillers du Commerce Extérieur :**
Veiller futé à l'international, 2ème tome - Le savoir-faire des CCE - Mai 2009
http://www.cnccef.org

◆ **Guide des bonnes pratiques en matière d'intelligence économique**
Préfecture de la région Franche-Comté et Préfecture du Doubs.
http://franche-comte.cci.fr/crci/biblio/doc/Guidebonnes pratiques IE.pdf

◆ **Guide bonnes pratiques en matière d'Intelligence Economique**
Chambre Régionale de Commerce et d'Industrie de Lorraine.
http://www.lorraine.cci.fr/download/pdf/guide_ie.pdf

◆ **Guide de sensibilisation à la sécurisation du système d'information et du patrimoine informationnel de l'entreprise**
MEDEF
http://www.cyber.ccip.fr/pdf/medefsecusi.pdf

Gérer le courrier électronique indésirable

« Chaque jour, les collaborateurs perdent du temps à faire le tri entre les messages électroniques sollicités et les spams. Les gains de productivité de la communication par email s'amoindrissent de plus en plus. »

Le courrier électronique est aujourd'hui largement utilisé dans les entreprises. Le nombre croissant d'emails publicitaires ou malveillants rend néanmoins sa gestion problématique.
Ces courriers électroniques non sollicités portent le nom de spams ou pourriels. Ils représentent près de 50% du trafic quotidien d'emails.

Cette fiche vous aidera à mieux gérer et sécuriser votre messagerie électronique.

Voici les points clés à retenir :

- Utiliser un anti-spam
- Se méfier des adresses électroniques d'expéditeurs inconnus et ne pas ouvrir les courriers électroniques douteux (sujet du message sans intérêt).
- Ne pas diffuser son adresse électronique à n'importe qui ou sur un site internet où elle peut être récupérée très facilement.
- Paramétrer la messagerie électronique pour désactiver l'ouverture automatique des pièces jointes et des images.
- Sensibiliser le personnel aux risques : virus, phishing…
- Ne jamais répondre à un spam.

Sommaire

1. Le spam, qu'est-ce que c'est ?

1.1. Origine du mot

A l'origine, « SPAM » est la marque déposée d'une conserve de jambon épicée « SPiced hAM », consommée en très grande quantité par les américains lors de la seconde guerre mondiale et redevenue populaire grâce aux Monthy Pythons en 1970.

En 1994, un internaute excédé utilise ce terme pour la 1ère fois sur Internet pour dénoncer la première pratique de SPAM de l'histoire.

1.2. Principe

Le spam consiste à envoyer massivement des emails non sollicités à des fins marchandes (vente de médicaments par exemple) ou malveillantes (récupération d'adresse emails valides, propagation de virus). Ce type de courrier électronique n'est généralement pas ciblé mais envoyé à une multitude de destinataires par l'intermédiaire de serveurs automatisés.

1.3. Exemple de spam très répandu : le phishing

◆ **Qu'est-ce-que c'est ?**

Le phishing ou hammeçonnage est l'association d'un e-mail non sollicité (spam) avec un lien vers un site internet illégal reproduisant l'allure visuelle d'un site commercial et incitant l'internaute à y inscrire des informations personnelles.

Ce type de spam, très construit et ciblé, est utilisé par des personnes malveillantes dans le but d'obtenir notamment des informations bancaires et d'effectuer des paiements frauduleux.

◆ **Comment se protéger du phishing ?**

➲ Ne jamais envoyer par mail des informations confidentielles (mot de passe, numéro de carte de crédit…)

➲ Être vigilant lorsqu'un e-mail demande des actions urgentes.

➲ Ne pas cliquer sur les liens contenus dans les courriers électroniques : les liens affichés peuvent en réalité vous diriger vers des sites frauduleux.

➲ Utiliser les filtres du navigateur Internet contre le phishing. La plupart des navigateurs proposent une fonction d'alerte contre le spam, fonction régulièrement mise à jour.

2. Les impacts du spam

➲ La saturation du réseau ou des serveurs de messagerie de l'entreprise.

➲ Des risques de blocage de l'adresse IP de l'entreprise par les fournisseurs d'accès Internet si l'adresse de l'entreprise est usurpée par un spammeur.

➲ Le gaspillage de la bande passante et de l'espace de stockage des utilisateurs.

➲ La dégradation de l'image de l'entreprise si l'adresse de l'entreprise est usurpée par un spammeur.

➲ La perte de productivité des employés qui risquent de surcroit de passer à coté d'emails importants.

3. Comment se protéger contre le spam?

3.1. Eviter d'être spammé

➲ Ne jamais répondre à un message dont l'objet ou l'expéditeur est douteux.

➲ Ne pas diffuser son adresse sur le web (dans des forums ou des sites par exemple).

➲ Créer une ou plusieurs « adresses poubelles » servant uniquement à vous inscrire ou vous identifier sur les sites jugés dignes de confiance.

➲ Sur son site Internet, crypter les adresses de la page contact.

➲ Paramétrer la messagerie électronique pour désactiver l'ouverture automatique des pièces jointes et des images. Dans la mesure du possible, désactiver la fonction de prévisualisation systématique des images contenues dans les courriers électroniques.

➲ Ne pas ouvrir les pièces jointes de messages douteux.

➲ Ne jamais ouvrir une pièce jointe avec l'extension .exe ou .src, car ce sont des fichiers exécutables pouvant infecter l'ordinateur.

3.2. Mettre en place un anti spam

◆ **Les logiciels**

Il existe différents types de logiciels anti-spam. Vous pouvez en choisir un seul ou en cumuler plusieurs. Pour les entreprises possédant moins de 500 postes informatiques, 3 types d'outils sont conseillés :

➲ **Les outils clients** : il s'agit de logiciels installés sur chaque poste informatique.

➲ **Les outils serveurs** : les messages reçus sont filtrés dès leur arrivée dans le serveur de messagerie avant d'être remis au destinataire.

➲ **Les solutions hébergées** : dans ce cas, l'analyse anti-spam intervient avant que le message n'arrive dans le serveur de messagerie. Le filtrage peut être réalisé par le fournisseur d'accès ou par une analyse anti-spam externalisée. Dans ce dernier cas, les messages sont redirigés vers une société qui filtre les messages entrants avant de les transmettre au serveur de messagerie de l'entreprise.

➲ Au-delà de 500 postes informatiques, l'entreprise a intérêt à investir dans un boîtier anti-spam. Cet outil analyse et filtre les messages avant qu'ils n'arrivent au serveur de messagerie.

◆ **Les méthodes de filtres anti-spam**

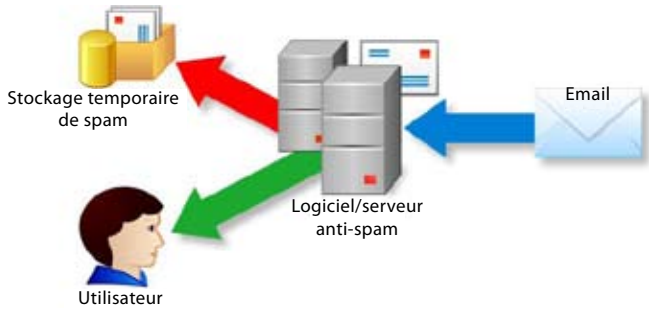
Ces logiciels utilisent une ou plusieurs des méthodes de filtrage suivantes.

➲ **Le filtrage par mot clé** permet d'effectuer un blocage des emails contenant certains mots répertoriés dans un dictionnaire de détection. Toutefois, il est très facile pour le spammeur de contourner cette technique.

➲ **Le filtrage par analyse lexicale** (bayésien) consiste à rechercher des mots clés associés à un système de pondération. Difficile à contourner, il tient compte de l'ensemble du message, est multilingue et utilise l'intelligence artificielle.

➲ **Le filtrage heuristique** consiste à analyser le contenu des messages en vérifiant la présence de forme et de code (HTML dans le corps du message, mots écrits uniquement avec des lettres majuscules ; mots clés correspondants à des produits souvent vantés au travers du Spam, très grand nombre de destinataires…). Cette technique vérifie beaucoup de règles mais elle nécessite une maintenance importante.

Principe de fonctionnement d'un logiciel anti-spam hébergé



➲ **Le filtrage d'image** permet d'analyser les images contenues dans les messages.

➲ **Le filtrage par signature électronique** génère une signature pour chaque email ou pièce jointe reçue puis les compare à des messages de spam qui ont une signature connue. La signature électronique permet de certifier que vous êtes bien l'expéditeur du message et qu'il n'a pas subi de modification.

➲ **Le filtrage d'URL** permet de vérifier des liens hypertextes contenus dans les messages généralement répertoriés sur des listes noires[9]. Pour contourner ce filtrage, le spammeur peut choisir de dissimuler le lien hypertexte.

➲ **Le filtrage par détection humaine**, appelé test de Turing, consiste à vérifier si l'émetteur du courrier électronique est un humain ou un robot. Pour ce faire, on va demander à l'expéditeur du courrier de faire une action qu'un robot ne sait pas faire : par exemple, recopier les lettres d'une image (exemple ci-dessous). Si le courrier n'est pas accepté, il est n'est pas envoyé au destinataire.

Exemple de CAPTCHA[10] : recopier le mot lu sur l'image

Afin d'assurer une protection minimale, un outil anti-spam réellement fonctionnel et performant doit utiliser au moins deux méthodes de filtrage. Le test de Turing et le filtrage par analyse lexicale restent les deux solutions anti-spam les plus évoluées actuellement.

4. Pour aller plus loin

◆ **Cases Luxembourg : Portail de la sécurité de l'information**
Ce site a pour objectif de développer un réseau opérant dans le domaine de la prévention et de la protection des systèmes d'information et de la communication. Il veille à la promotion des outils de protection informatique.
Plusieurs fiches pratiques traitent des différents types de spams qui existent.
http://www.cases.public.lu

◆ **Signal Spam**
Ce site regroupe la plupart des organisations françaises concernées par la lutte contre le spam, qu'il s'agisse des pouvoirs publics ou des professionnels de l'Internet. Il a pour objet de fédérer les efforts de tous pour lutter contre le fléau du spam.
http://www.signal-spam.fr

◆ **Internet-signalement**
Portail officiel de signalement des contenus illicites de l'Internet.
https://www.internet-signalement.gouv.fr

[9] Les listes noires (ou blacklist) sont des listes où figurent un ensemble d'adresses de serveurs identifiés comme « mauvais expéditeurs » et dont on refuse de recevoir les messages.

[10] CAPTCHA : Système de contrôle d'accès aux sites Internet.

Comment sauvegarder vos données numériques ?

« Un incendie s'est déclaré pendant la nuit dans le local où était stocké notre serveur. Malheureusement, c'était aussi dans cette pièce que nous entreposions les supports de sauvegarde. »

La sauvegarde informatique est en quelque sorte l'assurance vie du capital informationnel de l'entreprise. Elle permet de restaurer des données perdues ou altérées et participe ainsi à garantir la continuité de l'activité.
C'est pourquoi la sauvegarde des données numériques nécessite une gestion méthodique et contrôlée.

Cette fiche pratique vous aidera à :
- ➲ Elaborer un plan de sauvegarde adapté à votre entreprise.
- ➲ Adopter les bons réflexes pour conserver vos données numériques.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

Voici les points clés à retenir :

- ➲ Définir une fréquence de sauvegarde adaptée à l'importance des données.
- ➲ Stocker les supports de sauvegarde dans un lieu sécurisé (armoire ignifugée étanche, coffre fort, site externe).
- ➲ Installer les serveurs dans un local fermé à clé.
- ➲ Vérifier régulièrement le bon fonctionnement des dispositifs et procédures de sauvegarde.
- ➲ Transporter régulièrement des copies de sauvegarde en dehors de l'entreprise.

Si possible :
- ➲ Aménager un site de secours pour les applications vitales.
- ➲ Dupliquer les sauvegardes et répartir les informations sensibles sur plusieurs supports.

Sommaire

1. Etablir un état des lieux des données à sauvegarder

Il s'agit, dans un premier temps, de faire l'inventaire des données de l'entreprise : fichiers, base de données, emails, etc. Puis, les informations stratégiques devront être identifiées car une attention particulière devra leur être portée en matière de fréquence et de support de sauvegarde.

Enfin, il convient de distinguer les données hébergées par l'entreprise et celles hébergées par un tiers. Dans le cas où le stockage des informations est à la charge d'un prestataire informatique (ex : pages d'un site Internet), vérifiez les conditions d'hébergement et de sauvegarde des données.

2. Choisir le type de sauvegarde

2.1. Sauvegarde complète

Elle permet de réaliser une copie conforme des données à sauvegarder sur un support de sauvegarde séparé.

Avantages	Inconvénients
Sauvegarde très sûre, plus précise et plus simple pour restaurer les données sans erreur.	Problème de lenteur et de temps en cas d'importants volumes de données à sauvegarder.

2.2. Sauvegarde au fil de l'eau : sauvegarde incrémentale

Elle se limite uniquement aux informations modifiées ou ajoutées depuis la dernière sauvegarde.

Avantages	Inconvénients
- Sauvegarde plus performante et plus rapide des dernières modifications qu'une sauvegarde complète. - Espace de stockage plus faible.	Le temps d'analyse des modifications. Le risque lors de la restauration des données[11].

[11] Restauration de données : action de régénérer des données perdues ou altérées.

2.3. Sauvegarde différentielle

Elle permet de sauvegarder toutes les informations modifiées ou ajoutées depuis la dernière sauvegarde complète.

Avantages	Inconvénients
- Sauvegarde plus rapide que la sauvegarde complète. - Données moins volumineuses. - Plus fiable que la sauvegarde incrémentale.	- Prend plus de temps que la sauvegarde incrémentale. - Plus coûteuse en espace de stockage. - Pas de rémanence (ne restaure que le dernier état d'un fichier).

3. Choisir la fréquence des sauvegardes

La périodicité et la durée des sauvegardes dépendent de plusieurs facteurs :

- ➲ Le volume de données.
- ➲ La vitesse d'évolution des données.
- ➲ La quantité d'information que l'on accepte de perdre.
- ➲ Eventuellement, la durée légale de conservation de l'information (ex : facture).

C'est pourquoi, selon les entreprises, la stratégie de sauvegarde sera différente.

Voici un exemple de stratégie de sauvegarde :

Fréquence de sauvegarde:

- Une sauvegarde complète dans la nuit du vendredi au samedi pour ne pas gêner l'activité de l'entreprise.
- Une sauvegarde incrémentale les autres nuits.
- Une sauvegarde système (serveurs et applications de production) une fois par mois.
- Le support de sauvegarde journalière du lundi au jeudi est doublé et utilisé par alternance toutes les deux semaines.

Délai de conservation des sauvegardes :

- Le support du vendredi est conservé 1 mois comme sauvegarde hebdomadaire.
- Le support du dernier vendredi du mois est conservé 1 an comme sauvegarde mensuelle.
- Le support du dernier vendredi de l'année est conservé sans limitation de durée comme sauvegarde annuelle.

Des sauvegardes spécifiques peuvent être réalisées en parallèle pour des données sensibles comme les données financières de l'entreprise et conservées suivant les obligations légales (s'assurer que les applications ayant générées ces données soient également accessibles).

4. Choisir le support de sauvegarde

4.1. Sauvegarde en interne

◆ **Sur des supports de petit volume de stockage (DVD, clé USB, disque dur externe)**
Pour les opérations quotidiennes, utiliser le disque dur externe est simple, rapide et fiable. Si votre entreprise possède seulement quelques postes informatiques, vous pouvez programmer les sauvegardes directement sur votre ordinateur.

Ce type de sauvegarde est préconisé pour des quantités d´information assez faibles. Le principe consiste à sélectionner les fichiers à sauvegarder poste par poste puis de procéder à leur sauvegarde.

◆ **Sur des bandes magnétiques ou cartouches numériques[12]**
Ces supports sont utilisés pour la sauvegarde de données stockées sur un serveur. Ils s'utilisent avec une application dédiée qui programme, gère et teste les enregistrements.

Les coûts matériels sont relativement faibles. En revanche, les sauvegardes réalisées ne se faisant pas toujours en temps réel, il y a un risque de perte de d'information. Par ailleurs, la restauration de données nécessite également des compétences techniques.

◆ **Sur le serveur du réseau interne de l'entreprise**
Il s'agit de réserver un espace dédié à la sauvegarde sur le disque dur du serveur.
Toutefois, préférez les modèles proposant une version amovible de ce disque dur de secours afin d'éviter qu'en cas de sinistre, le serveur et sa sauvegarde ne soient détruits.

[12] Cartouche numérique : bandes magnétiques intégrées dans un boîtier plastique et moins volumineux que la bande magnétique.

Par ailleurs, il est possible de configurer le serveur pour que l'espace dédié à la sauvegarde soit une copie exacte en temps réel du disque dur principal.

Remarque :

Il est nécessaire de veiller à bien sécuriser le local dédié aux supports de sauvegarde. Dans l'idéal, il est préférable de les stocker en dehors de l'entreprise.

4.2. Sauvegarde à distance

Elle consiste à sous-traiter la sauvegarde des données à un prestataire spécialisé dans l'hébergement. Cette solution offre l'avantage de ne plus avoir à gérer le support physique des sauvegardes ou la charge de travail associée, car ils sont externalisés via un réseau haut débit.

Toutefois, des risques associés à de mauvaises sauvegardes subsistent. Il est d'ailleurs nécessaire de bien définir les données à sauvegarder, leur dimensionnement et s'assurer que les sauvegardes sont bien réalisées.

Par ailleurs, le choix d'une solution de sauvegarde à distance doit être associé à une lecture attentive des contrats de service. Il convient de s'assurer qu'en cas de problème, la prestation soit efficace.
Il est d'ailleurs intéressant de procéder à un test préalable afin de voir concrètement les fonctionnalités et performances de cette solution. Il est également recommandé de vérifier la santé financière de ce prestataire stratégique et la présence d'un cryptage des données sauvegardées par ses soins.

5. Tester l'intégrité des données

Afin de s'assurer du bon fonctionnement des sauvegardes, des tests réguliers d'intégrité et de restauration des données doivent être réalisés pour détecter d'éventuelles anomalies (erreur d'application ou support saturé).
Le test de restauration consiste à simuler un sinistre et à utiliser des sauvegardes pour que l'entreprise puisse reprendre son activité.

Une vérification partielle permet de tester uniquement les fichiers les plus importants alors qu'une vérification complète permet de tester l'ensemble des fichiers.

6. Pour aller plus loin

6.1. Le plan de sauvegarde

Le plan de sauvegarde permet d'organiser la restauration des données en cas de sinistre. Ce document formel est utilisé au cas où plus rien ne fonctionne.

Il doit ainsi garantir la continuité de la disponibilité des données et des activités de l'entreprise.
Il consiste principalement à prioriser les ressources informationnelles à restaurer (messagerie, documents internes…).
Le plan de sauvegarde doit être approuvé par la direction et testé périodiquement (au moins une fois par an) afin de s'assurer de son bon fonctionnement.

6.2. Bibliographie

◆ **Les dossiers du numérique n°3 - La sécurisation du système d'information de l'entreprise**
Rhône Alpes Numérique
www.agencenumerique.com

Les droits et obligations du chef d'entreprise en matière de SSI

« Nous avons envoyé un e-mailing pour faire connaître notre nouveau produit à une liste de contacts fournie gracieusement par un partenaire. L'un des destinataires, mécontent de recevoir notre publicité, nous a menacés de porter plainte. »

Aujourd'hui, tous les chefs d'entreprises sont soumis à diverses réglementations. Ces obligations valent également en matière de sécurité informatique.
Ils doivent donc être en mesure de respecter et de faire respecter certaines obligations légales au sein de l'entreprise pour éviter que leur responsabilité civile et/ou pénale[13] et celle de leur entreprise ne soit engagée, y compris en cas de négligence de leur part.
En contrepartie, ce cadre juridique permet aux entreprises de se défendre en cas d'attaque sur leur système d'information ou de négligence interne.

Cette fiche pratique vous présentera les principales dispositions juridiques à appliquer en matière de sécurité informatique.

La présente fiche a été établie avec la collaboration de Me Raphaël Peuchot, avocat au Barreau de Lyon.

[13] La responsabilité civile : l'employeur est civilement responsable de fait de l'activité de ses employés, notamment en cas d'utilisation malveillante des moyens informatiques et de communication électronique au préjudice des tiers.

La responsabilité pénale : l'employeur peut être pénalement responsable de son propre fait et l'entreprise du fait des agissements des employés dès lors qu'ils commettent des infractions susceptibles d'engager la responsabilité pénale des personnes morales.

POINTS CLES

Voici les points clés à retenir :

- Prévoir des moyens de traçabilité et de conservation des connexions au réseau.
- Informer les salariés de leurs droits et obligations au moyen d'une charte informatique pertinente.
- Organiser une surveillance du réseau informatique de l'entreprise en respectant les droits des salariés.
- Mettre l'entreprise en conformité avec la législation relative à la protection des données à caractère personnel.
- Vérifier périodiquement la validité des licences logicielles pour éviter toute contrefaçon.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

Sommaire

1. Les obligations légales

Voici les principales obligations qu'une PME doit respecter.

1.1. Le traitement des données à caractère personnel

◆ **De quoi s'agit-il ?**

Les données sont considérées à caractère personnel dès lors qu'elles concernent des personnes physiques identifiées directement ou indirectement. Une personne est identifiée lorsque, par exemple, son nom apparaît dans un fichier et identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification (ex. : n° d'immatriculation, adresse IP, n° de téléphone, photographie...).

En ce sens, toutes les informations dont le recoupement permet d'identifier une personne précise (ex : une empreinte digitale, l'ADN, une date de naissance associée à une commune de résidence …) constituent également des données à caractère personnel.

Aussi, dès lors que vous diffusez une newsletter, que vous collectez des informations sur les visiteurs de votre site Internet ou que votre fichier client est informatisé, vous êtes concerné par la loi « Informatique et Libertés » du 6 janvier 1978.

◆ **Les obligations à respecter**

➲ Recueillir le consentement de la personne pour utiliser une information qui l'identifie.

➲ Permettre aux personnes concernées par ces informations d'exercer pleinement leurs droits (accès, rectification, suppression) en leur communiquant l'identité de votre entreprise, la finalité du fichier, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de leurs droits et les transmissions envisagées des données à un tiers.

➲ Ne pas réutiliser ces données de manière incompatible avec la finalité première du fichier (ex : céder des adresses emails à un partenaire sans demander leur avis aux propriétaires de ces adresses).

➲ Ne pas collecter des données sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, données relatives à la vie sexuelle ou à la santé).

➲ Fixer une durée de conservation raisonnable (ou maximale ?) de ces données personnelles.

➲ Protéger et sécuriser l'accès aux fichiers de données personnelles.

En cas de non respect de la loi et de ses obligations, l'entreprise est passible de 5 ans de prison et 300 000 € d'amende (Article 226-16 du Code pénal). La divulgation d'informations par imprudence ou négligence peut être punie de 3 ans de prison et de 100 000 € d'amende.

◆ **Le responsable du traitement de données personnelles**

Afin de se protéger de façon optimale en respectant la loi, il est recommandé de désigner un correspondant Informatique et libertés au sein de l'entreprise. Cette personne, régulièrement avisée des modifications règlementaires, tient un registre exhaustif de l'ensemble des traitements en cours dans l'entreprise.

Ce « correspondant CNIL » est en outre chargé de sensibiliser les salariés pour éviter que l'entreprise ne soit mise en cause civilement ou pénalement du fait d'un comportement inapproprié d'un de ses salariés.

1.2. Le Secret des correspondances

Le courrier électronique est considéré comme de la correspondance privée dont le contenu est, par nature, accessible uniquement à son destinataire. Cependant, les messages électroniques envoyés ou reçus sur l'ordinateur de l'entreprise sont présumés être à caractère professionnel, sauf mention explicite de leur caractère personnel.

Sauf risque ou évènement particulier, les messages personnels ne peuvent être ouverts par l'employeur, si le salarié n'est pas présent ou dûment appelé. Par contre, l'employeur peut rechercher, même à l'insu du salarié et hors sa présence, les connexions à des sites internet étrangers à son travail.

1.3. Autres cas

La responsabilité de l'entreprise peut être engagée dans les cas suivants.

- L'utilisation malveillante des moyens informatiques et de communication électroniques.
- Le téléchargement et la réutilisation de documents non libres de droits.
- La contrefaçon ou utilisation de copies illicites de logiciels ou d'œuvres protégées sans autorisation des titulaires de droits.
- L'usurpation d'identité par un des salariés au préjudice de tiers.

2. Les droits

2.1. Vis-à-vis des actes malveillants

Si votre entreprise est victime de vol ou d'altération de votre système d'information, il existe des recours. Vous pouvez déposer une plainte pénale auprès du commissariat de police ou de la gendarmerie. Les faits y seront précisément exposés, en incluant tout détail utile sur l'origine de l'attaque et les dommages causés.
C'est pourquoi il est primordial de ne pas effacer les traces d'une éventuelle infraction et de conserver les preuves susceptibles d'aider l'action en justice : logs de connexion, copie de disque dur.

Il est également recommandé de faire appel à un huissier de justice spécialisé en fraude informatique pour établir un procès-verbal de constat, puis de décider avec le conseil d'un avocat des actions les plus appropriées.
Vous pouvez aussi informer le CERTA (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques) ou la DCRI (Direction Centrale du Renseignement Intérieur).

2.2. Vis-à-vis des salariés

En complément du contrat de travail et du règlement intérieur, il est fortement conseillé d'élaborer une charte de sécurité informatique afin d'organiser un bon usage du système d'information par tous.
Cette charte fixe à l'ensemble du personnel un cadre général et définit des règles pour l'usage des technologies de l'information et de la communication dans l'entreprise.
Elle permet ainsi de fournir des garanties et de délimiter les responsabilités de chacun.

La charte doit traiter des thématiques suivantes :

- Les règles générales d'utilisation du système d'information.
- Le rappel des principaux textes de loi.
- Les mesures de sécurité des accès aux applications et les conseils de vigilance.
- Les règles d'utilisation de la messagerie, d'Internet, etc.
- Le traitement des infections informatiques (virus…) et le comportement à adopter.
- Les moyens de contrôle mis en œuvre et les sanctions encourues en cas de non respect de la charte.

Généralement rédigé par le responsable informatique en collaboration avec la direction des ressources humaines, ce document doit être diffusé à l'ensemble du personnel dans un but pédagogique et de sensibilisation.

Voici un exemple de charte du CNRS:
http://www.sg.cnrs.fr/FSD/securite-systemes/documentations_pdf/securite_systemes/Charte.pdf

3. Pour aller plus loin

◆ **Droit NTIC**
Ce site propose des informations juridiques et pratiques sur les nouvelles technologies et Internet.
http://www.droit-ntic.com

◆ **CNIL : Commission Nationale de l'Informatique et des Libertés**
Autorité indépendante, créée en 1978, dont la mission est de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à la vie privée, ni aux libertés individuelles publiques ou aux droits de l'homme de manière générale.
http://www.cnil.fr

◆ **Ysosecure**
Ce site permet de comprendre l'intérêt des systèmes de management de la sécurité de l'information, des méthodes de gestion des risques ainsi que les bonnes pratiques pour améliorer la sécurité de l'information de votre entreprise.
http://www.ysosecure.com

Externaliser une partie de son activité sans danger

« Nous avions sous-traité la gestion complète de notre site Internet à notre prestataire. Lorsque celui-ci a déposé le bilan, nous n'avons rien pu récupérer. Nous avons dû refinancer intégralement le développement d'un nouveau site. »

L'externalisation consiste à confier tout ou partie de la gestion d'une activité de l'entreprise à un prestataire externe spécialisé.
Pour des raisons de coûts ou d'absence de compétences internes, nombre de PMI-PME ont recours à cette pratique. L'externalisation peut s'appliquer à plusieurs domaines d'activités (ressources humaines, marketing, administratif, financier…). Lorsqu'une entreprise sous-traite la maintenance de son infrastructure informatique, on parle d'infogérance.
Mais quelque soit l'activité sous-traitée, l'externalisation présente des risques pour le système d'information de l'entreprise car une partie n'est plus sous son contrôle direct. Il est donc nécessaire de rester vigilant quand au choix d'un prestataire et aux termes du contrat avec celui-ci.

Cette fiche vous donne des conseils pratiques pour externaliser tout ou partie de votre activité en sécurisant la relation avec votre prestataire.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

Voici les points clés à retenir :

- Définir les objectifs de l'externalisation et identifier les risques pour l'entreprise.
- Inclure dans le contrat de prestation de services des règles de sécurité à respecter par le prestataire.
- Se renseigner régulièrement sur la santé financière de son prestataire.
- Vérifier fréquemment la prise en compte de la sécurité par son prestataire.

La présente fiche réalisée avec la collaboration de Me Raphaël Peuchot, avocat au Barreau de Lyon.

Sommaire

1- Avantages et inconvénient de l'externalisation

Afin de s'assurer de prendre la décision la plus appropriée, il est important d'évaluer l'ensemble des avantages et inconvénients de l'externalisation d'une activité.

1.1. Avantages de l'externalisation

- Se recentrer sur son cœur de métier et générer plus de valeur ajoutée.
- Bénéficier d'experts qualifiés et de compétences spécifiques à certaines fonctions.
- Améliorer sa compétitivité.
- Etre plus flexible dans la gestion des ressources humaines.
- Réduire les coûts d'exploitation en mutualisant des moyens par l'intermédiaire du prestataire.

1.2. Inconvénients à l'externalisation

- Dépendre du prestataire.
- Perdre le contrôle et une partie des compétences de l'entreprise.
- Rencontrer des difficultés sociales en cas de dégradation des relations entre les partenaires.
- Faire face à des rétentions d'informations de la part du prestataire.
- Avoir des difficultés à réintégrer l'activité externalisée.

Remarque :

Externalisation ≠ sous-traitance
On parle de sous-traitance lorsque le prestataire assurant l'externalisation confie lui-même l'exécution de tout ou partie de sa prestation à un ou plusieurs tiers sous-traitants. Elle implique une chaîne de contrats et requiert une vraie compétence du prestataire principal pour coordonner ses sous-traitants.
Le recours à la sous-traitance peut s'inscrire dans le cadre d'un contrat d'externalisation, mais chaque sous-traitant du prestataire doit être agréé par l'entreprise cliente.

2- Comment choisir le meilleur prestataire ?

En matière d'externalisation, plusieurs critères sont à prendre en considération lors du choix d'un prestataire.

- Ses références (il n'est d'ailleurs pas interdit de prendre contact avec un client actuel ou passé du prestataire).
- Sa santé financière.
- Sa maîtrise du domaine (certification ISO par exemple).
- L'adéquation de sa réponse au cahier des charges eu égard aux exigences de votre entreprise en matière de sécurité.

En tant que client, vous pouvez par ailleurs demander à rencontrer les personnes qui auront accès aux informations de votre entreprise dans le cadre de l'externalisation ou à visiter les locaux dans lesquels seront hébergées vos données.

3 - Le contrat d'externalisation

La formalisation du contrat de prestation de services est une étape indispensable dans un processus d'externalisation. Il doit inclure la description des prestations, les rôles et responsabilités de chacun des partenaires, la durée, la reprise (des données ou du contrat ?), le renouvellement, la cession et le transfert du contrat ou encore les coûts et les différentes clauses essentielles (obligation de livrables, de collaboration, de performance…).

Un plan de réversibilité doit être prévu dans le contrat pour permettre de réintégrer l'activité sous-traitée en cas de détérioration des relations avec le prestataire. Ce chapitre du contrat doit décrire notamment de quelle manière votre entreprise pourra récupérer ses données.

Par ailleurs, il est fortement recommandé d'ajouter en annexe un engagement de confidentialité et d'intégrité des données portant sur la transmission d'informations par votre entreprise.

Voici le plan type d'un contrat de service :

1. Documents contractuels (mentionner la liste de l'ensemble des documents compris dans le contrat).
2. Description précise des prestations.
3. Régime de l'obligation du prestataire (obligation de moyens ou de résultat).
4. Prix des prestations (critère d'évolution des prix).
5. Etablissement du montant des pénalités (en cas de retard ou de non-performance de la part du prestataire).
6. Statut des matériels et des logiciels.
7. Etendue de la responsabilité.
8. Limitation du préjudice réparable.
9. Cession des droits (assurer la propriété des logiciels).
10. Juridiction compétente en cas de litige (désignation géographique).

Source : Guide SSI du MEDEF - Fiche 10 : Externaliser la mise en œuvre et la maintenance des politiques de sécurité, 2005

4- Les facteurs clés de succès d'un projet d'externalisation

- Construction d'un partenariat et d'une relation de confiance avec le prestataire.
- Communication constante.
- Organisation de réunions de suivi au besoin.
- Mise à jour des procédures de travail des salariés en interne.
- Révision du contrat d'externalisation en cas de besoin.
- Synthèse annuelle des actions réalisées.
- Respect de la confidentialité des informations.

5. Pour aller plus loin

◆ **Externaliser.net**
Portail regroupant de l'information sur l'externalisation et l'outsourcing.
www.externaliser.net

Gérer et contrôler les accès aux données de l'entreprise

« Cet employé de bureau a pu copier l'ensemble du fichier client de l'entreprise pour le revendre à un concurrent. Il fut licencié, mais cela n'empêcha pas le préjudice. »

Afin d'éviter les actes malveillants externes et d'éventuelles maladresses en interne, des contrôles d'accès performants aux systèmes informatiques sont essentiels pour assurer une sécurité optimale.
Ces contrôles consistent à surveiller à la fois les accès logiques et physiques[14] aux ressources informatiques de l'entreprise. Il n'est pas nécessaire que tout utilisateur puisse disposer de l'ensemble des ressources disponibles. Des limites doivent donc être définies en adéquation avec le poste de chaque collaborateur.

Cette fiche pratique vous donnera les clés de la mise en place d'un contrôle des accès efficace tant au niveau physique qu'au niveau logique (système informatique).

[14] L'accès physique désigne tout ce qui est physiquement accessible comme un bâtiment, une salle de réunion, un bureau...
L'accès logique désigne tout ce qui est virtuellement accessible comme un site internet, un fichier ou une application informatique.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

Voici les points clés à retenir :

- Sécuriser physiquement les zones sensibles de votre entreprise (portes, fenêtres, clôture).
- Utiliser des mots de passe complexes.
- Gérer l'arrivée et le départ de toute personne ayant accès au système d'information de l'entreprise.

Sommaire

1. Assurer la sécurité physique de votre entreprise

Avant même de s'intéresser au système informatique, la première étape consiste à protéger les locaux de votre entreprise. Pour éviter la circulation de personnes non autorisées dans vos locaux, il est important de disposer d'une part de bâtiments sûrs (clôture du site, fenêtres solides, grillage…) et d'autre part de systèmes de contrôle d'accès, notamment :

- Un portillon avec lecteur de badge à l'entrée permettant de filtrer les entrées et sorties et de tracer les accès aux locaux.

- Une procédure d'identification pour les personnes externes (clients, fournisseurs, prestataires). Dans l'idéal, elle doit être instaurée en tenant un registre précisant la nature et les horaires des visites. Il est par ailleurs fortement recommandé d'accompagner les visiteurs le temps de leur présence dans l'entreprise.

- Un verrouillage systématique des zones sensibles. Elles doivent être équipées de serrures de sûreté et accessibles uniquement aux personnels autorisés.

Enfin, pour un maximum de prévention, vous pouvez installer un système d'alarme, de vidéo surveillance, de lecture d'empreintes digitales ou encore engager des agents de sécurité.

2. Gérer les contrôles d'accès aux ressources informationnelles

Cette gestion implique deux types de contrôle :

- Vérifier que seul le personnel de l'entreprise peut accéder aux ressources internes.
- Vérifier que seuls les salariés autorisés accèdent aux informations sensibles de l'entreprise.

2.1. L'authentification des utilisateurs

Les contrôles d'accès passent par un protocole d'authentification qui garantit au système informatique l'identité de l'utilisateur.

Le système le plus répandu demeure le contrôle d'accès par mot de passe mais d'autres types d'authentification existent comme la lecture d'empreinte digitale (sur un ordinateur portable par exemple) ou l'utilisation d'un certificat électronique[15].
L'accès à des données est d'autant plus sécurisé que plusieurs systèmes d'authentification sont associés.

◆ Le contrôle d'accès par mot de passe

Il consiste à configurer les postes informatiques des utilisateurs (verrouillage par mot de passe) et à installer un serveur d'authentification. Cette manipulation doit être effectuée par un spécialiste.

Il s'agit ensuite d'attribuer à chaque utilisateur un compte comportant un identifiant fourni par le responsable informatique et un mot de passe personnel. Lors du processus d'authentification, l'utilisateur saisit le couple identifiant / mot de passe et le serveur d'authentification vérifie s'il est identique à celui enregistré dans sa base de données sécurisée.

◆ Etablir un mot de passe sécurisé

Les pirates informatiques disposent de logiciels très performants capables de tester très rapidement une série de combinaisons de caractères. Un mot de passe fiable est un mot de passe complexe.

Voici quelques recommandations pour établir un mot de passe sécurisé:

- Il doit être composé d'au moins 8 caractères combinant chiffres, lettres, minuscules, majuscules et caractères spéciaux. Au besoin, des systèmes permettent de contraindre l'utilisateur à intégrer ces règles.

- Il doit être facile à retenir en utilisant des moyens mnémotechniques tels que la méthode des premières lettres (qui consiste à prendre la première lettre de chaque mot d'une expression) ou la méthode phonétique (phrase codée phonétiquement : ght1CDà15€, j'ai acheté un CD à 15 euros). En cas d'oubli du mot de passe, il est possible d'en simplifier la réinitialisation en désignant un interlocuteur dédié et facilement joignable.

- Il ne doit pas s'agir d'un mot présent dans le dictionnaire.

[15] Pour en savoir plus sur le certificat électronique, se référer à la fiche 2 « Quels outils utiliser pour une protection minimum du SI ? »

- Il faut le renouveler périodiquement (au moins tous les ans et plus si il donne accès à des données sensibles). Cela implique la mise en place d'une procédure donnant une durée de validité maximale au mot de passe.

- Le mot de passe ne doit pas être en lien avec une information personnelle (date de naissance, nom…).

- Il ne doit être écrit nulle part (Attention au post-it sur l'écran d'ordinateur ou sous le clavier).

Il est nécessaire de sensibiliser l'ensemble du personnel à ces usages. Des sanctions peuvent être appliquées par l'entreprise en cas de non respect des règles par les utilisateurs.

2.2. La gestion des droits d'accès des utilisateurs

Il s'agit de déterminer de quelles informations chaque utilisateur doit disposer et ce qu'il peut en faire.
Pour simplifier la tâche d'administration des utilisateurs et de leurs droits d'accès, des profils peuvent être créés sur le serveur d'authentification. Un profil est un ensemble de règles d'accès aux ressources informatiques qui sont attribuées à un ensemble d'utilisateurs ayant un besoin d'accès aux mêmes ressources ou un rôle et des responsabilités similaires.
Le profil de l'utilisateur lui donnera des droits différents selon les informations : lecture seule, modification ou suppression.

Par ailleurs, le fait d'utiliser un système central d'authentification permet de tracer les actions des utilisateurs (heure de connexion, suivi des fichiers).

3. Gérer les mouvements de personnel

3.1. Gestion des comptes du personnel

On se méfie plus facilement d'une personne externe que d'un collaborateur qui quitte l'entreprise. Il n'est pourtant pas rare que ce dernier ait pris soin de copier des informations importantes avant son départ.

Idéalement, chaque entreprise devrait disposer d'une procédure d'entrée et de sortie pour gérer en temps réel la création et la suppression des comptes utilisateurs. L'administrateur système devrait être informé immédiatement de l'arrivée ou du départ définitif d'un salarié.

En l'absence de procédures, il convient de vérifier régulièrement que tous les comptes ouverts sont encore d'actualité et de fermer ceux qui sont inutilisés.

3.2. Gestion des comptes des stagiaires

Le cas du stagiaire est souvent traité avec moins d'attention que celui du salarié. A son arrivée, son compte est créé rapidement sans exclure les informations auxquelles il ne doit pas accéder et lorsqu'il part, son compte n'est pas automatiquement supprimé.

Voici quelques recommandations :

◆ **Avant le stage**

- Examiner en détail le Curriculum Vitae et recueillir toute information utile sur le candidat (stage précédent chez un concurrent).
- Définir les missions de stage et faire signer une clause de confidentialité si nécessaire.
- Refuser explicitement la diffusion sur Internet du futur rapport de stage.
- Désigner un tuteur.

◆ **Pendant le stage**

- Veiller au respect des horaires du stagiaire et des lieux auxquels il aura accès.
- Déterminer un accès restreint aux ressources de l'entreprise et surveiller, en cas de doute, son activité sur le réseau informatique et son utilisation de la photocopieuse.
- Répondre aux questions du stagiaire uniquement si cela correspond à son domaine de compétences. Ainsi, un stagiaire en marketing n'a pas à connaitre toutes la procédure de sauvegarde de l'entreprise.

➲ Proscrire l'utilisation de son matériel personnel (clé USB, ordinateur portable).

◆ **Après le stage**

➲ Vérifier de manière approfondie l'ensemble des travaux du stagiaire pour filtrer les données jugées stratégiques.

➲ Supprimer ses droits d'accès et récupérer son badge et ses clés.

4. Pour aller plus loin

◆ **Guide des bonnes pratiques en matière d'intelligence économique**
MINEFE**,** Février 2009.
http://www.entreprises.gouv.fr/document/Guide_des_bonnes_pratiques_en_matiere_d_IE.pdf

◆ **Cases Luxembourg : Portail de la sécurité de l'information**
Ce site a pour objectif de développer un réseau opérant dans le domaine de la prévention et de la protection des systèmes d'information et de la communication. Il veille à la promotion des outils de protection informatique.
http://www.cases.public.lu

◆ **Portail de la sécurité informatique (SGDN)**
http://www.securite-informatique.gouv.fr.
Rubrique « Autoformation » puis « Mot de passe ».

◆ **Guide de sensibilisation à la sécurisation du système d'information et du patrimoine informationnel de l'entreprise.**
MEDEF
http://www.cyber.ccip.fr/pdf/medefsecusi.pdf

Prendre en compte et maîtriser le facteur humain dans la SSI

« Pour plus de sécurité, nous avions choisi de changer le mot de passe des utilisateurs tous les 6 mois. Mais cela n'a pas duré longtemps car les collaborateurs écrivaient leur code sur un papier qu'ils cachaient dans leur tiroir ou sous leur clavier. Finalement cette mesure a créé des risques supplémentaires au lieu de mieux protéger notre système d'information. »

Même avec les meilleurs outils existants en matière de sécurité informatique, le système d'information d'une entreprise peut devenir perméable si l'entreprise ne maîtrise pas le facteur humain.
En effet, le personnel fait partie intégrante du SI. Il en est même un maillon essentiel. Chaque salarié ayant accès à tout ou partie du patrimoine informationnel, il est important qu'il ait conscience de la sensibilité et de la vulnérabilité des informations et qu'il respecte quotidiennement les règles internes de sécurité.

Cette fiche pratique vous explique comment sensibiliser le personnel à la sécurité informatique et pourquoi nommer un responsable dans ce domaine.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

Voici les points clés à retenir :

- Intégrer la protection de l'information dans la communication globale de l'entreprise.
- Sensibiliser, former, impliquer et responsabiliser le personnel à tous les niveaux.
- Communiquer sur la stratégie et les actions prévues en matière de sécurité, en insistant largement sur les bénéfices d'une telle démarche afin d'éviter les potentielles résistances aux changements.
- Assurer le responsable sécurité du soutien indispensable de la hiérarchie.
- Eviter que l'entreprise attende les problèmes pour agir, il est souvent déjà trop tard.
- Mettre en place des solutions réalistes et adaptées en fonction des risques encourus par l'entreprise.

Sommaire

1. Nommer un responsable « Sécurité du système d'information »

Le responsable SSI a pour mission de garantir l'intégrité, la confidentialité, la disponibilité et la traçabilité des données de l'ensemble des systèmes d'information de l'entreprise. Il définit les orientations, élabore et met en œuvre une politique de sécurité.
Il est aussi celui sur qui repose la maîtrise du facteur humain dans la sécurité du système d'information.

Il n'existe pas de profil type. Le responsable SSI doit réunir plusieurs compétences :

- Une bonne connaissance dans le domaine de la sécurité, sans pour autant connaître en détail le fonctionnement des technologies. Il doit acquérir et mettre à jour un minimum de connaissances à la fois pour être crédible vis-à-vis des techniciens en sécurité informatique et pour savoir apprécier les risques liés à l´utilisation du système d´information.

- Une vision transversale de l'activité de l'entreprise.

- Des aptitudes en communication pour mener des missions de sensibilisation.

- Des aptitudes en organisation car il sera le chef d'orchestre de la gestion d'éventuels sinistres.

Dans les PMI PME, cette fonction est très souvent assurée par le responsable informatique lui-même ou encore le responsable qualité.

2. Sensibiliser et former le personnel à la SSI

2.1. Comment ?

Il s'agit de mener régulièrement des actions d'information et de sensibilisation auprès du personnel pour lui faire comprendre les enjeux de la SSI. Ces actions facilitent l'acceptation et l'application de règles qui peuvent parfois paraître contraignantes.

L'objectif est de transmettre un premier niveau de connaissance et de diffuser les bonnes pratiques concernant la sécurité informatique.

Tout utilisateur doit :

- Avoir eu connaissance de la charte informatique et l'appliquer.
- Connaître la démarche à suivre en cas de problème de sécurité informatique (personne à contacter).
- Etre en mesure de juger de la sensibilité d'une information.
- Connaître son périmètre d'accès à l'information.

Les actions de sensibilisation peuvent se faire à travers :

- Des discussions informelles entre employés et responsables SSI.
- Des notes d'information (emails courts et pratiques).
- De l'affichage dans les zones sensibles (photocopieurs, bureau de recherche et développement).

➲ Des réunions thématiques régulières.
➲ Des séances de formation.

2.2. Les facteurs clés de succès

Les supports utilisés dans le cadre d'actions de sensibilisation à la SSI doivent être simples, ludiques et interactifs afin d'assurer l'efficacité des messages et de susciter l'intérêt du plus grand nombre.

L'introduction de nouvelles pratiques peut générer certaines résistances aux changements. Il est alors conseillé d'axer le discours de sensibilisation sur les avantages qu'apporte la SSI pour garantir l'activité de l'entreprise.

Par ailleurs, il convient de contrôler régulièrement le respect par le personnel des règles et sa connaissance des dispositions pratiques inscrites dans le règlement intérieur. Des mesures incitatives peuvent aussi être envisagées.Généralement, les actions de sensibilisation se font en complément d'une démarche de diffusion de la charte informatique interne[16].

Enfin, les règles seront d'autant plus prises au sérieux si les responsables les respectent eux-mêmes de manière exemplaire.

[16] Pour en savoir plus sur la charte informatique, se référer à la fiche n°6 « Les droits et obligations du chef d'entreprise en matière de SSI ».

L'usage des réseaux sociaux dans l'entreprise

« Un de nos anciens stagiaires cherchait du travail. Souhaitant se valoriser sur un réseau social, il a dévoilé notre plan marketing sur lequel il avait travaillé. »

Les réseaux sociaux (ou social networking) sont des sites communautaires d'échange et de partage entre des individus. Ils permettent essentiellement de mettre en relation des personnes partageant les mêmes centres d'intérêt personnels ou professionnels.
Parmi les réseaux sociaux les plus connus à destination des professionnels, Viadeo (Europe) et LinkedIn (international) sont les plus connus. Facebook et MySpace sont plutôt des plateformes d'échanges grand public même si elles sont aussi utilisées par des professionnels pour y faire du marketing communautaire (community management).

Le principe de fonctionnement d'un réseau social est simple. Il suffit de se créer un profil utilisateur et de suivre l'actualité des membres. Le contenu étant intégralement produit par l'internaute, chacun est responsable des informations qu'il publie.
Ce phénomène est encore mal compris pour la majorité des entreprises et donc peu contrôlé. Or, les réseaux sociaux représentent un risque de fuite d'informations stratégiques et de perte de réputation pour l'entreprise.

Cette fiche pratique vous informe sur les risques liés à l'usage des réseaux sociaux par les salariés.

Voici les points clés à retenir :

- Etre vigilant et curieux : surveiller en permanence ce qui se dit sur vous et votre entreprise sur Internet.
- Etre un membre impliqué et avoir une démarche active au sein du réseau social.
- Former et sensibiliser le personnel à une utilisation sécurisée des réseaux sociaux.

Avertissement : cette fiche est le fruit d'un travail de vulgarisation et comporte par conséquent une information générale et non exhaustive. Elle ne saurait engager la responsabilité de l'éditeur (Direccte, ENE) et de ses diffuseurs.

Sommaire

1. Les risques liés aux réseaux sociaux pour l'entreprise

De nombreux problèmes peuvent survenir en cas d'utilisation non maitrisée des plateformes sociales.

En voici quelques exemples :

- L'usurpation par une personne malveillante de l'identité d'un utilisateur de réseaux sociaux délivrant un nombre important d'informations dans son profil. Donner des informations personnelles peut notamment fournir une indication permettant de deviner un mot de passe.

- La divulgation sur un réseau social par un salarié d'informations stratégiques.

- Le dénigrement de l'entreprise par un salarié mécontent ce qui représente donc une perte de réputation pour la société.

- L'infection du système d'information par un virus via l'installation d'applications tierces[17] sur un ordinateur de l'entreprise.

C'est pourquoi il est indispensable de maîtriser la diffusion de l'information et, de ce fait, de ne jamais communiquer des données à caractère stratégique ou trop personnelles sur les réseaux sociaux.

2. Comment bien utiliser les réseaux sociaux ?

- Lire attentivement la charte d'utilisation et de confidentialité des réseaux sociaux avant toute inscription.

- Utiliser les paramètres de confidentialité de manière à ne pas se faire indexer par les moteurs de recherche (option demandée à l'inscription sur le réseau social).

- Ne pas publier d'informations confidentielles ou de données jugées sensibles pour l'entreprise.

- Demander aux salariés d'utiliser un mot de passe différent pour accéder au réseau social et aux applications de l'entreprise.

- Définir une ligne de conduite conforme aux principes et à l'éthique de l'entreprise afin de sensibiliser les employés aux risques éventuels liés à l'utilisation des réseaux sociaux.

- Réagir rapidement en cas de découverte de propos malveillants ou diffamatoires sur des plateformes sociales. Cela peut se faire aisément en contactant la direction ou l'hébergeur du site concerné.

3. Comment surveiller sa réputation sur Internet ?

Pour parfaire ces mesures de sécurité, il est recommandé d'effectuer une veille régulière sur ce qui se dit de votre entreprise sur Internet.

Plusieurs outils peuvent vous aider :

◆ **Google alertes : http://www.google.fr/alerts**

Cet outil gratuit de surveillance permet d'être alerté très simplement lors de la diffusion de certaines informations. Pour accéder au service, il suffit de s'inscrire avec son e-mail et de saisir les termes recherchés comme on le ferait sur Google.

Par exemple, vous pouvez surveiller le nom de votre entreprise ou les commentaires faits sur vos produits. Vous pouvez ensuite choisir la fréquence d'envoi des alertes. Toutefois, le système de filtrage n'est pas toujours très pertinent et génère parfois trop d'informations. Vous serez averti des alertes par email.

◆ **Spyple : http://www.spyple.com**

Ce tout nouveau moteur de recherche 2.0 vous permet d'évaluer la présence d'une marque ou d'une personne sur certains réseaux sociaux.

[17] Exemples d'applications : Superwall, Topfriends sur le réseau Facebook.

Enfin, pour rechercher des informations sur des personnes par type de sources (blogs, réseaux sociaux…), vous pouvez utiliser les moteurs de recherche 123 people, pipl ou encore addict-o-matic[18].

4. Pour aller plus loin

◆ **Article « Quelle place pour les réseaux sociaux en entreprise ? »**
Indexel.net - Novembre 2008.
http://www.indexel.net

◆ **L'impact des réseaux sociaux**
Livre blanc de Jérôme Bondu et Alain Garnier – Février 2009

◆ **Place des réseaux**
Webmagazine des entrepreneurs en réseaux
http://www.placedesreseaux.com

[18] http://www.123people.fr, http://pipl.com et http://addictomatic.

Janvier 2010

Pour toute question, contactez l'ENE.

Contacts

Vous avez un projet autour de la sécurité des systèmes d'information ? Votre entreprise est victime d'un sinistre ou d'une attaque informatique ?

Quatre centres d'expertise TIC sont à votre service en Rhône-Alpes :

➲Ardèche

Cybardèche
4 avenue de l'Europe Unie
BP 114
07001 PRIVAS CEDEX

[tél.] 04 75 20 28 57
[fax] 01 56 72 94 57
[mail] contact@cybardeche.fr

➲Rhône - Loire - Ain

Espace Numérique Entreprises
Villa Créatis
2, rue des Mûriers - CP 601
69258 LYON CEDEX 09

[tél.] 04 37 64 46 10
[fax] 04 78 83 99 60
[mail] renseignements@ene.fr

➲Isère

Espace Numérique Nord-Isère
5 rue Condorcet
BP 108
38093 VILLEFONTAINE CEDEX

[tél.] 04 74 95 98 32
[fax] 09 72 11 32 32
[mail] info@enni.fr

➲Drôme

Pôle Numérique
Le Rhovalparc - BP 15155
1 avenue de la Gare
26958 VALENCE CEDEX 9

[tél.] 04 75 83 50 58
[fax] 04 75 82 96 31
[mail] entreprise@pole-numerique.fr

Espace Numérique Entreprises

Direccte Rhône Alpes

Direction Régionale de l'Entreprise, de la Concurrence, de la Communication, du Travail et de l'Emploi

Espace Numérique Entreprises

Villa Créatis - 2, rue des Mûriers
CP 601 - 69258 LYON CEDEX 09
[tél.] 04 37 64 46 10
[fax] 04 78 83 99 60

DIRECCTE Rhône-Alpes

Tour Suisse - 1 Bd Vivier Merle
69443 Lyon Cedex 03
[tél.] 04 72 68 29 00
[fax] 04 72 68 29 29

Conception : Espace Numériue Entreprises - Photos : Fotolia