

**GROUPE Y**  
■ **CABINETS PARTENAIRES**



## *Les Cahiers Thématiques*

# **SECURITE INFORMATIQUE**

**Un enjeu devenu vital  
Pour votre entreprise**

*Avec le concours de :  
La Direction Générale de la Gendarmerie  
Et du Ministère de l'Economie et des Finances*



## Sommaire

Présentation générale.....	page 3
<b><u>I. Protéger le patrimoine de l'entreprise</u></b> .....	page 4
I.1 Les ressources stratégiques.....	page 4
I.2 Les moyens de production .....	page 4
I.3 Et la loi dans tout cela ?.....	page 5
<b><u>II. Se protéger : quelques règles de base, un zeste de bon sens</u></b> .....	page 8
II.1 L'organisation, le fondement de tout .....	page 8
II.2 La technique, le passage obligé .....	page 11
II.3 L'humain, le maillon faible .....	page 13
<b><u>III. Que faire lorsqu'il est (presque) trop tard</u></b> .....	page 13
III.1 Méthodologie à appliquer .....	page 13
III.2 Les organismes d'Etat et leurs compétences.....	page 14
<b><u>IV. Evaluer ma sécurité en 10 questions</u></b> .....	page 18
IV.1 Organisationnel.....	page 18
IV.2 Technique.....	page 19
IV.3 Humain.....	page 19
<b><u>Annexes</u></b>	
Le CLUSIF.....	page 21
Le CLUSIR Poitou-Charentes.....	page 22

## ■ Présentation générale

Les ordinateurs, et bientôt de nombreux objets de notre vie quotidienne, ne s'envisagent plus sans des capacités de communication. Au sein même des entreprises, l'informatique en réseau, ouverte vers l'extérieur, s'est démocratisée rapidement.

On retrouve à la base de toutes ces évolutions, le phénomène Internet. Ce concept, et les protocoles qui lui sont associés, bien qu'inventés pour satisfaire à des besoins de l'armée américaine, présentent de nombreuses lacunes en matière de sécurité.

Les entreprises, de plus en plus multinationales, délocalisées, éclatées, misent sur leur Système d'Information pour maintenir une cohésion efficace et fluidifier leurs échanges internes et externes.

On voit ainsi apparaître des grands projets de réseau intranet, extranet au niveau mondial.

Le « zéro papier » est de rigueur et toute la substance de l'entreprise réside dans les hommes et dans le **Système d'Information** qui **constituent donc la moelle épinière de cet ensemble.**

De nombreuses entreprises ont d'ores et déjà compris l'importance de ces enjeux et définissent une **politique de sécurité** qui est déterminée au niveau mondial pour ensuite être appliquée dans toutes les filiales.

Ces règles ont souvent pour objet de réglementer non seulement la conception des Systèmes d'Information, mais surtout les comportements des utilisateurs. On remarquera, dans un contexte de guerre économique, leur origine militaire.

Dès lors, la sécurité revêt une importance qui grandit avec le développement des réseaux Internet.

La complexité des technologies utilisées, la croissance exponentielle des terminaux à protéger ainsi que la prolifération de nouvelles menaces (virus, mais aussi outils de «hacking» faciles d'accès) démontrent que la sécurité est, et sera plus encore demain, un **enjeu stratégique majeur.**

De plus, elle concernera toutes les entreprises quelle que soit leur taille.

# I. Protéger le patrimoine de l'entreprise

## I. Protéger le patrimoine de l'entreprise

Toute société dispose d'un patrimoine d'informations très important.

Au delà de la simple protection contre les vols de matériels, et d'arrêt des serveurs dû à des virus ou autres logiciels malveillants, il devient critique pour l'entreprise d'aborder la sécurité sur l'aspect global et stratégique.

### *I.1 Les ressources stratégiques*

Toute entreprise dispose aujourd'hui d'une multitude de ressources lui permettant de produire.

Ces ressources sont aussi bien des **ressources matérielles** :

- Machines industrielles
- Serveurs Informatiques
- Poste informatique des commerciaux
- Matières premières

Que des **ressources immatérielles** :

- Bases tarifaires
- Fichiers des clients

- Flux de données
- Brevets sur des procédés de fabrication

Si la concurrence, qu'elle soit locale, nationale ou internationale, venait à obtenir tout ou partie de ces ressources, la vie de l'entreprise se verrait sûrement mise en péril.

### *I.2 Les moyens de production*

Les moyens de production, qu'ils soient des serveurs informatiques, des logiciels ou des machines industrielles, sont tous dépendants d'éléments qui sont amenés régulièrement à subir des incidents.

Lorsqu'un moyen de production s'arrête, il devient critique qu'une solution rapide soit trouvée (exemple : reprise après un arrêt électrique).

Il est donc nécessaire de **bâtir un plan de secours et de reprise** permettant de répondre à toutes les demandes d'arrêt inopinées ou de disparition des moyens de production.

## I. Protéger le patrimoine de l'entreprise

### *1.3 Et la loi dans tout cela ?*

A différentes périodes, différentes lois. Aujourd'hui, toutes les contraintes réglementaires ou législatives sont importantes et doivent être intégrées dans la réflexion des Systèmes d'Information.

**En 2004, 2005 et 2006** ont été votées différentes lois autour des problèmes liés aux Systèmes d'Information.

La mise en place de ces lois au sein d'une entreprise est importante et nécessite une étude approfondie des obligations :

#### **Obligation de traçabilité**

Toute personne morale mettant en œuvre un moyen d'accès à Internet et agissant donc en ce sens en Fournisseur d'Accès à l'Internet, doit pouvoir fournir une identification des personnes connectées aux autorités compétentes.

#### **Obligation de transparence**

Toute personne morale mettant en œuvre un moyen de stockage, de présentation de données sur Internet

et agissant donc en ce sens en Hébergeur de contenu, doit pouvoir sur demande motivée, « débrancher » le site de contenu et fournir les informations nécessaires à l'identification du propriétaire aux autorités compétentes.

#### **Obligation de vie privée**

Toute entreprise mettant en place des moyens de traçabilité des échanges en interne, doit informer et permettre à chaque salarié de disposer d'un espace « privatif ».

#### **Obligation de sécurité**

Toute entreprise stockant des données de personnes physiques ou morales se doit de mettre en œuvre des mécanismes de protection permettant d'en assurer la confidentialité.

#### **Obligation d'intégrité et de probité**

Toute entreprise disposant de moyens de comptabilité informatisés, se doit de pouvoir fournir l'ensemble des éléments de sa comptabilité à la Direction Générale des Impôts en format « compatible » et assurer l'intégrité des données saisies ainsi que leur disponibilité.

## I. Protéger le patrimoine de l'entreprise

Toute entreprise qui manipule des données et effectue des traitements sur celles-ci doit prendre en compte la loi Informatique et Libertés de 1978. Cette loi a créé la Commission Nationale Informatique et Liberté (CNIL).

### Les Missions de la CNIL

#### Informer

La CNIL informe les personnes de leurs droits et obligations et propose au gouvernement les mesures législatives ou réglementaires de nature à adapter la protection des libertés et de la vie privée à l'évolution des techniques.

L'avis de la CNIL doit d'ailleurs être sollicité avant toute transmission au Parlement d'un projet de loi créant un traitement automatisé de données nominatives.

#### Garantir le droit d'accès

La CNIL veille à ce que les modalités de mise en œuvre du droit d'accès aux données contenues dans les traitements n'entraient pas le

libre exercice de ce droit. Elle exerce, pour le compte des citoyens qui le souhaitent, l'accès aux fichiers intéressant la sûreté de l'État, la défense et la sécurité publique, notamment ceux des Renseignements Généraux.

#### Recenser les fichiers

Les traitements de données à "risques" sont soumis à autorisation de la CNIL.

Elle donne un avis sur les traitements publics utilisant le numéro national d'identification des personnes.

Elle reçoit les déclarations des autres traitements.

Le non-respect de ces formalités par les responsables de fichiers est passible de sanctions administratives ou pénales.

La CNIL tient à la disposition du public le "fichier des fichiers", c'est-à-dire la liste des traitements déclarés et leurs principales caractéristiques.

## I. Protéger le patrimoine de l'entreprise

### **Contrôler**

La CNIL vérifie que la loi est respectée en contrôlant les applications informatiques.

La Commission use de ses pouvoirs de vérification et d'investigation pour instruire les plaintes, pour disposer d'une meilleure connaissance de certains fichiers, pour mieux apprécier les conséquences du recours à l'informatique dans certains secteurs, pour assurer un suivi de ses délibérations.

La CNIL surveille, par ailleurs, la sécurité des Systèmes d'Information en s'assurant que toutes les précautions sont prises pour empêcher que les données ne soient déformées ou communiquées à des personnes non-autorisées.

### **Sanctionner**

La CNIL peut prononcer diverses sanctions graduées : avertissement, mise en demeure, sanctions pécuniaires pouvant atteindre 300.000 €, injonction de cesser le traitement.

Enfin, le Président peut demander par référé à la juridiction compétente d'ordonner toute mesure de sécurité nécessaire. Il peut, au nom de la Commission, dénoncer au Procureur de la République les violations de la loi.

### **Réglementer**

La CNIL établit des normes simplifiées, afin que les traitements les plus courants et les moins dangereux pour les libertés fassent l'objet de formalités allégées.

Elle peut aussi décider de dispenser de toute déclaration des catégories de traitement sans risque.

## ■ II. Se protéger : quelques règles de base

### II. Se protéger : quelques règles de base, un zeste de bon sens

La protection du patrimoine de l'entreprise n'est pas uniquement l'affaire du dirigeant, ou du responsable informatique, chaque salarié doit être aujourd'hui acteur de la sécurité de l'information.

Pour cela, les acteurs chargés de la protection de l'entreprise doivent mettre en œuvre quelques règles simples, tout en gardant à l'esprit :

- **qu'il y a toujours une faille dans un système de protection, il faut juste faire en sorte que cette faille ait l'impact le plus faible possible sur l'écosystème de l'entreprise,**
- **qu'un système de protection n'est efficace que s'il est régulièrement testé,**
- **qu'un système de protection ne doit pas coûter plus cher que le risque maximal couvert.**

### *II.1 L'organisation, le fondement de tout*

Il n'y a pas de socle plus important que de mettre en place l'ensemble de l'organisation relative à la sécurité pour permettre au dirigeant :

- d'assurer que l'ensemble de l'entreprise prenne en compte la dimension sécurité,
- d'identifier ses risques,
- de mettre en place des moyens de réduction de ces risques,
- de disposer d'indicateurs de suivi.

### **A -Prendre en compte la dimension sécurité**

Cela passe par la mise en place d'une organisation de la sécurité et par la nomination d'un Responsable de la Sécurité des Systèmes d'Information.

Cette personne sera le garant de la bonne protection des Informations Stratégiques et devra dépendre directement de la Direction Générale.

## II. Se protéger : quelques règles de base

Il est important que cette personne dispose d'une vision stratégique sur l'entreprise pour lui permettre d'assurer la prise de bonne décision autour des moyens de protection à déployer en fonction de l'analyse des risques menés.

### B – Identifier ses risques

Cette opération consiste à définir quels sont les actifs matériels et immatériels à protéger : serveurs informatiques, procédés de fabrication, locaux, matières premières, ....

Ensuite, commence l'identification des scénarios de risques pouvant s'appliquer à chacun des actifs, en prenant en compte :

- l'impact : est-ce que, si le scénario venait à se produire, l'entreprise subirait un sinistre (aucun, mineur, moyen, majeur).
- la probabilité de survenance : quelles sont les chances de déclenchement du scénario.

En fonction de ces éléments, il est possible de dresser **un tableau récapitulatif des risques** s'appliquant à un ou des actifs.

Actif(s)	Serveurs Internet, fichier clients, fichier des commandes
Scénario	Intrusion dans le système Informatique depuis Internet
Risque	Perte du fichier client, vol des numéros de cartes bancaires
Impact	Majeur
Probabilité	Faible à moyenne
Impact financier	Incalculable.

## II. Se protéger : quelques règles de base

Ensuite, un tableau composé des impacts et des probabilités de réalisation des différents scénarios permet de définir les zones à risques :

Impact Majeur	Risque Faible	Risque moyen	Risque fort	Risque fort
Impact Moyen	Risque Faible	Risque moyen	Risque moyen	Risque fort
Impact Faible	Risque nul	Risque Faible	Risque Faible	Risque moyen
Impact nul	Risque nul	Risque nul	Risque nul	Risque Faible
	Probabilité nulle	Probabilité Faible	Probabilité Moyenne	Probabilité Forte

La probabilité de survenance du scénario est alors fonction des différents éléments techniques ou non techniques.

Il devient alors nécessaire de définir quels risques l'entreprise souhaite couvrir.

### C – Réduire ses risques

Une fois les risques à couvrir identifiés, ces derniers pourront alors chacun faire l'objet de divers traitements :

- Réduire le risque grâce à des

moyens de protection adéquats en fonction des critères financiers et de la probabilité de survenance.

- Transférer le risque sur un tiers, une assurance, un prestataire extérieur, ....
- Accepter le risque.

### D – Suivre le niveau de protection

Après la réduction des risques, il est nécessaire de mettre en place des indicateurs de suivi de ces mécanismes. En effet, ces indicateurs seront les seules solutions permettant de suivre les mesures choisies.

## II. Se protéger : quelques règles de base

C'est le bon moment pour effectuer les revues de sécurité tels les tests d'intrusion et les audits de sécurité.

Grâce à ces référentiels (ISO 27000, PCI-DSS, ....), il est alors possible de maintenir des indicateurs de sécurité et de comparer les résultats tout au long du cycle de vie du moyen de protection.

### *II.2 La technique : le passage obligé*

Tout moyen de protection passe forcément par un ensemble de mesures de sécurité techniques. Ces mesures sont différentes suivant les ressources à protéger.

On peut classer rapidement l'ensemble de ces mesures ou moyens suivants trois thèmes principaux :

- La protection de l'environnement physique : locaux, salles informatiques, ...
- La protection des ressources informatiques : serveurs, postes de travail, ...

- La protection des moyens de télécommunication ; téléphonie, accès Internet, serveurs de commerce électronique, ...

### **A –La protection physique et environnementale**

Le premier moyen de protection consiste à mettre en place des contrôles d'accès aux locaux, qu'ils soient sensibles ou non.

Chacune des personnes accédant aux locaux de l'entreprise doit pouvoir être identifiée clairement et des niveaux d'habilitation aux différentes zones de l'entreprise leur être affectés.

Les locaux, informatiques ou non, doivent être équipés de matériels adéquats pouvant couvrir les risques d'incendie, de catastrophe naturelle de tout type (pluie, neige, tremblement de terre, ...).

Les postes de travail ne doivent pas permettre de « lire » le contenu d'un écran de manière simple (à la jumelle par exemple...).

## II. Se protéger : quelques règles de base

### B –La protection logique

Les Systèmes d'Information sont aujourd'hui au cœur des entreprises et nécessitent une protection particulière :

- mettre en place des contrôles d'accès et des habilitations pour chaque serveur, chaque application, chaque base de données, chaque fichier,
- tracer l'activité du système sur les accès logiques,
- déployer des outils techniques, tel : anti-virus, firewall, sonde de détection d'intrusion, ...
- sécuriser les données ; mettre en place les sauvegardes **et les restaurations, ...**

### C –La protection des moyens de télécommunication

L'entreprise qui ne communique pas n'est pas aujourd'hui une entreprise concurrentielle.

Les moyens de communication sont vastes et correspondent à tous les métiers de l'entreprise :

- le standard téléphonique : c'est le premier moyen de prise de contact avec le monde extérieur. Mais c'est aussi le premier moyen

permettant de se renseigner sur l'entreprise.

- le site internet : c'est par lui aujourd'hui que se passe toute la partie communication institutionnelle. Il dispose donc d'informations potentiellement intéressantes pour une personne malveillante.
- les connexions vers les partenaires/fournisseurs : c'est un bon moyen aujourd'hui de s'échanger des flux d'informations tout comme des commandes.

Ces différents moyens de communication nécessitent tous un moyen particulier de protection :

- le téléphone : mettre en place des identifiants d'appels.
- le site internet : mettre en place des éléments tels que des Firewalls, des moyens de vérification des fichiers disponibles sur le serveur et effectuer des tests d'intrusion et des audits.
- les connexions vers les partenaires : effectuer une ségrégation des flux, vérifier la transmission pour ne pas accepter n'importe quel flux.

## III. Que faire lorsqu'il est (presque) trop tard

### *II.3 L'humain : le maillon faible*

En dernier lieu, l'Homme sera toujours derrière les actions de production. Il devient donc critique de « sécuriser » l'élément humain :

- Pour cela, des séances régulières de sensibilisation à la sécurité de l'information sont nécessaires.
- Des mesures plus juridiques telles que des chartes informatiques et des clauses de confidentialité contractuelles sont impératives.

### III. Que faire lorsqu'il est (presque) trop tard

Les risques ont été identifiés, les moyens de protection sont en place, néanmoins, la sécurité n'étant pas une science à 100%, il arrive que des incidents de sécurité surviennent.

#### *III.1 Méthodologie à appliquer*

Il devient alors important de savoir comment réagir face à cette situation particulière.

##### Première étape :

évaluer les dégâts causés, prendre des mesures simples de bon sens permettant de circonscrire le sinistre et mettre en place une cellule de crise spécifique.

##### Deuxième étape :

s'assurer de disposer d'un moyen de remise en état des éléments impactés ; principalement des sauvegardes de données, ou du matériel de secours.

## III. Que faire lorsqu'il est (presque) trop tard

### Troisième étape :

s'adjoindre les compétences d'une personne spécialisée en sécurité pour pouvoir récolter suffisamment d'informations permettant de mettre en exergue les moyens de protection défaillants et de proposer des mesures correctives.

### Quatrième étape :

suivant le type de sinistre, différentes solutions sont possibles :

- Dans le cas d'un arrêt de la production ; faire en sorte de vérifier les causes de l'arrêt et remettre en état le Système de production. Que cela passe par un système de secours ou la remise en place des sauvegardes antérieures au sinistre.
- Dans le cas d'un vol/perte d'informations ; vérifier que l'on dispose bien des sauvegardes de données.
- Dans le cas d'une dégradation des équipements de production ; s'assurer de disposer des bonnes sauvegardes de fichier, d'avoir identifié le problème avant de remettre dans l'état précédent.

### Cinquième étape :

se retourner vers les autorités compétentes permettant de porter plainte.

## *III.2 Les organismes d'Etat et leurs compétences*

### **A –Gendarmerie Nationale**

#### **Présentation de la mission**

La Gendarmerie Nationale conseille les entreprises pour améliorer la protection de leur patrimoine informationnel.

Elle apporte également une information sur la sécurité globale dans le cadre de la prévention de la délinquance.

L'institution apporte sa capacité d'analyse des vulnérabilités à toutes les PMI-PME, TPI-TPE de son ressort territorial qui présentent un intérêt en termes d'emploi ou de technologie.

### III. Que faire lorsqu'il est (presque) trop tard

Forte de son maillage territorial, l'exercice de l'intelligence économique, dans son volet défensif, s'inscrit dans la continuité des actions quotidiennes de tous les personnels visant à la protection des personnes et des biens, parmi lesquels figure naturellement la protection des entreprises.

Dans le cadre de ces missions, les personnels de la Gendarmerie interviennent lors de conférences au sein de clubs d'entreprises afin de sensibiliser à l'intelligence économique, ou lors de la réalisation d'audits de protection individualisés au sein des entreprises.

#### **Territorialité**

Les unités de gendarmerie nationale sont implantées sur l'ensemble du territoire français, en métropole et outre-mer.

La gendarmerie est chargée de la sécurité publique en dehors des grandes villes, ce qui représente environ 95% du territoire national et 50% de la population.

#### **Domaine de compétence**

Les personnels de la gendarmerie

sont juridiquement compétents pour traiter de toute infraction, et notamment de toute atteinte à un système de traitement automatisé de données.

Des enquêteurs spécialisés en technologies numériques (150 NTECH au 1er mai 2007) sont implantés sur l'ensemble du territoire.

La gendarmerie participe aux activités de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (O.C.L.C.T.I.C.) de la DCPJ de la police nationale. C'est une des modalités de l'échange permanent d'information entre les deux institutions dans ce domaine.

#### **Contact en Poitou-Charentes**

Chef d'escadron Christian VAURY,  
Région de gendarmerie de Poitou-Charentes

Tél.: 05 49 00 57 62

Fax : 05 49 00 57 78

[christian.vaury@gendarmerie.defense.gouv.fr](mailto:christian.vaury@gendarmerie.defense.gouv.fr)

## III. Que faire lorsqu'il est (presque) trop tard

### **Contact National**

Pour trouver un enquêteur spécialisé susceptible de répondre à vos questions ou de prendre une plainte dans votre secteur d'implantation, vous pouvez contacter toute brigade de gendarmerie et demander à être mis en relation avec un "enquêteur NTECH".

Vous pouvez aussi contacter la division de lutte contre la cybercriminalité du service technique de recherches judiciaires et de documentation (STRJD) à Rosny-sous-Bois en envoyant un courrier électronique à l'adresse [judiciaire@gendarmerie.defense.gouv.fr](mailto:judiciaire@gendarmerie.defense.gouv.fr).

### **B – O.C.L.C.T.I.C.**

#### **Présentation de la mission**

L'Office Centrale de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication est une structure nationale, à vocation inter-ministérielle et opérationnelle, compétente dans le domaine des infractions aux technologies de

l'information et de la communication.

Outre sa vocation opérationnelle, l'O.C.L.C.T.I.C. intègre d'autres missions relatives à l'animation, à la coordination, l'assistance technique, la centralisation et la diffusion de l'information dans le domaine de la cybercriminalité.

L'O.C.L.C.T.I.C. assure également la gestion des échanges internationaux (Interpol, Europol et G8H24) en tant que point de contact unique national dans son domaine d'activité.

L'O.C.L.C.T.I.C. gère enfin une plateforme police-gendarmerie de signalement sur Internet. Cette plateforme, qui est destinée à recueillir tous les signalements de contenus illicites sur Internet, fonctionne actuellement sur la base de relations engagées avec les professionnels de l'Internet et sera accessible au grand public fin 2007.

#### **Territorialité**

L'O.C.L.C.T.I.C. est compétent sur l'ensemble du territoire national. La Direction Centrale de la Police Judiciaire dispose également sur l'ensemble de ses services

## III. Que faire lorsqu'il est (presque) trop tard

territoriaux (Directions inter-régionales et régionales de Police Judiciaire) d'un réseau d'Enquêteurs Spécialisés en Criminalité Informatique compétents pour diligenter des enquêtes dans leur ressort de compétence géographique.

### **Domaine de compétence**

L'O.C.L.C.T.I.C; intervient sur des affaires d'envergure nationale et internationale dans le cadre d'enquêtes liées aux technologies de l'information et de la communication (ex : intrusion, entrave ou altération de systèmes informatiques, de contrefaçon de cartes de paiement, atteintes aux personnes et aux biens).

### **Contact**

[ocltic@interieur.gouv.fr](mailto:ocltic@interieur.gouv.fr)

Tél. : 01 47 44 97 55

### **Adresses web :**

- Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (O.C.L.C.T.I.C.)
- <http://www.internet-mineurs.gouv.fr>

pour ce qui concerne les signalements de contenus pédopornographiques.

### **C-DCRI**

#### **Présentation de la mission**

La Direction Centrale du Renseignement Intérieur est un service de renseignement de sécurité disposant de pouvoirs de police judiciaire spécialisée.

Le décret n°2008-609 du 27 juin 2008 (publié au journal officiel du 28 juin 2008) définit les missions et l'organisation de la Direction Centrale du Renseignement Intérieur (DCRI), grand service de renseignement intérieur unique qui marque la disparition de la DST (Direction de la Surveillance du Territoire) et des RG (Renseignements Généraux).

La DCRI a compétence pour rechercher et prévenir, sur le territoire de la République Française, les activités inspirées, engagées ou soutenues par des puissances étrangères et de nature à menacer la sécurité du pays, et plus

## IV. Evaluer ma sécurité en 10 questions

Généralement pour lutter contre ces activités.

A ce titre, la DCRI exerce une mission se rapportant à la défense.

### Territorialité

La Direction Centrale du Renseignement Intérieur est compétente sur tout le territoire national.

### Domaine de compétence

Concrètement, les missions de la DCRI sont traditionnellement de trois types : contre-espionnage, contre-terrorisme, protection du patrimoine économique et scientifique. De nouvelles menaces de niveau stratégique apparaissent et sont d'ores et déjà prises en compte, telles la prolifération des armes nucléaires, bactériologiques, chimiques et balistiques ou la grande criminalité organisée.

### Contact

Une cellule spécialisée dans la "cybercriminalité" peut être jointe au 01 77 92 5000.

## IV. Evaluer ma sécurité en 10 questions

### *IV.1 Organisationnel*

**Est-ce que je dispose d'une charte d'utilisation des moyens informatiques ?**

Oui : en définissant le cadre strict d'utilisation des moyens informatiques, je limite le risque d'utilisation frauduleuse ou de mauvais usage.

Non : s'il n'est pas indiqué clairement l'usage autorisé et les bons réflexes à employer, il est très probable qu'un sinistre lié au poste de travail surviendra.

**Ai-je procédé à une analyse de mes risques ?**

Oui : je peux mettre en place des moyens de protection adéquats permettant de protéger efficacement mes actifs.

Non : je ne sais pas quels pourront être les sinistres, ni comment les palier ou réduire leur impact.

## IV. Evaluer ma sécurité en 10 questions

**Le Responsable de la Sécurité des Systèmes d'Information dépend-il directement de la Direction Générale ?**

Oui : il aura alors les moyens de prendre des décisions en fonction des risques qui lui seront remontés et des critères stratégiques de l'entreprise.

Non : sans vision stratégique, le choix des moyens de protection ne pourra se faire de façon très opportune pour l'entreprise.

### IV.2 Technique

**Est-ce que je dispose de moyens de protection contre les codes malveillants ?**

Oui : la propagation de virus, chevaux de Troie,...sera bien plus difficile au sein de l'entreprise.

Non : l'introduction ou la connexion d'un élément extérieur (clef USB, flux d'informations , ...) peut contribuer à une infection du Système d'Information.

**Est-ce que je dispose de normes de développement ?**

Oui : toute norme permet d'éviter d'avoir de mauvaises surprises lors de la phase de maintenance de l'application achetée.

Non : les portes dérobées peuvent se trouver dans une application.

**Les extincteurs sont-ils correctement positionnés ?**

Oui : s'il n'est nul besoin de chercher trop longtemps les éléments nécessaires à une extinction incendie, le feu ne se propagera pas.

Non : le mauvais emploi d'un extincteur peut engendrer des flammes plus importantes.

### IV.3 Humain

**Est-ce que toutes les personnes travaillant dans le domaine de la sécurité reçoivent une formation régulière ?**

Oui : les techniques de vol et de destruction ont toujours une petite longueur d'avance sur les techniques de protection. Il est nécessaire d'avoir un personnel correctement formé et au fait des dernières techniques.

Non : la sécurité informatique est une science en perpétuelle évolution. S'arrêter sur un acquis est un mal qui risque de causer l'inefficacité du moyen de protection.

## IV. Evaluer ma sécurité en 10 questions

**Est-ce que tous mes salariés sont sensibilisés régulièrement à la sécurité ?**

**Oui** : une personne sensibilisée se posera de bonnes questions, lorsqu'un technicien lui demandera un identifiant ou l'accès à un local sensible.

**Non** : chaque salarié doit être acteur de la protection. Il est nécessaire de « former » le personnel à la sécurité de l'information.  
Ex : ne pas jeter un document important, mais le détruire.

**Non** : l'évaluation d'un moyen de sécurité par un expert du domaine permettra d'obtenir un regard neuf et non biaisé du sujet. De plus, cela permettra de soulever des problématiques autres non évaluées en interne par manque de temps/compétence/expertise.

**Est-ce que tout intervenant extérieur est identifié et contrôlé ?**

**Oui** : l'accès pourra alors être correctement contrôlé dans chacun de ses déplacements.

**Non** : si l'intervenant est malveillant, il pourra alors s'attaquer à n'importe quel élément de la chaîne de protection.

**Suis-je le seul à évaluer ma sécurité ?**

**Oui** : la sécurité par l'obscurité n'a jamais payé. En effet, ce n'est pas le fait d'utiliser des mécanismes uniques et non évalués par des experts du domaine qui prouve que ma sécurité est bonne.

## LE CLUSIF



Le CLUSIF est un club professionnel, constitué en association indépendante, ouvert à toute entreprise ou collectivité.

Il accueille des utilisateurs et des offreurs issus de tous les secteurs d'activité de l'économie.

La finalité du CLUSIF est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques.

Il entend ainsi sensibiliser tous les acteurs en intégrant une dimension transversale dans ses groupes de réflexion : management des risques, droit, intelligence économique ...

Les réflexions menées par le Clusif s'élaborent au sein de Groupes de Travail (GT), certains étant regroupés en Espace de Travail. Les thématiques des GT sont choisies par les membres : tout membre du Clusif peut proposer de créer un GT. Chaque groupe a pour objectif de publier un ouvrage.

Il se constitue de nouveaux groupes tout au long de l'année. La liste ci-

dessous est donc amenée à évoluer en permanence.

### Les groupes actifs en 2008

- Botnet
- Conception d'un centre informatique sécurisé
- Criminalistique
- Documentation de MEHARI™
- Enquête sur les politiques de sécurité et la sinistralité informatique en France
- Fiches de sécurité pour la micro-informatique
- Gestion des incidents
- Infogérance
- Intégration de MEHARI™
- Label Formation CLUSIF
- Malveillance téléphonique
- MEHARI 2007
- Panorama de la cybercriminalité
- Série 27000 / Métriques

Outre ces groupes, des Espaces coordonnent des réflexions autour de thèmes centralisateurs :

### Espaces de travail actifs en 2008

- Espace Méthodes
- Espace Menaces
- Espace RSSI

## LE CLUSIR

**Les CLUSIR, Club de la Sécurité de l'Information Régionaux, sont des associations régionales décentralisées par Le CLUSIF (Club de la Sécurité de l'Information Français).**

**Agréées par le CLUSIF, ces antennes ont pour objectif de rassembler l'ensemble des acteurs de la sécurité des Systèmes d'Informations (institutionnels, collectivités publiques, entreprises privées...) afin de participer à un véritable observatoire des pratiques et risques liés aux Systèmes d'Information.**



**Le CLUSIR Poitou-Charentes est donc le dernier né des CLUSIR !**

Créé début octobre 2008, ce projet a été mis en route il y a plus d'un an

grâce aux 7 fondateurs actuels, tous occupant des fonctions de Responsables Sécurité ou Consultant Sécurité.

*« Nous avons pour vocation de relayer en région les travaux réalisés par le CLUSIF mais également de mettre en œuvre nos propres actions locales et régionales afin d'améliorer la compétence de tous », déclare Sébastien Gioria, Président du CLUSIR Poitou-Charentes.*

*« Notre ambition est d'échanger continuellement sur les nouvelles pratiques et les nouveaux enjeux actuels dans le monde des systèmes d'information, d'être en veille constante et d'informer à travers nos membres, tous professionnels du secteur ».*

Le bureau a décidé la création de 3 groupes de travail pour 2009.

**Groupe de travail sur les aspects juridiques liés à la sécurité** : CNIL, responsabilité du chef d'entreprise, open source, charte NTIC, propriété intellectuelle des développements, ...

**Groupe de travail sur les indicateurs de la sécurité** : tableaux de bord qualitatifs, quantitatifs, financiers, ...

**Groupe de travail sur la gestion globale du poste de travail** : mobilité, sauvegardes, chiffrement, sécurité des accès distants, mises à jour des postes, ... Ce groupe de travail sera volontairement orienté TPE et PME.

A ce jour, une vingtaine d'institutions et entreprises locales (de toute taille et de tous secteurs d'activité) ont porté un vif intérêt à rejoindre le CLUSIR en qualité de membre. « *Nous en sommes au début et nous travaillons tous pour accroître notre notoriété et visibilité afin d'inciter le maximum de sociétés à nous rejoindre* », ajoute Sébastien Gioria.



Ce cahier a été conçu et rédigé par

*Sébastien GIORIA*

Expert en sécurité des Systèmes d'informations

Président du Clusir Poitou-Charentes

Membre du CLUSIR

Tel : 05 49 32 49 20—06 23 04 00 51

E-mail : s.gioria@fr-c.com



Technopole Venise Verte

Rue Euclide

79024 NIORT Cedex

Sébastien GIORIA

Tel : 05 49 32 49 20—06 23 04 00 51

E-mail : s.gioria@fr-c.com